

iES26GF

Intelligent 26 Port Managed Gigabit Ethernet Switch
IEC61850-3 and IEEE1613 Compliant



Version 1.92.4, Nov 2023



SERVICES • SUPPORT • SECURITY • SOLUTIONS • SYSTEMS

© 2023 iS5 Communications Inc. All rights reserved.

COPYRIGHT NOTICE

© 2023 iS5 Communications Inc. All rights reserved.

No part of this publication may be reproduced in any form without the prior written consent of iS5 Communications Inc. (iS5).

TRADEMARKS

iS5Com is a registered trademark of iS5. All other trademarks belong to their respective owners.

REGULATORY COMPLIANCE STATEMENT

Product(s) associated with this publication complies/comply with all applicable regulations. For more details, refer to the [Technical Specifications](#) section.

WARRANTY

iS5 warrants that all products are free from defects in material and workmanship for a specified warranty period from the invoice date (5 years for most products). iS5 will repair or replace products found to be defective within this warranty period including shipping costs. This warranty does not cover product modifications or repairs done by persons other than iS5-approved personnel, and this warranty does not apply to products that are misused, abused, improperly installed, or damaged by accident.

Refer to the [Technical Specifications](#) section for the actual warranty period(s) of the product(s) associated with this publication.

DISCLAIMER

Information in this publication is intended to be accurate. iS5 shall not be responsible for its use or infringements on third-parties because of the use of this publication. There may occasionally be unintentional errors on this publication. iS5 reserves the right to revise the contents of this publication without notice.

CONTACT INFORMATION

iS5 Communications Inc.

5895 Ambler Drive, Mississauga, ON, L4W 5B7

Tel: 1+ 905-670-0004

Website: www.iS5Com.com

Technical Support

E-mail: support@iS5Com.com

Sales Contact

E-mail: info@is5com.com

Table of Contents

FCC STATEMENT AND CAUTIONS	1
Federal Communications Commission Radio Frequency Interference Statement	1
Caution: LASER.....	1
Caution: Service	1
Caution: Physical Access	1
 1. Getting Started	 2
1.1 About iES26GF	2
1.2 Acronyms.....	2
1.3 Software Features.....	5
1.4 Hardware Features.....	5
 2. Hardware Overview	 6
2.1 Front Panel	6
2.2 Rear Panel View	7
2.3 Power Panel.....	7
 3. Hardware Installation.....	 9
3.1 Rack Mount Assembly	9
3.2 Wiring	10
3.2.1 Grounding.....	10
3.2.2 Power Inputs	11
3.2.3 Fault Relay	12
3.3 Connection.....	13
3.3.1 Ethernet Cables	13
3.3.2 SFP	16
3.3.3 iRing/iChain.....	17
 4. Redundancy.....	 19
4.1 iRing Introduction	19
4.2 iChain Introduction	20
4.3 STP/RSTP/MSTP	21
4.3.1 STP/RSTP Introduction	21
4.3.2 MSTP Introduction.....	21
4.4 MRP Introduction	21
4.5 Fast Recovery Introduction	21
 5. Management.....	 22
5.1 Basic Settings	23
5.1.1 System Information Configuration	23
5.1.2 Banner.....	24
5.1.3 Admin Password	25
5.1.4 Guest Password	25
5.1.5 Authentication Method.....	26

5.1.6	Auto Logout.....	26
5.1.7	IP Setting.....	27
5.1.8	IPv6 Configuration	27
5.1.9	SNTP Configuration (only for SNTP Version)	28
5.1.10	NTP Configuration (only for NTP Version)	28
5.1.11	Daylight Saving Time	30
5.1.12	Switch Time.....	33
5.1.13	HTTPS Configuration.....	33
5.1.14	SSH.....	34
5.1.15	Telnet.....	34
5.1.16	LLDP	35
5.1.17	MODBUS TCP	38
5.1.18	Backup & Restore Configuration	39
5.1.19	Upgrade Firmware.....	39
5.2	DHCP Server/Relay.....	40
5.2.1	Setting.....	40
5.2.2	DHCP Dynamic Client List	41
5.2.3	DHCP Static Client List	41
5.2.4	DHCP Relay Agent	42
5.3	Port Setting.....	45
5.3.1	Port Control.....	45
5.3.2	Port Trunk	46
5.3.3	Loop Protection.....	51
5.4	Redundancy	53
5.4.1	iRing Configuration.....	53
5.4.2	iChain.....	53
5.4.3	iBridge	54
5.4.4	RSTP	55
5.4.5	MSTP	59
5.4.6	MRP	66
5.4.7	Fast Recovery.....	67
5.4.8	Dual Port Recovery	68
5.5	VLAN.....	70
5.5.1	VLAN Membership	70
5.5.2	Port Configurations.....	71
5.5.3	Private VLAN.....	79
5.6	SNMP.....	81
5.6.1	SNMP System Configuration	81
5.6.2	SNMP Trap Configuration	81
5.6.3	SNMPv3 Communities Configuration.....	82
5.6.4	SNMP Users Configuration.....	83
5.6.5	SNMP Group Configuration	85
5.6.6	SNMP View Configuration.....	85
5.6.7	SNMP Access Configuration.....	87
5.7	Traffic Prioritization.....	88
5.7.1	Storm Control.....	88
5.7.2	Port Classification	88
5.7.3	Port Tag Remarking	90
5.7.4	Port DSCP.....	91
5.7.5	Port Policing.....	92

5.7.6	Queue Policing	92
5.7.7	Port Scheduler	93
5.7.8	DSCP Based QoS	97
5.7.9	DSCP Translation	98
5.7.10	DSCP Classification.....	99
5.7.11	QoS Control List	99
5.7.12	QoS Statistics.....	102
5.7.13	QCL Status.....	103
5.8	Multicast.....	104
5.8.1	IGMP Snooping Basic Configuration	104
5.8.2	IGMP Snooping VLAN Configuration.....	105
5.8.3	IGMP Snooping Status	106
5.8.4	IGMP Snooping Group Information.....	107
5.9	Security	108
5.9.1	Remote Control Security Configurations	108
5.9.2	Device Binding.....	108
5.9.3	ACL	114
5.9.4	AAA.....	119
5.9.5	NAS (802.1x)	124
5.10	Warning	135
5.10.1	Fault Alarm.....	135
5.10.2	System Warning.....	136
5.11	Monitoring and Diagnostic.....	139
5.11.1	MAC Table	139
5.11.2	Port Statistics.....	141
5.11.3	Port Monitoring.....	143
5.11.4	System Log Information	143
5.11.5	SFP Monitor.....	144
5.11.6	Ping	145
5.11.7	Ping6	146
5.12	Factory Defaults	148
5.13	System Reboot.....	148
5.14	Command Line Interface Management.....	149
5.14.1	CLI Management by RS-232 Serial Console (115200, 8, none, 1, none).....	149
5.14.2	CLI Management by Telnet.....	151

Appendix A: iES26GF Modbus Information 171

Table of Figures

Figure 1 - Front View.....	6
Figure 2 - Rear Panel View	7
Figure 3 - Power Panel View.....	7
Figure 4- iES26GF Dimensions	9
Figure 5 - Grounding.....	10
Figure 6 - Power Inputs.....	11
Figure 7 - Fault Relay.....	12
Figure 8 - RJ45 Cable.....	15
Figure 9 - Connection between TX port (Switch A) and RX port (Switch B)	16

Figure 10 - Ring Topology	17
Figure 11 - Coupling Ring	17
Figure 12 - Dual Homing	18
Figure 13 - iChain Topology	18
Figure 14 - iRing Topology	19
Figure 15 - iChain Topology iBridge	20
Figure 16 - Login screen	22
Figure 17 - Main Interface	23
Figure 18 - System Information Configuration interface	23
Figure 19 - System Banner Configuration interface	24
Figure 20 - System Password interface	25
Figure 21 - Guest Password Configuration interface	25
Figure 22 - Authentication Method Configuration interface	26
Figure 23 - Auto Logout Configuration interface	26
Figure 24 - IP Configuration interface	27
Figure 25 - IPv6 Configuration interface	27
Figure 26 - IP Configuration interface	28
Figure 27 - NTP Configuration	28
Figure 28 - Time Zone Configuration interface	30
Figure 29 - Switch Time Configuration interface	33
Figure 30 - HTTPS Configuration interface	33
Figure 31 - SSH Configuration interface	34
Figure 32 - Telnet Configuration interface	34
Figure 33 - LLDP Configuration interface	35
Figure 34 - LLDP Neighbour Information	36
Figure 35 - LLDP Global Counters interface	37
Figure 36 - MODBUS Configuration Interface	38
Figure 37 - Configuration Save Interface	39
Figure 38 - Configuration Upload interface	39
Figure 39 - Upgrade Firmware interface	39
Figure 40 - DHCP Server Configuration interface	40
Figure 41 - DHCP Dynamic Client List interface	41
Figure 42 - DHCP Client List	41
Figure 43 - DHCP Relay Configuration interface	42
Figure 44 - DHCP Relay Statistics interface (Server Statistics)	43
Figure 45 - DHCP Relay Statistics interface (Client Statistics)	44
Figure 46 - Port Configuration interface	45
Figure 47 - Aggregation Mode Configuration interface (Hash Code Contributors)	46
Figure 48 - Aggregation Group Configuration interface	46
Figure 49 - LACP Port Configuration interface	47
Figure 50 - LACP System Status interface	48
Figure 51 - LACP Status interface	49
Figure 52 - LACP Statistics interface	50
Figure 53 - Global Settings interface (Global Configuration)	51
Figure 54 - Port Configuration interface	51
Figure 55 - Loop Protection Status interface	52
Figure 56 - iRing Configuration interface	53
Figure 57 - iChain Configuration interface	54
Figure 58 - iBridge interface	54
Figure 59 - RSTP Bridge Setting interface	55
Figure 60 - RSTP Port Setting interface	56
Figure 61 - RSTP Bridge Status interface	57
Figure 62 - RSTP Port Status interface	58
Figure 63 - STP Bridge Configuration interface	59
Figure 64 - MSTI Configuration interface	61
Figure 65 - MSTI Configuration interface	61
Figure 66 - CIST Aggregated Port Configuration interface	62
Figure 67 - MST1 MSTI Port Configuration interface	64
Figure 68 - STP Bridges interface	64
Figure 69 - STP Port Status interface	65

Figure 70 - STP Statistics interface	66
Figure 71 - MRP	66
Figure 72 - Fast Recovery interface	67
Figure 73 - Dual Port Recovery interface	69
Figure 74- VLAN Membership Configuration interface	70
Figure 75 - VLAN Port Configuration interface	71
Figure 76 - Unaware and C-port Port Types	73
Figure 77 - S-port and S-custom Port Types	74
Figure 78 - VLAN Access Mode topology	75
Figure 79 - VLAN 1Qtrunk Mode topology	76
Figure 80 - VLAN QinQ Mode topology	78
Figure 81 - Private VLAN Membership Configuration interface	79
Figure 82 - Port Isolation Configuration interface	80
Figure 83 - SNMP System Configuration interface	81
Figure 84 - SNMP Trap Configuration interface	81
Figure 85 - SNMPv3 Community Configuration interface	82
Figure 86 - SNMPv3 User Configuration	83
Figure 87 - SNMPv3 Group Configuration interface	85
Figure 88 - SNMPv3 View Configuration interface	85
Figure 89 - SNMPv3 Access Configuration interface	87
Figure 90 - Storm Control Configuration interface	88
Figure 91 - QoS Ingress Port Classification interface	88
Figure 92 - QoS Egress Port Tag Remarking interface	90
Figure 93 - QoS Port DSCP Configuration interface	91
Figure 94 - QoS Ingress Port Policers interface	92
Figure 95 - QoS Ingress Queue Policers interface	92
Figure 96 - QoS Egress Port Schedulers interface	93
Figure 97 - QoS Egress Port Scheduler and Shapers Port 1	94
Figure 98 - QoS Egress Port Scheduler and Shapers Port 1	95
Figure 99 - QoS Egress Port Shapers interface	96
Figure 100 - DSCP-Based QoS Ingress Classification interface	97
Figure 101 - DSCP Translation interface	98
Figure 102 - DSCP Classification interface	99
Figure 103 - QoS Control List Configuration interface	99
Figure 104 - QCE Configuration interface	100
Figure 105 - Queuing Counters	102
Figure 106 - QoS Control List Status interface	103
Figure 107 - IGMP Snooping Configuration interface	104
Figure 108 - IGMP Snooping VLAN Configuration	105
Figure 109 - IGMP Snooping Status	106
Figure 110 - IGMP Snooping Group Information interface	107
Figure 111 - Remote Control Security Configuration interface	108
Figure 112 - Device Binding interface	108
Figure 113 - Alias IP Address interface	109
Figure 114 - Alive Check interface	110
Figure 115 - DDOS Prevention interface	111
Figure 116 - Device Description interface	112
Figure 117 - Steam Check interface	113
Figure 118 - ACL Ports Configuration	114
Figure 119 - ACL Rate Limiter Configuration	115
Figure 120 - Access Control List Configuration interface	116
Figure 121 - ACE Configuration interface	116
Figure 122 - ACL Status interface	118
Figure 123 - Authentication Server Configuration interface	119
Figure 124 - Radius Authentication Server Status Overview interface	120
Figure 125 - RADIUS Authentication Statistics for Server #1 interface	121
Figure 126 - Network Access Server Configuration interface	126
Figure 127 - Network Access Server Switch Status interface	130
Figure 128 - NAS Statistics Port 1 interface	131
Figure 129 - Fault Alarm interface	135

Figure 130 - System Log Configuration interface	136
Figure 131 - SMTP Setting interface	136
Figure 132 - System Warning - Event Selection	137
Figure 133 - MAC Address Table Configuration	139
Figure 134 - MAC Address Table	140
Figure 135 - Port Statistics Overview interface	141
Figure 136 - Detailed Port Statistics Port 1	142
Figure 137 - Mirror Configuration interface	143
Figure 138 - System Log Information interface	143
Figure 139 - SFP Monitor interface	144
Figure 140 - ICMP Ping	145
Figure 141 - ICMPv6 Ping	146
Figure 142 - Factory Defaults	148
Figure 143 - System Reboot interface	148
Figure 144 - Tera Term VT interface	149
Figure 145 - Tera Term: Serial port setup interface	150
Figure 146 - Console Login Screen	150
Figure 147 - Windows Run interface	151
Figure 148 - Telnet Login Screen	151

Table of Tables

Table 1- Cable Types and Specifications	13
Table 2- 10/100 Base-T RJ45 Pin Assignments	13
Table 3- 1000 Base-T RJ45 Pin Assignments	13
Table 4- 10/100 Base-T MDI/MDI-X pin Assignments	14
Table 5- 1000 Base-T MDI/MDI-X pin Assignments	14
Table 6- Console Cable pin Assignments	15

FCC STATEMENT AND CAUTIONS

Federal Communications Commission Radio Frequency Interference Statement

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

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

Caution: LASER

This product contains a laser system and is classified as a CLASS 1 LASER PRODUCT. Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.

Caution: Service

This product contains no user-serviceable parts. Attempted service by unauthorized personnel shall render all warranties null and void.

Changes or modifications not expressly approved by iS5 Communications Inc. could invalidate specifications, test results, and agency approvals, and void the user's authority to operate the equipment.

Should this device require service, please contact support@iS5Com.com.

Caution: Physical Access

This product should be installed in a restricted access location. Access should only be gained by qualified service personnel or users who have been instructed on the reasons for the restrictions applied at the location, and any precautions that have been taken. Access must only be via the use of a tool or lock and key, or other means of security, and is controlled by the authority responsible for the location.

1. GETTING STARTED

1.1 About iES26GF

The iES26GF is a powerful managed industrial switch for power station applications with many features. The iES26GF is an IEC 61850-3 and IEEE 1613 compliant switch which can operate under a wide temperature range, in dusty environments, and humid conditions.

It can be managed by the WEB, TELNET, the Console, or other third-party SNMP software. It can also be managed by iS5Com's network management suite iManage. iManage has a friendly and powerful interface which can be used to configure easily multiple switches at the same time and monitor switch's status.

1.2 Acronyms

The following table shows all acronyms used in this document.

Acronym	Explanation
ACE	Access Control Entry
ACL	Access Control List
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
CLI	Command Line Interface
DCHP	Dynamic Host Configuration Protocol
DDM	Digital Diagnostic Monitoring
DEI	Discard Eligibility (subfield in an <i>IEEE 802.1Q</i> frame header)
DNS	Domain Name Server
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DP	Drop Precedence
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
HLN	Hardware Address Length
HRD	hardware address space (i.e. ARP <i>hardware address type</i> (ar\$hrd)))

Acronym	Explanation
HSR	High-availability Seamless Redundancy
HTTPS	Hyper Text Transfer Protocol Secure or HTTP over SSL
ICMP	Internet Control Message Protocol
IP	Internet Protocol (IP)
IPMCv4	IPv4 MultiCast
LLDP	Link Layer Discovery Protocol
LLDP- MED	LLDP - Media Endpoint Discovery
LLDPDU	LLDP Data Unit
MIB	Management Information Base
MRP	Media Redundancy Protocol
MSTI	Multiple Spanning Tree Instances
MSTP	Multiple Spanning Tree Protocol
NTP	Network Time Protocol
OID	Object Identifier
OUI	Organizationally Unique Identifier (In Linux)
PDU	Protocol Data Unit
PID	Process Identifier
P2P	Point-To-Point (link)
PSH	Push Function (a value for the ACE)
PWR	Power
QCE	QoS Control Entry
QCL	QoS Control List
QoS	Quality of Service
RARP	Reverse Address Resolution Protocol (Reverse ARP)
RIP	Routing Information Protocol

Acronym	Explanation
RMON	Remote Monitoring
RSTP	Rapid Spanning Tree Protocol
SIP	Source IP
SMAC	Source MAC Address
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SSAP	Source Service Access Point
SSH	Secure Shel
TACACS	Terminal Access Controller Access Control System
TCN	Topology Change Notification
TCP	Transmission Control Protocol
THA	target Hardware Address
TLV	Type-Length-Value
TPID	Tag protocol identifier
TTL	Time to live
SSH	Secure Shell
UDP	User Datagram Protocol
URG	Urgent Pointer Field Significant (an ACE value)
USM	User-based Security Model
UTC	Coordinated Universal Time
VACM	View based Access Control Model
VCXO	Voltage Controlled Crystal Oscillator
VID	VLAN ID
VRIP	Virtual Router IP

1.3 Software Features

- Dynamic Host Configuration Protocol (DHCP) server function (5.2)
- Web or CLI based Management (RS-232 Serial Console or Telnet/SSH) (5.14)
- Redundancy—RSTP/MSTP, Fast Recovery and Dual Port Recovery
- VLAN (802.1Q) to segregate and secure network traffic (5.5)
- Supports SNMPv1/v2/v3 (5.6)
- Traffic Prioritization—Storm Control and Quality of Service (QoS) including DSCP Based QoS Ingress Port Classification (5.7)
- Multicast traffic—IGMP Snooping (IGMP v1/v2 / v3) and Unregistered IPMCv4 Flooding enabled (5.8)
- Security—Access Control List (ACL) for every port, AAA – Radius Server Configuration, network access control (NAS) (802.1x), Remote Control Security, and Device Binding (5.9)
- Supports standard IEC 62439-2 MRP (Media Redundancy Protocol) functionality
- Warnings (Syslog and SMTP) and Fault Alarm (power failure) (5.10)
- Monitoring and Diagnostics—MAC Table and Port Statistics (ports monitoring including for SFP ports, system information, issuing ICMP PING packets for troubleshoot IP connectivity issues) (5.11)

1.4 Hardware Features

- Isolated redundant power inputs—dual inputs of 18-36VDC or 36-75VDC, or 110-370VDC or 90-264VAC
- Operating Temperature—from -40°C to 85°C
- Operating Humidity—5% to 95%, non-condensing
- Up to 24 x 10/100Base-T(X) RJ45 Ethernet ports
- 2 X 10/100/1000Base-T(X) RJ45, or 2 X 1000Base-X SFP, or Combo 2 X 10/100/1000Base-T(X) RJ45 and 2 X 1000Base-X SFP, or 2 X 1000SX MM SC/ST, or 2 X 1000LX SM SC/ST
- 1 x Console Port
- Dimensions—486 (W) x 290 (D) x 44 (H) mm (19.12 x 11.41 x 1.74 inches)
- 19 inches rack mountable, IP40 galvanized steel chassis

2. HARDWARE OVERVIEW

2.1 Front Panel

Product description

Port	Description
10/100 RJ-45 fast Ethernet ports	Up to 24 x 10/100Base-T(X) RJ-45 fast Ethernet ports supporting auto-negotiation. Default Setting: Speed: auto Duplex: auto Flow control: disable
Gigabit ports	2 X 10/100/1000Base-T(X) RJ45 or 2 X 1000Base-X SFP or Combo 2 X 10/100/1000Base-T(X) RJ45 and 2 X 1000Base-X SFP, or 2 X 1000SX MM SC/ST, or 2 X 1000LX SM SC/ST
Console	Use a RS-232 to RJ-45 cable assembly to manage the switch

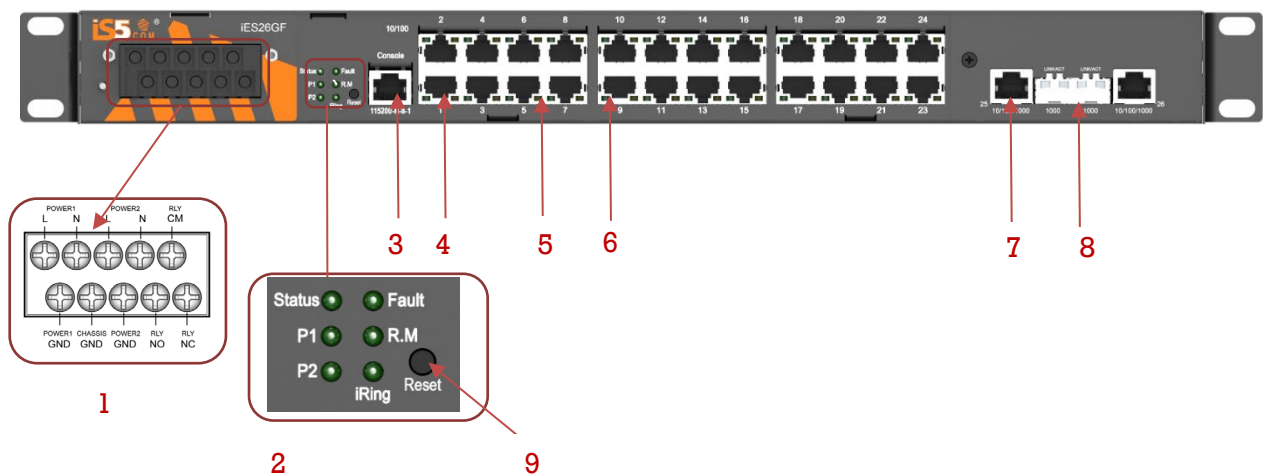


Figure 1 - Front View

- Power supply input
- LED Status:
 - P1 LED: PWR1, shows status of power supply 1
 - P2 LED: PWR2, shows status of power supply 2
 - Status LED: **ON** when the system is ready
 - R. M LED: Ring master. **ON** indicates that the switch is operating as the Master
 - iRing LED: **ON** indicates that iRing is activated.
 - Fault LED: **ON** (amber) indicates that a fault occurred. Fault relay, power failure or port down/fail.
- RS-232 Console Port; Set connection at 115200bps, N, 8, 1
- 10/100Base-T(X) Ethernet ports
- LED for Ethernet ports Link status
- LED for Ethernet ports ACT status
- 1000Base-X fiber ports
- 10/100/1000Base-T(X) Ethernet port
- Reset Button

2.2 Rear Panel View

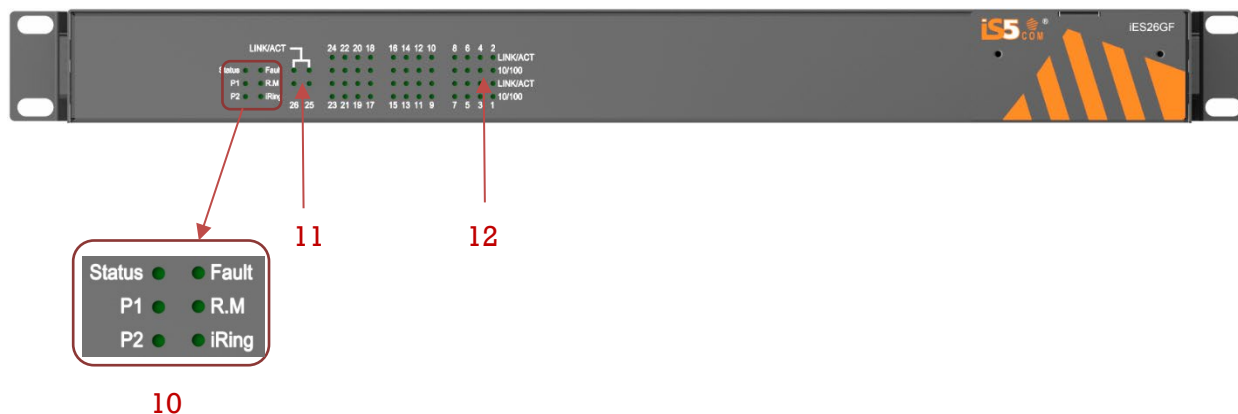


Figure 2 - Rear Panel View

10. LED Status (rear panel)

- Status LED: **ON** when the system is ready
- P1 LED: PWR1, it shows status of power supply one (1)
- P2 LED: PWR2, it shows status of power supply two (2)
- Fault LED: **ON** (amber) indicates that a fault occurred. Fault relay, power failure, or port down/failed for ports 25 and 26 (Link/ACT status)
- R. M LED: Ring master. **ON** indicates that the switch is operating as the Master
- iRing LED: **ON** indicates that iRing is activated.

11. LED for ports 25 and 26 Link / ACT status

12. LED for Combo Copper Ports Link/ACT status

2.3 Power Panel

The iES26GF's power connections are as follows:

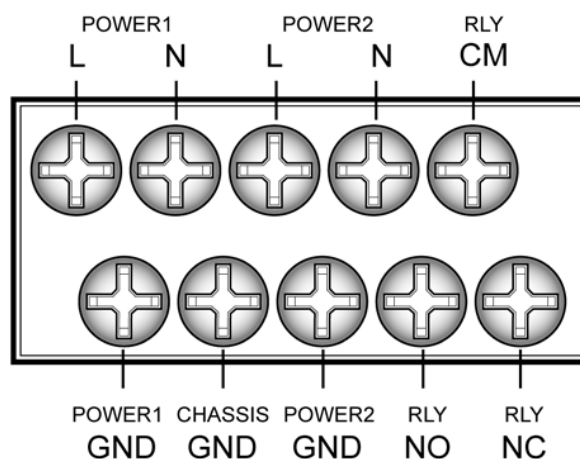


Figure 3 - Power Panel View

Note:

RLY COM– Relay Com

RLY NO – Relay Normal Open

RLY NC – Relay Normal Close

Chassis Connections

Terminal No	Description	Connection
1	PWR1 (L)–Live	Connected to the (Live) terminal of an AC power source
2	PWR1 (G)–Ground	Power supply 1 round connection.
3	PWR1 (N)–Neutral	Connected to the (Neutral) terminal of an AC power source.
4	G–Chassis Ground	Connected to the Safety Ground terminal for AC Units or the ground bus for DC inputs. Chassis Ground connects to both power supply surge grounds via a removable jumper.
5	PWR2 (L)–Live	Connected to the (Live) terminal of an AC power source.
6	PWR2 (G)–Ground	Power supply 2 round connection.
7	PWR2 (N)–Neutral	Connected to the (Neutral) terminal of an AC power source.
8	RLY NO	Failsafe Relay, (Normally Open) contact.
9	RLY CM	Failsafe Relay (Common) contact.
10	RLY NC	Failsafe Relay (Normally Closed) contact.



- 100-240VAC rated equipment: A 250VAC appropriately rated circuit breaker must be installed.
- Equipment must be installed according to the applicable country wiring codes.
- When equipped with a HI voltage power supply and DC backup,



- 88-300VDC rated equipment: A 300VDC appropriately rated circuit breaker must be installed.
- A circuit breaker is not required for DC power supply voltages of 10-48VDC.
- For Dual DC power supplies, separate circuit breakers must be installed and separately identified.
- Equipment must be installed according to the applicable country wiring

3. Hardware Installation

3.1 Rack Mount Assembly

The iES26GF comes with a kit for rack mount assembly.

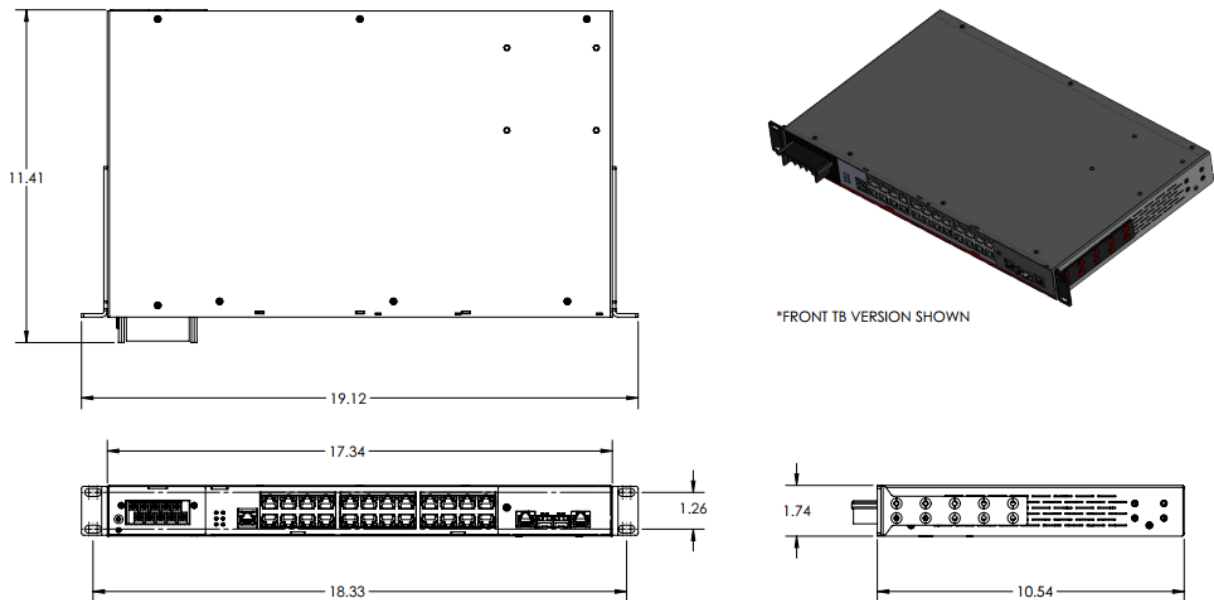


Figure 4- iES26GF Dimensions

3.2 Wiring



WARNING

Do not disconnect modules or wires unless power has been turned off or the area is known to be non-hazardous. Ensure that the proper supply voltage is supplied as indicated on the power supply label.



ATTENTION

1. Be sure to disconnect the power cord before installing and/or wiring your switches.
2. Calculate the maximum possible current in each power wire and common wire. Observe all electrical codes dictating the maximum current allowable for each wire size.
3. If the current goes above the maximum ratings, the wiring could overheat, causing serious damage to your equipment.
4. Use separate paths to route wiring for power and devices. If power wiring and device wiring paths must cross make sure the wires are perpendicular at the intersection point.
5. Do not run signal or communications wiring and power wiring through the same wire conduit. To avoid interference, wires with different signal characteristics should be routed separately.
6. You can use the type of signal transmitted through a wire to determine which wires should be kept separate. The rule of thumb is that wiring sharing similar electrical characteristics can be bundled together.
7. You should separate input wiring from output wiring.
8. It is advised to label the wiring to all devices in the system.

3.2.1 Grounding

Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the Earth GND screw to the grounding surface prior to connecting devices.

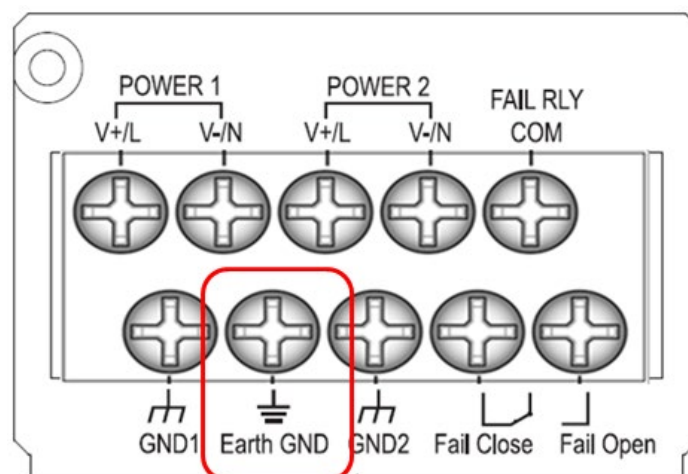


Figure 5 - Grounding

3.2.2 Power Inputs

The iES26GF supports dual redundant, hot swappable power supplies, Power Supply 1 (PWR1) and Power Supply 2 (PWR2). The connections for PWR1 and PWR2 are located on the terminal block. To connect power, follow the steps below:

- 1) Remove the cover designed for protection from the terminal block.
- 2) Connect the ground from the first power source to GND1 terminal screw.
- 3) Connect the Positive or Live from the first power source to the POWER 1 V+/L terminal screw.
- 4) Connect the Negative or Neutral from the first power source to the POWER 1 V-/N terminal screw.
- 5) If a redundant power supply is required repeat steps 2 to 4 connecting the wires from the second power source to the POWER 2 terminal screws.
- 6) To keep the wires from pulling loose, use a small flat-blade screwdriver to tighten the wire-clamp screws on the front of the terminal block connector.
- 7) After wiring is completed, put the transparent cover back onto the terminal block

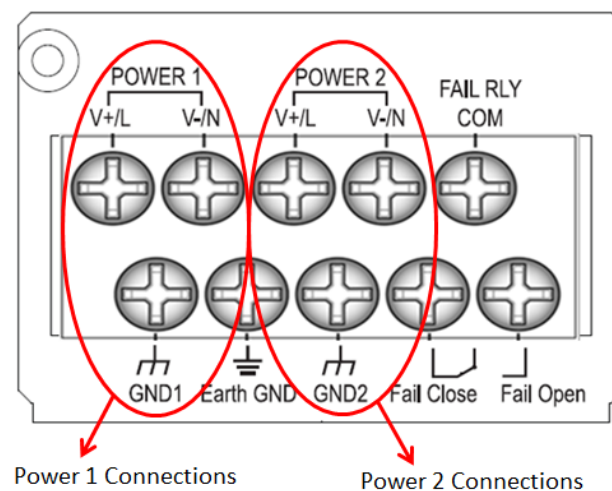


Figure 6 - Power Inputs

3.2.3 Fault Relay

The relay contact of the terminal block connector is used to detect user-configured events. The switch provides fail open and fail close options to form relay circuits based on requirements. The contacts are energized upon power-up of the unit and remain energized unless a critical error occurs. One common application for this output is to signal an alarm if a power failure or removal of control power occurs.

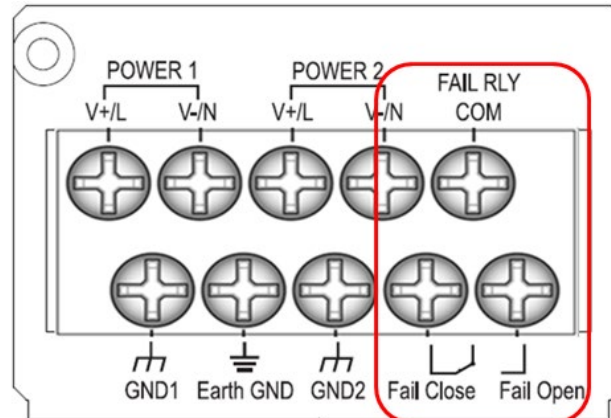


Figure 7 - Fault Relay

3.3 Connection

3.3.1 Ethernet Cables

The iES26GF switch has standard Ethernet ports. According to the link type, these switches use CAT 3, 4, 5, or 5e UTP cables to connect to other network devices i.e. PCs, servers, switches, routers, or hubs. Refer to the following table for cable specifications.

Table 1 - Cable Types and Specifications

Cable	Type	Max. Length	Connector
10BASE-T	Cat.3, 4, 5 100-ohm	UTP 100 m (328 ft)	RJ-45
100BASE-TX	Cat.5 100-ohm UTP	UTP 100 m (328 ft)	RJ-45
1000BASE-T	Cat.5/Cat.5e 100-ohm UTP	UTP 100 m (328ft)	RJ-45

3.3.1.1 100Base-T(X)/10Base-T Pin Assignments

With 100Base-T(X)/10Base-T cable, pins 1 and 2 are used for transmitting data. Pins 3 and 6 are used for receiving data.

Table 2 - 10/100 Base-T RJ45 Pin Assignments

Pin Number	Assignment
1	TD+
2	TD-
3	RD+
4	Not used
5	Not used
6	RD-
7	Not used
8	Not used

Table 3 - 1000 Base-T RJ45 Pin Assignments

Pin Number	Assignment
1	BI_DA+
2	BI_DA-
3	BI_DB+
4	BI_DC+
5	BI_DC-
6	BI_DB-
7	BI_DD+
8	BI_DD-

The iES26GF switch supports auto MDI/MDI-X operation; a straight-through cable can be used to connect a PC to the switch.

The table below shows the 10Base-T/100Base-T(X), MDI and MDI-X port pin outs.

Table 4 - 10/100 Base-T MDI/MDI-X pin Assignments

Pin Number	MDI port	MDI-X port
1	TD+(transmit)	RD+(receive)
2	TD-(transmit)	RD-(receive)
3	RD+(receive)	TD+(transmit)
4	Not used	Not used
5	Not used	Not used
6	RD-(receive)	TD-(transmit)
7	Not used	Not used
8	Not used	Not used

Table 5 - 1000 Base-T MDI/MDI-X pin Assignments

Pin Number	MDI port	MDI-X port
1	BI_DA+	BI_DB+
2	BI_DA-	BI_DB-
3	BI_DB+	BI_DA+
4	BI_DC+	BI_DD+
5	BI_DC-	BI_DD-
6	BI_DB-	BI_DA-
7	BI_DD+	BI_DC+
8	BI_DD-	BI_DC-

Note: “+” and “-” signs represent the polarity of the wires that make up each wire pair.

3.3.1.2 Console Cable

The iES26GF switch can be managed via the console port. Using the supplied standard DB-9 to RJ45 cable, you can connect to a local PC.

Table 6 - Console Cable pin Assignments

PC pin out (male) assignment	DB9 to RJ 45
Pin #2 RD	Pin #2 TD
Pin #3 TD	Pin #3 RD
Pin #5 GD	Pin #5 GD

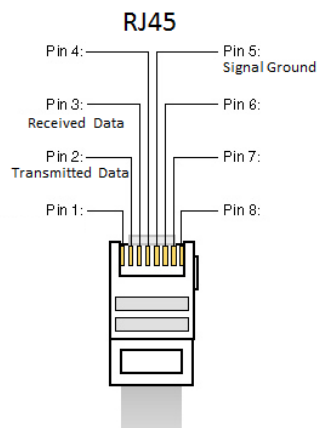


Figure 8 - RJ45 Cable

3.3.2 SFP

For ports 25 and 26, the iES26GF has fiber optical ports with options for SFP, SC, and ST connectors.

The fiber optical ports are in Multimode (0 to 550M, 850 nm with 50/125 μm , 62.5/125 μm fiber) and Singlemode with LC connector. Always connect the TX port of Switch A to the RX port of Switch B.

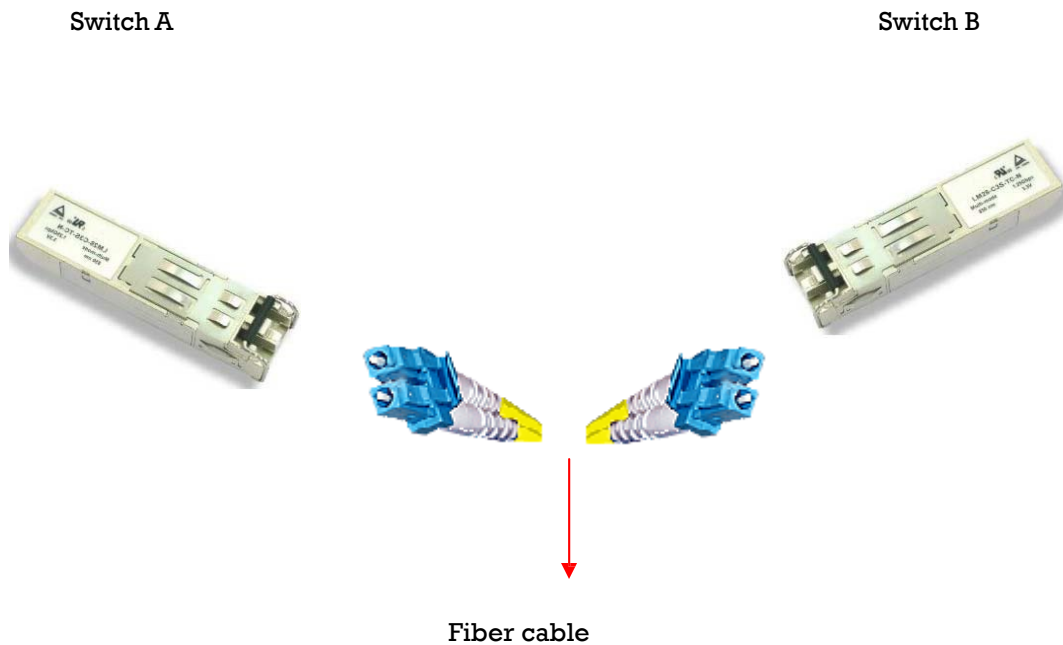


Figure 9 - Connection between TX port (Switch A) and RX port (Switch B)

3.3.3 iRing/iChain

3.3.3.1 iRing

Three or more switches can be connected to form a ring topology with network redundancy capabilities by following the steps below.

1. Connect each switch to form a daisy chain using an Ethernet or fiber optic cable.
2. Set one of the connected switches to be the master and make sure the port setting of each connected switch on the management page corresponds to the physical ports connected. For information about the port setting, refer to Section 5.4.1 iRing Configuration.
3. Connect the last switch to the first switch to form a ring topology.

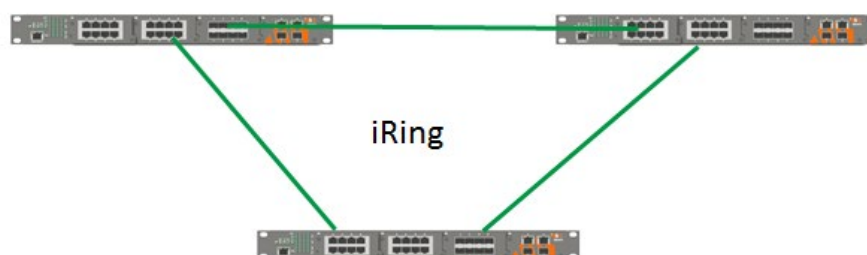


Figure 10 - Ring Topology

3.3.3.2 Coupling Ring

If two iRing topologies exist and you would like to connect the rings, a coupling ring can be formed. Select two switches from each ring to be connected, for example, switch A and B from Ring 1 and switch C and D from Ring 2, then decide which port on each switch will be used as the coupling ports and then link them together. For example, port 1 of switch A to port 2 of switch C and port 1 of switch B to port 2 of switch D. Then, enable Coupling Ring on the management page and select the coupling ring in correspondence to the connected port. For more information on port setting, please refer to Section 5.4.1 iRing Configuration. Once the setting is completed, one of the connections will act as the main path, while the other will act as the backup path.

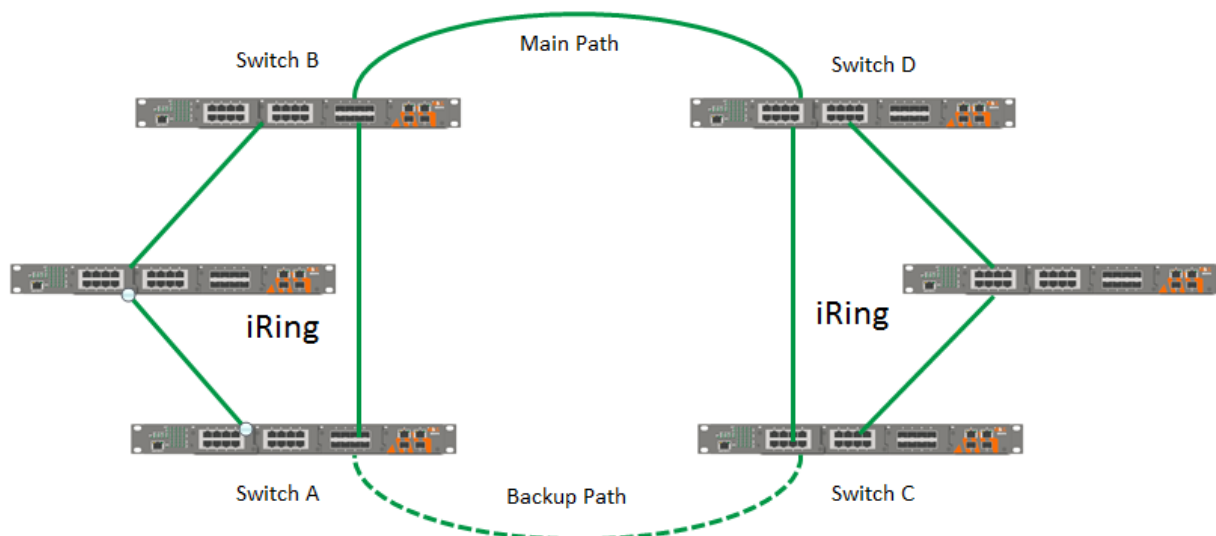


Figure 11 - Coupling Ring

3.3.3.3 Dual Homing

Dual Homing is used to connect a ring topology to a RSTP network environment. Choose the two switches (Switch A & B) from the ring to connect the switches in the RSTP network (backbone switches). The connection of one of the switches (Switch A or B) will act as the primary path, while the other will act as the backup path when the primary path connection fails.

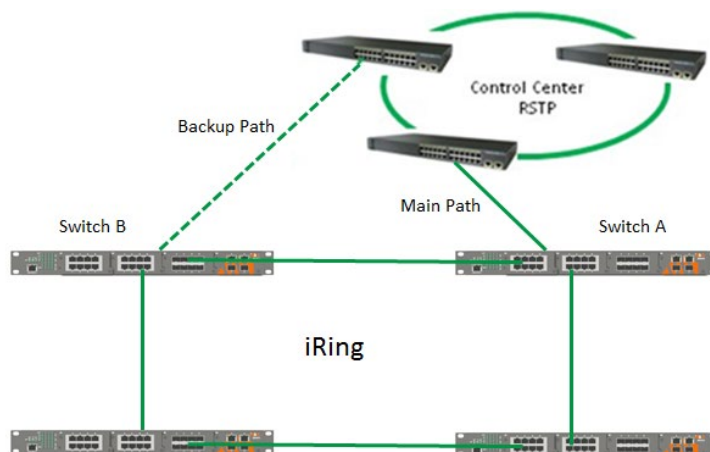


Figure 12 - Dual Homing

3.3.3.4 iChain

By connecting multiple iRings to meet expansion demands, an iChain topology can be created following the steps below:

1. Select two switches from the chain (Switch A & B) that you want to connect to the iRing and connect them to the switches in the ring (Switch C & D).
2. In correspondence to the ports connected to the ring, configure an edge port for both connected switches in the chain by checking the box in the iChain management page (see Section 5.4.2 iChain).
3. Once the setting is completed, one of the connections will act as the main path, and the other as the backup path.

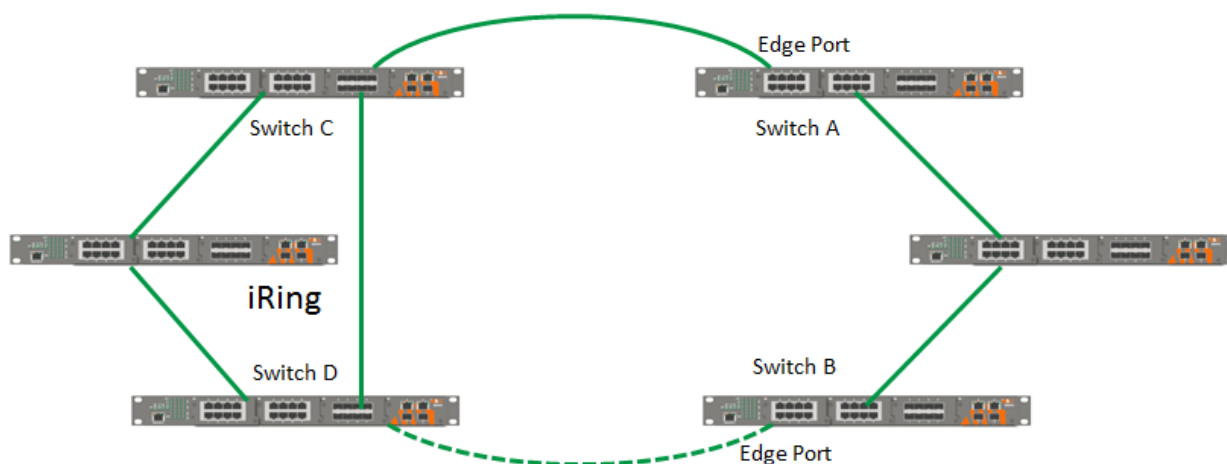


Figure 13 - iChain Topology

4. Redundancy

Use of redundancy for minimizing system downtime is one of the most important concerns for industrial networking devices. iRing and iBridge, two iS5Co's proprietary redundant ring technologies, feature faster recovery times compared to the existing redundancy technologies widely used in commercial applications, such as STP, RSTP, and MSTP. These redundancy technologies not only support different networking topologies, but also assure the reliability of the network.

4.1 iRing Introduction

iRing is an iS5Co's proprietary redundant ring technology, with recovery times of less than 30 milliseconds (in full-duplex Gigabit operation) or 10 milliseconds (in full-duplex Fast Ethernet operation) with up to 250 nodes. The ring protocols identify one switch as the master of the network, and then automatically block packets from traveling through any of the network's redundant loops. If one branch of the ring gets disconnected from the rest of the network, the protocol automatically re-adjusts the ring so that the part of the network that was disconnected may re-establish contact with the rest of the network. The iRing redundant ring technology can protect mission-critical applications from network interruptions or temporary malfunction with its fast recover technology.

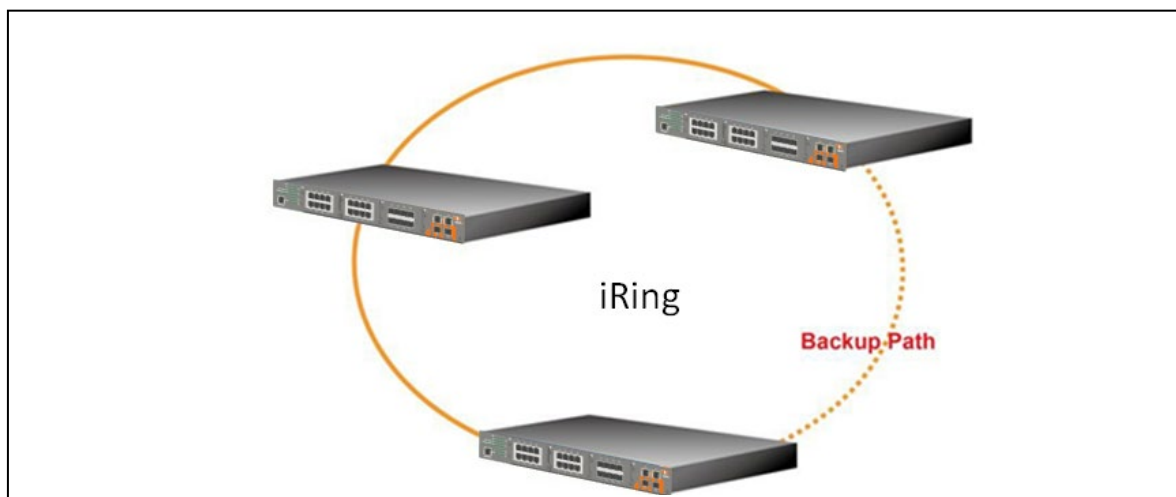


Figure 14 - iRing Topology

For details on iRing Configuration, see Section 5.4.1 iRing Configuration.

4.2 iChain Introduction

iChain is a revolutionary network redundancy technology which enhances network redundancy for any backbone network, providing ease-of-use and maximum fault-recovery times, flexibility, compatibility, and cost-effectiveness. The self-healing Ethernet technology designed for distributed and complex industrial networks enables the network to recover in less than 30 milliseconds (in full-duplex Gigabit operation) or 10 milliseconds (in full-duplex Fast Ethernet operation) for up to 250 switches if at any time a segment of the chain fails.

iChain allows multiple redundant rings of different redundancy protocols to interoperate together as a large robust network topology. It can create multiple redundant networks beyond the limitations of current redundant ring technologies.

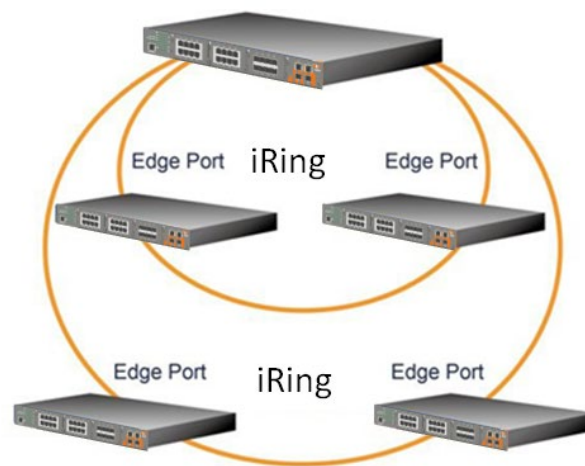


Figure 15 - iChain Topology iBridge

For details on iChain Configuration, go to Section 5.4.2 iBridge.

4.3 STP/RSTP/MSTP

4.3.1 STP/RSTP Introduction

STP (Spanning Tree Protocol), its advanced versions RSTP (Rapid Spanning Tree Protocol) and MSTP (Multiple Spanning Tree Protocol), are designed to prevent network loops and provide network redundancy. Network loops occur frequently in large networks when two or more paths run to the same destination, broadcast packets could get in to an infinite loop and cause congestion in the network. STP can identify the best path to the destination and block all other paths. The blocked links will stay connected but inactive. When the best path fails, the blocked links will be activated. Compared to STP which recovers a link in 30 to 50 seconds, RSTP can shorten the time to 5 to 6 seconds.

For details on RSTP, see Section 5.4.4 RSTP.

4.3.2 MSTP Introduction

MSTP was developed to improve recovery times since STP and RSTP takes seconds, which is not acceptable in some industrial applications. MSTP supports multiple spanning trees within a network by grouping and mapping multiple VLAN's into different spanning-tree instances, known as MSTI's, forming individual MST regions. Each switch is assigned an MST region. Each MST region consists of one or more MSTP switches with the same VLAN's, at least one MST instance, and the same MST region name. This allows the switches to use different paths in the network to effectively balance loads.

4.4 MRP Introduction


MRP (Media Redundancy Protocol) is an industry standard for high-availability Ethernet networks. MRP allows Ethernet switches in ring configuration to recover from failure rapidly to ensure seamless data transmission. A MRP ring (IEC 62439) can support up to 50 devices and will enable a back-up link in 80ms (adjustable to max. 200ms/500ms).

4.5 Fast Recovery Introduction

Fast recovery mode can be set to connect multiple ports to one or more switches providing redundant links. Fast recovery mode supports 12 priorities. Only the first priority will be active port, the other ports with different priorities will be backup ports.

. For details on Fast Recovery, see Section 5.4.6 Fast Recovery.

5. MANAGEMENT



Warning!!!

Prior to upgrading the firmware, remove any physical loop connections.

DO NOT power off the unit during a firmware upgrade.

This section introduces configuration of the iES26GF switch by Web browser.

An embedded HTML web site resides in the flash memory of the CPU board. It contains advanced management features that allow the user to manage the iES26GF switch from anywhere on the network via a standard web browser such as Microsoft Internet Explorer.

The Web-Based Management function supports Internet Explorer 5.0 or later. It is based on Java Applets with an aim at reducing network bandwidth consumption and enhances access speed in a viewing screen.

Note: By default, IE5.0 or later versions do not allow Java Applets to open sockets. The browser settings need to be explicitly modified to enable Java Applets for use on network ports.

The default values are as below:

- IP Address: **192.168.10.1**
- Subnet Mask: **255.255.255.0**
- Default Gateway: **192.168.10.254**
- User Name: **admin**
- Password: **admin**

For System Login, perform the following:

1. Launch the Internet Explorer.
2. Type `http://` and the switch's IP address (default is 192.168.10.1), then press **Enter**.
3. The login screen appears (see Figure 16).
4. Enter username and password. The default username and password are "admin".
5. Click **OK**. Then the main interface of the Web-based management appears (see Figure 17).

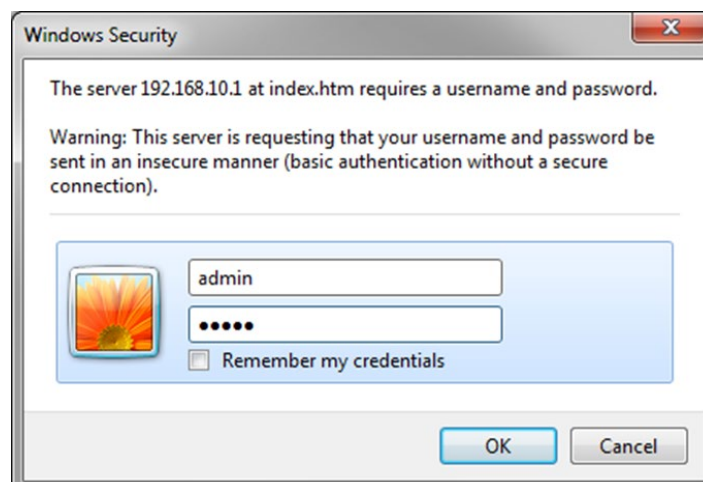


Figure 16 - Login screen

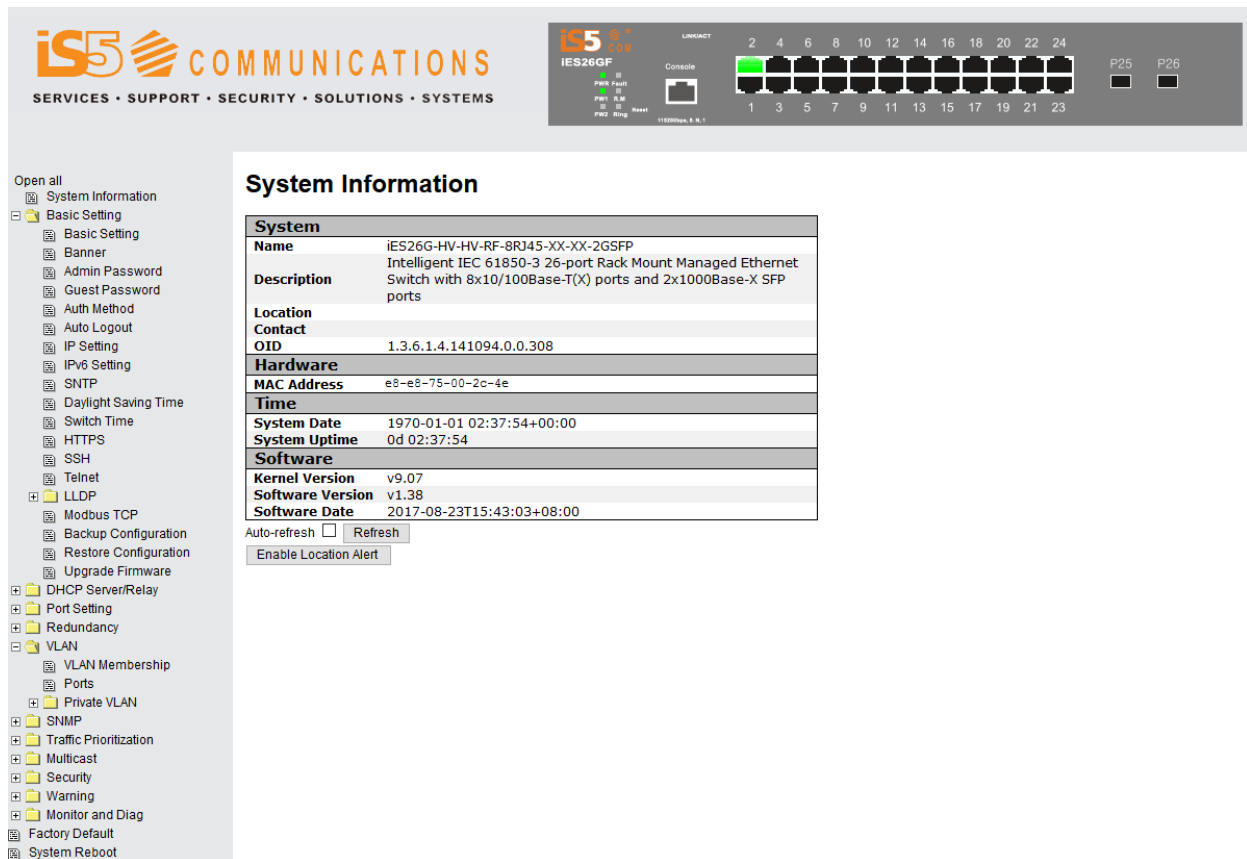


Figure 17 – Main Interface

5.1 Basic Settings

5.1.1 System Information Configuration

System Information Configuration

System Name	
System Description	
System Location	
System Contact	
System Timezone Offset (minutes)	

Save Reset

Figure 18 – System Information Configuration interface

The system information will display the configuration of Basic/Switch Setting page.

The following table describes the labels for the **System Information Configuration** screen.

Label	Description
System Name	An administratively assigned name for the managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string consisting of alphabets (A-Z, a-z), digits (0-9), and minus sign (-). Space is not allowed to be part of the name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
System Description	Description of the device
System Location	The physical location of the node (e.g., telephone closet, 3 rd floor). The allowed string length is 0 to 255, and only ASCII characters from 32 to 126 are allowed.
System Contact	The textual identification of the contact person for this managed node, together with information on how to contact this person. The allowed string length is 0 to 255, and only ASCII characters from 32 to 126 are allowed.
System Time zone offset (minutes)	Provides the time-zone offset from UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.1.2 Banner

System Banner Configuration

System Banner Title	Title
System Banner Messages	Messages

Save Reset

Figure 19 – System Banner Configuration interface

The following table describes the labels for the **System Banner Configuration** screen.

Label	Description
System Banner Title	The title of the Login Banner. Note: restricted to 0 – 64 characters
System Banner Message	The Content of the Login Banner Message. Note: restricted to 0 – 512 characters
Save	Click to save changes.
Reset	Click to reset changes.

5.1.3 Admin Password

Admin Password allows the username and password for the Web Management login to be changed.

System Password

Username	admin
Old Password	
New Password	
Confirm New Password	

Save

Figure 20 - System Password interface

The following table describes the labels for the **System Password** screen.

Label	Description
User Name	Enter new username (the default is admin)
Old Password	The existing password. If this is incorrect, you cannot set the new password
New Password	Enter the new password (the default is admin). The allowed string length is 0 to 31, and only ASCII characters from 32 to 126 are allowed
Confirm Password	Re-type the new password.
Save	Click Save to save the changes.

5.1.4 Guest Password

This page allows you to configure the system guest password required to access the web interface or log in to the CLI.

Guest Password Configuration

Guest Name	guest
Old Password	
New Password	
Confirm New Password	

Save

Figure 21 - Guest Password Configuration interface

The following table describes the labels for the **Guest Password Configuration** screen.

Label	Description
Guest name	The Guest Name should be used. The default Guest Name is: <i>guest</i>
Old Password	The existing password. If this is incorrect, you cannot set the new password. The default Guest Name is: <i>guest</i>
New Password	The new system password. The allowed string length is 0 to 31, and only ASCII characters from 32 to 126 are allowed.
Confirm New Password	Re-type the new password.
Save	Click to save changes.

5.1.5 Authentication Method

Configure how a user is authenticated when he/she logs into the switch via one of the management interfaces.

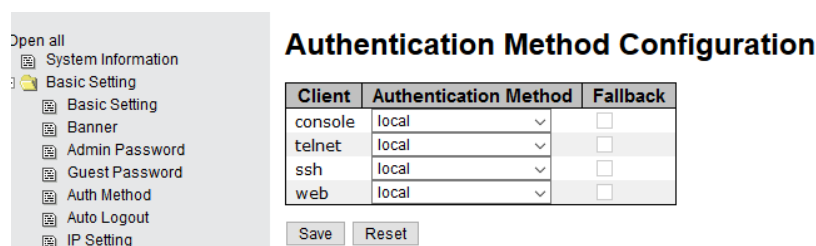


Figure 22 - Authentication Method Configuration interface

The following table describes the labels for the **Authentication Method Configuration** screen.

Label	Description
Client	The management Client for which the configuration below applies.
Authentication Method	Authentication Method can be set to one of the following values: none : authentication is disabled and login is not possible. local : local user database on the switch is used for authentication. RADIUS : a remote RADIUS server is used for authentication.
Fallback	Add a check mark if you want to activate this option.
Save	Click Save to save changes
Reset	Click Reset to undo any changes made locally and revert to previously saved values

5.1.6 Auto Logout

You can define automatic logout time for WebUI and for CLI access.

Auto Logout Configuration

Web Auto-Logout Timer (minutes)	0
CLI Auto-Logout Timer (minutes)	0

Save Reset

Figure 23 - Auto Logout Configuration interface

The following table describes the labels for the **Auto Logout Configuration** screen.

Label	Description
Web Auto-Logout Timer (minutes)	Define the auto logout time for WebUI access Note: values are 0-9999 min; default: 0 means 10 min
CLI Auto-Logout Timer (minutes)	Define the auto logout time for CLI access Note: values are 0-9999 min; default: 0 means 10 min
Save	Click Save to save changes
Reset	Click Reset to undo any changes made.

5.1.7 IP Setting

You can configure the IP Settings and DHCP client function through IP Configuration screen.

IP Configuration

	Configured	Current
DHCP Client	<input type="checkbox"/>	<input type="button" value="Renew"/>
IP Address	192.168.10.1	192.168.10.1
IP Mask	255.255.255.0	255.255.255.0
IP Router	0.0.0.0	0.0.0.0
VLAN ID	1	1

Figure 24 - IP Configuration interface

The following table describes the labels for the **IP Configuration** screen.

Label	Description
DHCP Client	Enables or disables DHCP Client function. When the DHCP Client function is enabled, an IP address from the network DHCP server will be assigned to the switch.
IP Address	Assigns the IP Address that the network is using. If the DHCP client function is enabled, you do not need to assign an IP Address. The network DHCP server will assign the IP Address for the switch and it will be displayed in this column. The default IP Address is 192.168.10.1.
IP Mask	Assigns IP Mask . If the DHCP client function is enabled, you do not need to assign an IP Mask . The default is 255.255.255.0.
IP Router	Assigns IP Router . If the DHCP client function is enabled, you do not need to assign an IP Router . The default is 0.0.0.0.
VLAN ID	Assigns VLAN ID . If the DHCP client function is enabled, you do not need to assign an VLAN ID . The default is 1.
Save	Click Save to save changes
Reset	Click Reset to undo any changes made.

5.1.8 IPv6 Configuration

IPv6 Configuration

	Configured	Current
Auto Configuration	<input type="checkbox"/>	<input type="button" value="Renew"/>
Address	::192.0.2.1	::192.0.2.1 Link-Local Address: fe80::eae8:75ff:fe00:2c4e
Prefix	96	96
Router	::	::
SNTP Server1	::	::
SNTP Server2	::	::

Figure 25 - IPv6 Configuration interface

The following table describes the labels for the **IPv6 Configuration** screen.

Label	Description
Auto Configuration	Add a checkmark in Configured to enable Auto Configuration .
Address	Enter a IPv6 Address . The default is 192.0.2.1
Prefix	Enter Prefix .
Router	Enter Router .
Save	Click Save to save changes
Reset	Click Reset to undo any changes made.

5.1.9 SNTP Configuration (only for SNTP Version)

The Simple Network Time Protocol (SNTP) settings allow you to synchronize switch clocks over the Internet. Configure the SNTP on the following page.

IP Configuration

Mode	Disabled ▾
SNTP Server1	0.0.0.0
SNTP Server2	0.0.0.0

Figure 26 - IP Configuration interface

The following table describes the labels for the **IP Configuration** screen.

Label	Description
Mode	Enables or disables the SNTP function. When enabled the switch gets the time from the SNTP server. The modes include: Enabled: Enables SNTP client mode operation. Disabled: Disables SNTP client mode operation.
SNTP Server 1	Enter the IPv6 address of a SNTP Server 1 .
SNTP Server 2	Enter the IPv6 address of a SNTP Server 1 .
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made.

5.1.10 NTP Configuration (only for NTP Version)

Configure NTP on this page.

NTP Configuration

Mode	Disabled ▾
Server 1	0.0.0.0
Server 2	
Server 3	
Server 4	
Server 5	

Figure 27 - NTP Configuration

Label	Description
Mode	Indicates the selected Network Time Protocol (NTP) mode. The modes include: Enabled: Enable NTP client mode operation. Disabled: Disable NTP client mode operation.
Server Address	Provide the IPv4 address of a NTP server. There 2 cells so a dual NTP server or active / active model is supported.
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved

5.1.11 Daylight Saving Time

This page allows you to configure the Time Zone.

Time Zone Configuration

Time Zone Configuration	
Time Zone	None
Acronym	(0 - 16 characters)

Daylight Saving Time Configuration

Daylight Saving Time Mode	
Daylight Saving Time	Disabled

Start Time settings	
Month	Jan
Date	1
Year	2000
Hours	0
Minutes	0

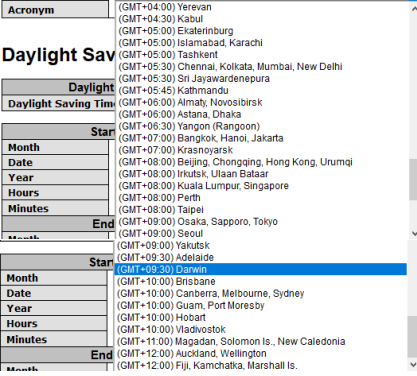
End Time settings	
Month	Jan
Date	1
Year	2000
Hours	0
Minutes	0

Offset settings	
Offset	1 (1 - 1440) Minutes

Figure 28 - Time Zone Configuration interface

The following table describes the labels for the **Time Zone Configuration** screen.

Label	Description
Time Zone	<p>Lists various time zones worldwide. Select appropriate Time Zone from the drop-down list and click Save to set it up.</p>

	
Acronym	The user can set the Acronym of the time zone. This is a User configurable acronym to identify the time zone. (Range: Up to 16 characters)
Daylight Savings Time Mode	<p>This is used to set the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration. Selections include:</p> <p>Disable: disables the Daylight Saving Time configuration. (Default)</p> <p>Recurring: The Daylight Saving Time duration configuration will be repeated every year.</p> <p>Non-Recurring: The Daylight Saving Time duration configuration will be used once.</p>
Start Time Settings	<ul style="list-style-type: none"> • Week - Select the starting week number. (Recurring) • Day - Select the starting day. (Recurring) • Month - Select the starting month. • Date - Select the starting date. (Non-Recurring) • Year - Select the starting year. (Non-Recurring) • Hours - Select the starting hour. • Minutes - Select the starting minute.
End Time Settings	<ul style="list-style-type: none"> • Week - Select the ending week number. (Recurring) • Day - Select the ending day. (Recurring) • Month - Select the ending month. • Date - Select the ending date. (Non-Recurring) • Year - Select the ending year. (Non-Recurring) • Hours - Select the ending hour.
Offset Settings	Enter the number of minutes to add during Daylight Saving Time. (Range is from 1 to 1440)
Save	Click Save to save changes
Reset	Click Reset to undo any changes made locally and revert to previously saved values

Local Time Zone	Conversion from UTC	Time at 12:00 UTC
November Time Zone	- 1 hour	11 am
Oscar Time Zone	-2 hours	10 am
ADT - Atlantic Daylight	-3 hours	9 am
AST - Atlantic Standard EDT - Eastern Daylight	-4 hours	8 am
EST - Eastern Standard CDT - Central Daylight	-5 hours	7 am
CST - Central Standard MDT - Mountain Daylight	-6 hours	6 am
MST - Mountain Standard PDT - Pacific Daylight	-7 hours	5 am
PST - Pacific Standard ADT - Alaskan Daylight	-8 hours	4 am
ALA - Alaskan Standard	-9 hours	3 am
HAW - Hawaiian Standard	-10 hours	2 am
Nome, Alaska	-11 hours	1 am
CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	+1 hour	1 pm
EET - Eastern European, Zone 1	+2 hours	2 pm
BT - Baghdad, Zone 2	+3 hours	3 pm
ZP4 - Zone 3	+4 hours	4 pm
ZP5 - Zone 4	+5 hours	5 pm
ZP6 - Zone 5	+6 hours	6 pm
WAST - West Australian Standard	+7 hours	7 pm
CCT - China Coast, Zone 7	+8 hours	8 pm
JST - Japan Standard, Zone 8	+9 hours	9 pm
EAST - East Australian Standard GST Guam Standard, Zone 9	+10 hours	10 pm
IDLE - International Date Line NZST - New Zealand Standard NZT - New Zealand	+12 hours	Midnight

5.1.12 Switch Time

Configure date and time on this page.

Switch Time Configuration

Current Date	1970	-	1	-	1
Current Time	4	:	27	:	12

Figure 29 - Switch Time Configuration interface

The following table describes the labels for the **Switch Time Configuration** screen.

Mode	Description
Current Date	Modify Current Date in the following order according to your preference: Year – Month - Day
Current Time	Modify Current Time in the following order according to your preference: Hour: Minutes: Seconds
Save	Click Save to save changes
Reset	Click Reset to undo any changes made locally and revert to previous saved values

5.1.13 HTTPS Configuration

Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP. Select **HTTPS Configuration Mode** on this page.

HTTPS Configuration

Mode Disabled ▾

Figure 30 - HTTPS Configuration interface

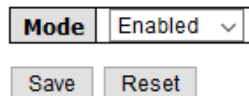
The following table describes the labels for the **HTTPS Configuration** screen.

Label	Description
Mode	Choose a HTTPS mode from the drop-down list. When the current connection is HTTPS, disabling HTTPS will automatically redirect the web browser to an HTTP connection. The modes include: Enabled: enables HTTPS. Disabled: disables HTTPS.
Save	Click Save to save changes
Reset	Click Reset to undo any changes made locally and revert to previously saved values

5.1.14 SSH

Secure Shell (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. Select **SSH Configuration Mode** on this page.

SSH Configuration



The image shows a configuration interface for SSH. It features a label 'Mode' followed by a dropdown menu currently displaying 'Enabled'. Below this are two buttons: 'Save' and 'Reset'.

Figure 31 - SSH Configuration interface

The following table describes the labels for the **SSH Configuration** screen.

Label	Description
Mode	Choose a SSH mode from the drop-down list. The modes include: Enabled: enables SSH. Disabled: disables SSH.
Save	Click Save to save changes
Reset	Click Reset to undo any changes made locally and revert to previously saved values

5.1.15 Telnet

Select **Telnet Configuration Mode** on this page.

Telnet Configuration



The image shows a configuration interface for Telnet. It features a label 'Mode' followed by a dropdown menu currently displaying 'Disabled'. Below this are two buttons: 'Save' and 'Reset'.

Figure 32 - Telnet Configuration interface

The following table describes the labels for the **Telnet Configuration** screen.

Label	Description
Mode	Choose a Telnet mode from the drop-down list. The modes include: Enabled: enables Telnet. Disabled: disables Telnet.
Save	Click Save to save changes
Reset	Click Reset to undo any changes made locally and revert to previously saved values

5.1.16 LLDP

LLDP (Link Layer Discovery Protocol) function allows the switch to advertise its identity, abilities, and neighbours to other nodes on the network and store the discovered information. Select **LLDP Configuration**, **LLDP Neighbour Information**, and **Port Statistics** on the following pages.

5.1.16.1 LLDP Configuration

LLDP Configuration

LLDP Parameters

Tx Interval 30 seconds

LLDP Port Configuration

Port	Mode
*	<> ▾
1	Enabled ▾
2	Enabled ▾
3	Enabled ▾
4	Enabled ▾
5	Enabled ▾
6	Enabled ▾
7	Enabled ▾
8	Enabled ▾
9	Enabled ▾
10	Enabled ▾
11	Enabled ▾
12	Enabled ▾
13	Enabled ▾
14	Enabled ▾
15	Enabled ▾
16	Enabled ▾
17	Enabled ▾
18	Enabled ▾
19	Enabled ▾
20	Enabled ▾
21	Enabled ▾
22	Enabled ▾
23	Enabled ▾
24	Enabled ▾
25	Enabled ▾
26	Enabled ▾

Save Reset

Figure 33 - LLDP Configuration interface

The following table describes the labels for the **LLDP Configuration** screen.

Label	Description
Tx Interval	Enter value for the Tx Interval . The default is 30 seconds.
Mode	Select from the drop-down list a mode for every LLDP Port. The following modes are available: Disabled: the switch will not send out LLDP information, and will drop LLDP information received from its neighbors. Enabled: the switch will send out LLDP information, and will analyze LLDP information received from its neighbors.
Save	Click Save to save changes
Reset	Click Reset to undo any changes made locally and revert to previously

5.1.16.2 Neighbours

This page provides a status overview for all LLDP neighbors. The following table contains information for each port on which an LLDP neighbor is detected.

LLDP Neighbour Information

Auto-refresh ☐ Refresh

Local Port	Chassis ID	Remote Port ID	System Name	Port Description	System Capabilities	Management Address
Port 2	54-E1-AD-07-0D-87	54-E1-AD-07-0D-87				

Figure 34 - LLDP Neighbour Information

The following table describes the columns for the **LLDP Neighbour** screen.

Label	Description
Local Port	The port used to transmit and receive LLDP frames.
Chassis ID	The identification number of the neighbor sending out the LLDP frames.
Remote Port ID	The identification of the neighbour port
Port Description	The description of the port advertised by the neighbour.
System Name	The name advertised by the neighbour.
System Capabilities	<p>Description of the neighbor's capabilities. The capabilities include:</p> <ul style="list-style-type: none"> • Other • Repeater • Bridge • WLAN Access Point • Router • Telephone • DOCSIS Cable Device • Station Only • Reserved <p>When a capability is enabled, a (+) will be displayed. If the capability is disabled, a (-) will be displayed.</p>
Management Address	The neighbour's address which can be used to help network management. This may contain the neighbour's IP address.
Refresh	Click to refresh the page immediately
Auto-refresh	Check to enable an automatic refresh of the page at regular Intervals

5.1.16.3 LLDP Global Counters

This page provides an overview of all LLDP traffic. Two types of counters are shown. Global counters will apply settings to the whole switch stack, while local counters will apply settings to specified switches.

Auto-refresh ☐

LLDP Global Counters

Global Counters	
Neighbour entries were last changed	1970-01-01 02:32:11+00:00 (10629 secs. ago)
Total Neighbours Entries Added	1
Total Neighbours Entries Deleted	0
Total Neighbours Entries Dropped	0
Total Neighbours Entries Aged Out	0

LLDP Statistics Local Counters

Local Port	Tx Frames	Rx Frames	Rx Errors	Frames Discarded	TLVs Discarded	TLVs Unrecognized	Org. Discarded	Age-Outs
1	0	0	0	0	0	0	0	0
2	354	13	0	0	0	0	26	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
11	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0

Figure 35 - LLDP Global Counters interface

The following table describes the labels for the **LLDP Global Counters** screen

Label	Description
Neighbour entries were last changed at	Shows the time when the last entry was deleted or added.
Total Neighbours Entries Added	Shows the number of new entries added since switch reboot
Total Neighbours Entries Deleted	Shows the number of new entries deleted since switch reboot
Total Neighbours Entries Dropped	Shows the number of LLDP frames dropped due to full entry table
Total Neighbours Entries Aged Out	Shows the number of entries deleted due to expired time-to-live

The following table describes the columns for the **LLDP Statistics Local Counters** screen.

Label	Description
Local Port	The port that receives or transmits LLDP frames
Tx Frames	The number of LLDP frames transmitted on the Local Port
Rx Frames	The number of LLDP frames received on the Local Port
Rx Errors	The number of received LLDP frames containing errors
Frames Discarded	If a port receives an LLDP frame, and the switch's internal table is full, the LLDP frame will be counted and discarded. In the LLDP standard, this situation is known as "too many neighbors". LLDP frames require a new entry in the table if Chassis ID or Remote Port ID is not included in the table. Entries are removed from the table when a given port links down, a LLDP shutdown frame is received, or when the entry ages out.
TLVs Discarded	Each LLDP frame can contain multiple pieces of information, known as TLVs (Type Length Value). If a TLV is malformed, it will be counted and discarded.
TLVs Unrecognized	The number of well-formed TLVs, but with an unknown type value
Org. Discarded	The number of TLVs received organizationally
Age-Outs	Each LLDP frame contains information about how long the LLDP information is valid (age-out time). If no new LLDP frame is received during the age-out time, the LLDP information will be removed, and the value of the age-out counter will be incremented.
Refresh	Click Refresh to refresh the page immediately.
Clear	Click Clear to clear the local counters. All counters (including global counters) are cleared upon reboot.
Auto-refresh	Check Auto-refresh to enable an automatic refresh of the page at regular intervals

5.1.17 MODBUS TCP



Figure 36 - MODBUS Configuration Interface

The following table describes the columns for the **MODBUS Configuration** screen.

Label	Description
Mode	Shows the existing status of the Modbus TCP function
Save	Click Save to save changes
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

Note: For Modbus commands, see [Appendix A](#).

5.1.18 Backup & Restore Configuration

The user can save current EEPROM values for the switch to the TFTP server or restore them from the TFTP configuration page. A local PC can be used instead of a TFTP server.

Configuration Save

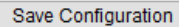
A screenshot of the 'Configuration Save' interface. It features a single button labeled 'Save Configuration'.

Figure 37 - Configuration Save Interface

Configuration Upload

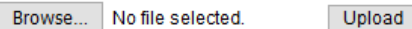
A screenshot of the 'Configuration Upload' interface. It contains three elements: a 'Browse...' button, a text label 'No file selected.', and an 'Upload' button.

Figure 38 - Configuration Upload interface

5.1.19 Upgrade Firmware

This page allows you to update the firmware of the switch. Click **Browse** and select the file to be uploaded, then click **Upload**. After the software image is uploaded, a page announces that the firmware update is initiated. After about a minute, the firmware is updated and .

Software Upload

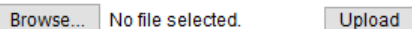
A screenshot of the 'Software Upload' interface. It contains three elements: a 'Browse...' button, a text label 'No file selected.', and an 'Upload' button.

Figure 39 - Upgrade Firmware interface

5.2 DHCP Server/Relay

The switch provides Dynamic Host Configuration Protocol (DHCP) server functions. By enabling DHCP, the switch will become a DHCP server and will assign dynamically IP addresses and related configuration information such as subnet mask and default gateway to network clients.

5.2.1 Setting

This page allows you to set up DHCP settings for the switch. You can check the **Enabled** checkbox to activate the function. Once the box is checked, input information in each column.

DHCP Server Configuration

Enabled	<input type="checkbox"/>
Start IP Address	192.168.10.100
End IP Address	192.168.10.200
Subnet Mask	255.255.255.0
Router	192.168.10.254
DNS	192.168.10.254
Lease Time (sec.)	86400
TFTP Server	0.0.0.0
Boot File Name	

Save Reset

Figure 40 - DHCP Server Configuration interface

The following table describes the labels for the **DHCP Server Configuration** screen.

Label	Description
Enabled	Select Enabled to enable the DHCP server.
Start IP Address	The first IP address of IP pool
End IP Address	The Last IP address of IP pool
Subnet Mask	The Subnet Mask
Router	The IP address of the gateway
DNS	The IP address of the Domain Name Server (DNS)
Lease Time	Lease Time counted in seconds
TFTP Server	The IP address of the TFTP Server (Option 66).
Boot File Name	The name of Boot File (Option 67).
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.2.2 DHCP Dynamic Client List

When DHCP server functions are activated in the **DHCP Server Configuration** dialog box, the switch will collect DHCP client information and display it in the following table.

DHCP Dynamic Client List

No.	Select	Type	MAC Address	IP Address	Surplus Lease
<div> <input type="button" value="Select/Clear All"/> <input type="button" value="Add to static Table"/> </div>					

Figure 41 - DHCP Dynamic Client List interface

The following table describes the columns and labels for the **DHCP Dynamic Client List** screen.

Label	Description
No	Number of client
Select	To add to static table
Type	The Type of client (Dynamic or Static)
MAC Address	The MAC Address of client
IP Address	The IP Address of client
Surplus Lease	The Surplus Lease time
Select/Clear All	Select or Clear All check boxes.
Add to Static Table	Adds a dynamic entry to static table.

5.2.3 DHCP Static Client List

You can assign a specific IP address (dependent upon each client's MAC address) within the dynamic IP range to a specific port. When a device is connected to the port and requests for dynamic IP assigning, the switch will assign the IP address that has previously been assigned to the connected device.

DHCP Client List

MAC Address	<input type="text"/>				
IP Address	<input type="text"/>				
<input type="button" value="Add as Static"/>					
No.	Select	Type	MAC Address	IP Address	Surplus Lease
<div> <input type="button" value="Delete"/> <input type="button" value="Select/Clear All"/> </div>					

Figure 42 - DHCP Client List

The following table describes the columns and labels for the **DHCP Client List** screen.

Label	Description
MAC Address	Enter the MAC address to be added to the Static Client List.
IP Address	Enter the MAC address to be added to the Static Client List.
Add as Static	Add new entry to static table.
Type	The Type of client (Dynamic or Static)
MAC Address	The MAC Address of client
IP Address	The IP Address of client
Surplus Lease	The Surplus Lease time
Delete	Click Delete to remove the selected entry.
Select/Clear All	Select or Clear All check boxes.

5.2.4 DHCP Relay Agent

When DHCP relay agent is enabled, the relay agent forwards and transfers DHCP messages (packets) between clients and the server when they are not in the same subnet domain, to prevent the DHCP broadcast message from flooding for security considerations. You can configure this function on the following page.

5.2.4.1 Relay

DHCP Relay Configuration

Relay Mode	Disabled ▼
Relay Server	0.0.0.0
Relay Information Mode	Enabled ▼
Relay Information Policy	Replace ▼

Figure 43 - DHCP Relay Configuration interface

The following table describes the columns and labels for the **DHCP Relay Configuration** screen.

Label	Description
Relay Mode	Indicates the existing DHCP Relay Agent Mode. The modes include: <ul style="list-style-type: none"> • Enabled: activates DHCP relay. • Disabled: disables DHCP relay
Relay Server	Indicates the DHCP Relay Server IP address. A DHCP relay agent is used to forward and transfer DHCP messages between the client and the server when they are not in the same subnet domain.
Relay Information Mode	Indicates the existing DHCP's Relay Information Mode . The format of DHCP option 82 circuit ID is "[vlan_id] [module_id] [port_no]". The first four characters represent the VLAN ID, the fifth and sixth characters are the module ID. In stand-alone devices, the module ID always equals to 0; in stacked devices, it means switch ID. The last two characters are the port number. For example, "00030108" means the DHCP message received from VLAN ID 3, switch ID 1, and port No. 8. The option 82 remote ID value equals to the switch MAC address. The Relay Information Modes include: <ul style="list-style-type: none"> • Enabled: activates DHCP relay information. When DHCP relay information is enabled, the agent inserts specific information (option 82) into a DHCP message when forwarding to a DHCP server, and it removes it from a DHCP message when transferring to a DHCP client. This only works when the DHCP relay mode is enabled. • Disabled: disable DHCP relay information
Relay Information Policy	Indicates the policies to be enforced when receiving DHCP relay information. When DHCP relay information mode is enabled, if the agent receives a DHCP message that already contains relay agent information, it will enforce the policy. The Replace option is invalid when relay information mode is disabled. The Relay Information Policy options shown on drop-down list include: <ul style="list-style-type: none"> • Replace: replaces the original relay information when a DHCP message containing the information is received. • Keep: keeps the original relay information when a DHCP message containing the information is received. • Drop: drops the package when a DHCP message containing the information is received.
Save	Click Save to save the selected DHCP Relay Configuration.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.2.4.2 Relay Statistics

The **Relay Statistics** shows the information of the relayed packet of the switch.

Auto-refresh ☐ Refresh Clear

DHCP Relay Statistics

Server Statistics

Transmit to Server	Transmit Error	Receive from Server	Receive Missing Agent Option	Receive Missing Circuit ID	Receive Missing Remote ID	Receive Bad Circuit ID	Receive Bad Remote ID
0	0	0	0	0	0	0	0

Figure 44 - DHCP Relay Statistics interface (Server Statistics)

The following table describes the columns and labels for the **DHCP Relay Statistics** screen.

Label	Description
Transmit to Server	The number of packets relayed from the client to the server
Transmit Error	The number of packets with errors when being sent to clients
Receive from Server	The number of packets received from the server
Receive Missing Agent Option	The number of packets received without agent information
Receive Missing Circuit ID	The number of packets received with Circuit ID
Receive Missing Remote ID	The number of packets received with the Remote ID option missing.
Receive Bad Circuit ID	The number of packets whose Circuit IDs do not match the known circuit ID
Receive Bad Remote ID	The number of packets whose Remote IDs do not match the known Remote ID

Client Statistics

Transmit to Client	Transmit Error	Receive from Client	Receive Agent Option	Replace Agent Option	Keep Agent Option	Drop Agent Option
0	0	0	0	0	0	0

Figure 45 - DHCP Relay Statistics interface (Client Statistics)

The following table describes the columns and labels for the **Client Statistics** screen.

Label	Description
Transmit to Client	The number of packets relayed from the server to the client
Transmit Error	The number of packets with errors when being sent to servers
Receive from Client	The number of packets received from the server
Receive Agent Option	The number of received packets containing relay agent information
Replace Agent Option	The number of packets replaced when received messages contain relay agent information.
Keep Agent Option	The number of packets whose relay agent information is retained
Drop Agent Option	The number of packets dropped when received messages contain relay agent information.
Refresh	Click Refresh to refresh the page immediately
Auto-refresh	Check Auto-refresh to enable an automatic refresh of the page at regular intervals
Clear	Click Clear to remove the changes to the configuration.

5.3 Port Setting

5.3.1 Port Control

By this function, you can set the state, negotiation, speed/duplex, flow control, and security for the port. Port Setting allows you to manage individual ports of the switch, including traffic, power, and trunks. This page shows current port configurations. Ports can also be configured here.

Port Configuration

Port	Link	Speed		Flow Control			Maximum Frame Size	Power Control
		Current	Configured	Current Rx	Current Tx	Configured		
*			<>				9600	<>
1	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
2	● 100fdx	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
3	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
4	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
5	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
6	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
7	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
8	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
9	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
10	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
11	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
12	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
13	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
14	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
15	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
16	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
17	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
18	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
19	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
20	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
21	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
22	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
23	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
24	● Down	Auto	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
25	● Down	1000-X_AMS	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼
26	● Down	1000-X_AMS	▼	×	×	<input type="checkbox"/>	9600	Disabled ▼

Figure 46 - Port Configuration interface

The following table describes the columns and labels for the **Port Configuration** screen.

Label	Description
Port	The switch port number to which the following settings will be applied.
Link	The current link state is shown by different colors. Green indicates the link is up and Red means the link is down.
Current Link Speed	Indicates the current link speed of the port
Configured Link Speed	The drop-down list provides available link speed options for a given switch port Auto selects the highest speed supported by the link partner Disabled disables switch port configuration
Flow Control	The Flow Control columns are Current Rx , Current Tx , and Configured .
Maximum Frame	You can enter the maximum frame size allowed for the switch port in this column, including FCS. The allowed range is 1518 bytes to 9600 bytes.
Refresh	Click Refresh to refresh the page immediately.
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

The following table describes the columns and labels for the **Aggregation Group Configuration** screen.

Label	Description
Group ID	Indicates the ID of each aggregation group. Normal means no aggregation. Only one group ID is valid per port.
Port Members	Lists each switch port for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and the ports must be in the same speed in each group.
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.3.2.2 LACP Port

This page allows you to enable LACP functions for grouping ports together to form single virtual links, thereby increasing the bandwidth between the switch and other LACP-compatible devices. LACP trunks are similar to static port trunks, but they are more flexible because LACP is compliant with the IEEE 802.3ad standard. Hence, it is interoperable with equipment from other vendors that also comply with the standard. You can change LACP port settings on this page.

LACP Port Configuration

Port	LACP Enabled	Key	Role
*	<input type="checkbox"/>	<> ▾	<> ▾
1	<input type="checkbox"/>	Auto ▾	Active ▾
2	<input type="checkbox"/>	Auto ▾	Active ▾
3	<input type="checkbox"/>	Auto ▾	Active ▾
4	<input type="checkbox"/>	Auto ▾	Active ▾
5	<input type="checkbox"/>	Auto ▾	Active ▾
6	<input type="checkbox"/>	Auto ▾	Active ▾
7	<input type="checkbox"/>	Auto ▾	Active ▾
8	<input type="checkbox"/>	Auto ▾	Active ▾
9	<input type="checkbox"/>	Auto ▾	Active ▾
10	<input type="checkbox"/>	Auto ▾	Active ▾
11	<input type="checkbox"/>	Auto ▾	Active ▾
12	<input type="checkbox"/>	Auto ▾	Active ▾
13	<input type="checkbox"/>	Auto ▾	Active ▾
14	<input type="checkbox"/>	Auto ▾	Active ▾
15	<input type="checkbox"/>	Auto ▾	Active ▾
16	<input type="checkbox"/>	Auto ▾	Active ▾
17	<input type="checkbox"/>	Auto ▾	Active ▾
18	<input type="checkbox"/>	Auto ▾	Active ▾
19	<input type="checkbox"/>	Auto ▾	Active ▾
20	<input type="checkbox"/>	Auto ▾	Active ▾
21	<input type="checkbox"/>	Auto ▾	Active ▾
22	<input type="checkbox"/>	Auto ▾	Active ▾
23	<input type="checkbox"/>	Auto ▾	Active ▾
24	<input type="checkbox"/>	Auto ▾	Active ▾
25	<input type="checkbox"/>	Auto ▾	Active ▾
26	<input type="checkbox"/>	Auto ▾	Active ▾

Save Reset

Figure 49 - LACP Port Configuration interface

The following table describes the columns and labels for the **LACP Port Configuration** screen.

Label	Description
Port	The switch port number.
LACP Enabled	Controls whether LACP is enabled on this switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner. Up to 32 aggregations are supported (if stackable).
Key	The Key value varies with the port, ranging from 1 to 65535. The options available from the drop-down list are: <ul style="list-style-type: none"> Auto will set the key according to the physical link speed (10Mb = 1, 100Mb = 2, 1Gb = 3). Specific allows you to enter a user-defined value. Ports with the same key value can join in the same aggregation group, while ports with different keys cannot.
Role	Indicates the LACP activity status. The options are: <ul style="list-style-type: none"> Active will transmit LACP packets every second; Passive will wait for a LACP packet from a partner (speak if spoken to).
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.3.2.3 System Status

This page provides a status overview for all LACP instances.

LACP System Status

Auto-refresh <input type="checkbox"/> <input type="button" value="Refresh"/>					
Aggr ID	Partner System ID	Partner Key	Partner Prio	Last Changed	Local Ports
No ports enabled or no existing partners					

Figure 50 - LACP System Status interface

The following table describes the columns and labels for the **LACP System Status** screen.

Label	Description
Aggr ID	The aggregation ID is associated with the aggregation instance. For LLAG, the ID is shown as ' isid:aggr-id ' and for GLAGs as ' aggr-id '.
Partner System ID	System ID (MAC address) of the aggregation partner.
Partner Key	The key assigned by the partner to the aggregation ID.
Partner Key	The partner's port priority.
Last Changed	The time since this aggregation changed.
Last Changed	Indicates which ports belong to the aggregation of the switch/stack. The format is Switch ID: Port .
Refresh	Click Refresh to refresh the page immediately.
Auto-refresh	Check Auto-refresh to enable an automatic refresh of the page at regular intervals.

5.3.2.4 Port Status

This page provides an overview of the LACP status for all ports.

LACP Status

Auto-refresh ☐

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port
1	No	-	-	-	-
2	No	-	-	-	-
3	No	-	-	-	-
4	No	-	-	-	-
5	No	-	-	-	-
6	No	-	-	-	-
7	No	-	-	-	-
8	No	-	-	-	-
9	No	-	-	-	-
10	No	-	-	-	-
11	No	-	-	-	-
12	No	-	-	-	-
13	No	-	-	-	-
14	No	-	-	-	-
15	No	-	-	-	-
16	No	-	-	-	-
17	No	-	-	-	-
18	No	-	-	-	-
19	No	-	-	-	-
20	No	-	-	-	-
21	No	-	-	-	-
22	No	-	-	-	-
23	No	-	-	-	-
24	No	-	-	-	-
25	No	-	-	-	-
26	No	-	-	-	-

Figure 51 - LACP Status interface

The following table describes the columns and labels for the **LACP Status** screen.

Label	Description
Port	Switch port number.
LACP	Yes means LACP is enabled and the port link is up. No means that LACP is not enabled or the port link is down. Backup means the port cannot join in the aggregation group unless other ports are removed and is in disabled LACP status.
Key	The key assigned to this port. Only ports with the same key can be Aggregated.
Aggr ID	The aggregation ID assigned to the aggregation group.
Partner System ID	The partner's system ID (MAC address).
Partner Port	The partner's port number associated with the port.
Refresh	Click Refresh to refresh the page immediately.
Auto-refresh	Check Auto-Refresh to enable an automatic refresh of the page at regular intervals.

5.3.2.5 Port Statistics

This page provides an overview of the LACP statistics for all ports.

LACP Statistics

Auto-refresh ☐

Port	LACP Received	LACP Transmitted	Discarded	
			Unknown	Illegal
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	0	0
24	0	0	0	0
25	0	0	0	0
26	0	0	0	0

Figure 52 - LACP Statistics interface

The following table describes the columns and labels for the **LACP Statistics** screen.

Label	Description
Port	Switch port number.
LACP Received	The number of LACP frames received at each port.
LACP Transmitted	The number of LACP frames sent from each port.
Discarded	The number of Unknown or Illegal LACP frames discarded at each
Refresh	Click Refresh to refresh the page immediately.
Auto-refresh	Check Auto-refresh to enable an automatic refresh of the page at regular intervals.
Clear	Click Clear to clear the counters for all ports.

5.3.3 Loop Protection

This feature is used to prevent a loop attack. When receiving loop packets, the port will be disabled automatically, preventing the loop attack from affecting other network devices.

5.3.3.1 Configuration

Global Configuration	
Enable Loop Protection	Disable ▼
Transmission Time	5 seconds
Shutdown Time	180 seconds

Figure 53 - Global Settings interface (Global Configuration)

The following table describes the columns and labels for the **Global Settings** screen.

Label	Description
Enable Loop Protection	Activates loop protection functions (as a whole).
Transmission Time	The interval between each loop protection PDU sent to each port. The value must be between 1 to 10 seconds.
Shutdown Time	The period (in seconds) for which a port will be kept disabled when a loop is detected (shutting down the port). The valid value is 0 to 604800 seconds (7 days). A value of zero will keep a port disabled permanently (until the device is restarted).

Port	Enable	Action	Tx Mode
*	<input checked="" type="checkbox"/>	<> ▼	<> ▼
1	<input checked="" type="checkbox"/>	Shutdown Port ▼	Enable ▼
2	<input checked="" type="checkbox"/>	Shutdown Port ▼	Enable ▼
3	<input checked="" type="checkbox"/>	Shutdown Port ▼	Enable ▼
4	<input checked="" type="checkbox"/>	Shutdown Port ▼	Enable ▼
5	<input checked="" type="checkbox"/>	Shutdown Port ▼	Enable ▼
6	<input checked="" type="checkbox"/>	Shutdown Port ▼	Enable ▼

Figure 54 - Port Configuration interface

The following table describes the columns and labels for the **Port Configuration** screen.

Label	Description
Port	Switchs port number
Enable	Activates loop protection functions (as a whole)
Action	Configures the action to take when a loop is detected. Valid values include Shutdown Port and Log or Log Only .
Tx Mode	Controls whether the port is actively generating loop protection PDUs or only passively look for looped PDUs (protocol data units).

5.3.3.2 Status

The Loop Protection Status is shown on the following page.

Loop Protection Status

Auto-refresh ☐ Refresh

Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
No ports enabled						

Figure 55 - Loop Protection Status interface

The following table describes the columns and labels for the **Loop Protection Status** screen.

Label	Description
Port	The switch port number of the logical port.
Action	The currently configured port action.
Transmit	The currently configured port transmit mode.
Loops	The number of loops detected on this port.
Status	The current loop protection status of the port.
Loop	Whether a loop is currently detected on the port.
Time of Last Loop	The time of the last loop event detected.
Refresh	Click Refresh to refresh the page immediately.
Auto-refresh	Check Auto-refresh to enable an automatic refresh of the page at regular intervals.

5.4 Redundancy

5.4.1 iRing Configuration

iS5 supports three ring topologies: **Ring Master**, **Coupling Ring**, and **Dual Homing**. You can configure the settings in the interface below.

iRing Configuration

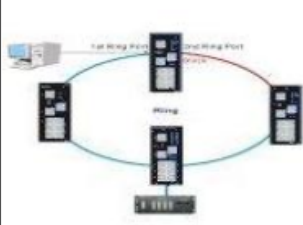
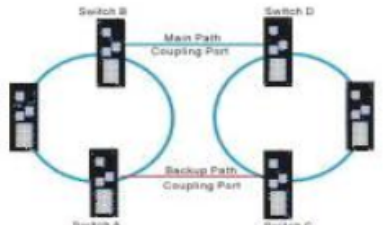

<input type="checkbox"/> iRing 		<input type="checkbox"/> Coupling Ring 		<input type="checkbox"/> Dual Homing 	
Ring Master	Disable ▾	Coupling Port	Port 3 ▾	Homing Port	Port 4 ▾
1st Ring Port	Port 1 ▾				
2nd Ring Port	Port 2 ▾				

Figure 56- iRing Configuration interface

The following table describes the columns and labels for the **iRing Configuration** screen.

Label	Description
iRing	Check to enable iRing topology.
Ring Master	Only one ring master is allowed in a ring. However, if more than one switch is set to enable Ring Master , the switch with the lowest MAC address will be the active ring master and the others will be backup masters.
1st Ring Port	The primary ring port
2nd Ring Port	The backup ring port
Coupling Ring	Having a check mark to enable Coupling Ring . Coupling Ring can divide a big ring into two smaller rings to avoid network topology changes affecting all switches. This is a good method for connecting two rings.
Coupling Port	Used for connecting multiple rings. A coupling ring needs four switches to build an active and a backup link. Links formed by the coupling ports will run in active/backup mode.
Dual Homing	Check to enable Dual Homing . When Dual Homing is enabled, the ring will be connected to normal switches through two RSTP links (e.g. a backbone switch). The two links work in active/backup mode and connect each ring to the normal switches in RSTP mode.
Save	Click Save to apply the configurations.

5.4.2 iChain

iChain is very easy to configure and manage. Only one edge port of the edge switch needs to be defined. Other switches beside them just need to have iChain enabled.

iChain Configuration

<input checked="" type="checkbox"/> Enable			
	Uplink Port	Edge Port	State
1st	Port 1 ▾	<input type="checkbox"/>	LinkDown
2nd	Port 2 ▾	<input checked="" type="checkbox"/>	Forwarding

Save Refresh

Figure 57 - iChain Configuration interface

The following table describes the columns and labels for the **iChain Configuration** screen.

Label	Description
Enable	Check to enable iChain function
Uplink Port; 1st Ring Port	From the drop-down list, choose the first port connecting to the ring.
Uplink Port; 2nd Ring Port	From the drop-down list, choose the second port connecting to the ring.
Edge Port	An iChain topology must begin with edge ports. The ports with a smaller switch MAC address will serve as backup link and RM LED will light up. There are two uplink ports for every device in the chain. The user must specify the ports according to topology of network.
State	Indicates the state of the Ring Port. There three states for uplink port: Link Down, Blocking, and Forwarding.
Save	Click Save to save the changes.
Refresh	Click Refresh to refresh the page immediately.

5.4.3 iBridge

The iBridge technology can be enabled to allow the addition of iS5Com switches into a network constructed by another vendor's proprietary ring and enable interoperability between managed switches. Use iBridge to connect 2 ring networks. Perform that on the next page.

iBridge

<input type="checkbox"/> Enable	
Vender	Moxx ▾
1st Ring Port	Port 1 ▾
2nd Ring Port	Port 2 ▾

Save

Figure 58 - iBridge interface

The following table describes the labels for the **iBridge** screen.

Label	Description
Enable	Enabling the iBridge function
Vender	Choosing a vendor to whose ring you want to join (e.g. Moxx).
1st Ring Port	Choosing the port which connects to the Ring
2nd Ring Port	Choosing the port which connects to the Ring

5.4.4 RSTP

The Rapid Spanning Tree Protocol (RSTP) is an evolution of the Spanning Tree Protocol (STP). It provides faster convergence of spanning tree after a topology change. The system also supports STP and will detect a connected device that is running STP or RSTP protocol automatically. RSTP is enabled by default.

5.4.4.1 RSTP Bridge Setting

The RSTP function can be disabled, STP or RSTP and parameters set for each port via the RSTP Setting interface as shown below.

RSTP Bridge Setting

Mode	Disable ▾
Bridge Priority	32768 ▾
Max Age	20
Hello Time	2
Forward Delay	15

Save

Figure 59 - RSTP Bridge Setting interface

The following table describes the labels for the **RSTP Bridge Setting** screen.

Label	Description
Mode	The RSTP function must be chosen or disabled before configuring any of the related parameters. Valid values are Disable STP and RSTP.
Bridge Priority (0-61440)	A value used to identify the root bridge. The bridge with the lowest value (highest priority) is selected as the root. If the value changes, the switch must be rebooted. The value must be a multiple of 4096 according to the protocol standard.
Max Age (6-40)	The maximum age of the information transmitted by the Bridge when it is the Root Bridge. Valid values are in the range 6 to 40 seconds, and MaxAge must be $\leq (\text{FwdDelay}-1) * 2$
Hello Time (1-10)	The time that the Control Switch sends out the BPDU (Bridge Protocol Data Unit) packet to verify the status of RSTP. Enter a value between 1 and 10.
Forwarding Delay Time (4-30)	The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode). Valid values are in the range 4 to 30 seconds.

NOTE: Follow this rule to configure the MAX Age, Hello Time, and Forward Delay Time: $2 \times (\text{Forward Delay Time value} - 1) \geq \text{Max Age value} \geq 2 \times (\text{Hello Time value} + 1)$.

5.4.4.2 Port Setting

This page allows the user to configure the current RSTP port configurations, and change them as well.

RSTP Port Setting

Port	Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Admin P2P
*	<input checked="" type="checkbox"/>	<> ▾	<> ▾	<> ▾	<input checked="" type="checkbox"/>	<> ▾
1	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
2	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
3	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
4	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
5	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
6	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
7	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
8	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
9	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
10	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
11	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
12	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
13	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
14	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
15	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
16	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
17	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
18	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
19	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
20	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
21	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
22	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
23	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
24	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
25	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾
26	<input checked="" type="checkbox"/>	Auto ▾	128 ▾	Edge ▾	<input checked="" type="checkbox"/>	Auto ▾

Save Reset

Figure 60 - RSTP Port Setting interface

The following table describes the labels for the **RSTP Port Setting** screen.

Label	Description
Port	The switch port number of the logical RSTP port
Enabled	Controls whether RSTP is enabled on this switch port.
Path Cost	The Auto setting will set the path cost as appropriate by the physical link speed, using the 802.1D 2004 recommended values. By using the Specific setting, a user-defined value can be entered. The path cost is used when establishing the active topology of the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. Valid values are in the range 1 to 200000000.
Priority	Enter which port should be blocked by setting the priority on the LAN. Enter a number between 0 and 240. The value of priority must be a multiple of 16.
Admin Edge	Admin Edge is the port which is directly connected to end stations. It cannot create a bridging loop on the network. To configure the port as an edge port, set the port to Edge . The other option is Non-Edge .
Auto Edge	Controls whether the bridge enables automatic edge detection on the Bridge port. This allows <i>operEdge</i> to be derived from whether BPDU's are received on the port or not.
Admin P2P	Controls whether the port connects to a point-to-point LAN rather than to a shared medium. This can be automatically determined—when Auto option is selected, or Forced True or Forced False . Transition to the forwarding state is faster for point-to-point LANs than for shared media.
Save	Click Save to apply the configurations.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.4.4.3 Bridge Status

This page provides detailed information on a single RSTP Bridge instance.

RSTP Bridge Status

Auto-refresh ☐ Refresh

RSTP is disabled.

This is the screen with RSTP disabled.

RSTP Bridge Status

Auto-refresh ☐ Refresh

Root Bridge ID	32768.E8-E8-75-00-01-B0
Root Port	--
Path Cost	0
Max Age	20
Hello Time	2
Forward Delay	15

Figure 61 - RSTP Bridge Status interface

The following table describes the labels for the **RSTP Bridge Status** screen.

Label	Description
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click Refresh to refresh the page immediately.
Root Bridge ID	The Bridge ID of this Bridge instance.
Root Port	The switch port currently assigned to the Root Port role.
Path Cost	This is the Root Path Cost. For the Root Bridge , this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge.
Max Age	The maximum age of information defined in this device.
Hello Time	The time that the Control Switch sends out the BPDU (Bridge Protocol Data Unit).
Forward Delay	The delay used by STP Bridges to transit Root and Designated Ports to Forwarding (used in STP compatible mode).

5.4.4.4 Port Status

This page displays the RSTP port status for physical ports of the switch.

RSTP Port Status

Auto-refresh ☐ [Refresh](#)

Port	Enabled	Port Priority	Path Cost	Oper Edge	Oper P2P	Role	State
1	Disabled	--	--	--	--	--	--
2	Disabled	--	--	--	--	--	--
3	Disabled	--	--	--	--	--	--
4	Disabled	--	--	--	--	--	--
5	Disabled	--	--	--	--	--	--
6	Disabled	--	--	--	--	--	--
7	Disabled	--	--	--	--	--	--
8	Disabled	--	--	--	--	--	--
9	Disabled	--	--	--	--	--	--
10	Disabled	--	--	--	--	--	--
11	Disabled	--	--	--	--	--	--
12	Disabled	--	--	--	--	--	--
13	Disabled	--	--	--	--	--	--
14	Disabled	--	--	--	--	--	--
15	Disabled	--	--	--	--	--	--
16	Disabled	--	--	--	--	--	--
17	Disabled	--	--	--	--	--	--
18	Disabled	--	--	--	--	--	--
19	Disabled	--	--	--	--	--	--
20	Disabled	--	--	--	--	--	--
21	Disabled	--	--	--	--	--	--
22	Disabled	--	--	--	--	--	--
23	Disabled	--	--	--	--	--	--
24	Disabled	--	--	--	--	--	--
25	Disabled	--	--	--	--	--	--
26	Disabled	--	--	--	--	--	--

Figure 62 - RSTP Port Status interface

The following table describes the labels for the **RSTP Port Status** screen.

Label	Description
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Click Refresh to refresh the page immediately.
Port	The switch port number of the logical RSTP port
Enabled	Controls whether RSTP is enabled or disabled on this switch port.
Port Priority	Which ports should be blocked by priority in LAN. A number 0 through 240. The value of priority must be the multiple of 16.
Path Cost	The cost of the path to the other bridge from this transmitting bridge at the specified port. A number 1 through 200000000.
Oper Edge	When True , Oper Edge is enabled, the port is configured as an edge port and directly connected to an end station and cannot create a bridging loop. False means Oper Edge disabled.
Oper P2P	Some of the rapid state transactions that are possible within RSTP are dependent upon whether the port concerned can only be connected to exactly one other bridge (i.e. It is served by a point-to-point LAN segment), or it can be connected to two or more bridges (i.e. It is served by a shared medium LAN segment). OperP2P shows the P2P status of the link to be manipulated administratively. True means P2P enabling. False means P2P disabling.
Role	The Role of each port is Disabled or Designated .
State	The State of each port is Disabled or Forwarding .

5.4.5 MSTP

5.4.5.1 Bridge Settings

This page allows you to configure STP system settings. The settings are used by all STP Bridge instances in the switch .

STP Bridge Configuration

Basic Settings

Protocol Version	MSTP
Bridge Priority	32768
Forward Delay	15
Max Age	20
Maximum Hop Count	20
Transmit Hold Count	6

Advanced Settings

Edge Port BPDU Filtering	<input type="checkbox"/>
Edge Port BPDU Guard	<input type="checkbox"/>
Port Error Recovery	<input type="checkbox"/>
Port Error Recovery Timeout	

Save

Reset

Figure 63 - STP Bridge Configuration interface

The following table describes the labels for the **RSTP Port Status** screen.

Label	Description
Protocol Version	The version of the STP protocol. Valid values include STP, RSTP and MSTP.
Bridge Priority	Controls the bridge priority. Lower numeric values have better priority. The bridge priority plus the MSTI instance number, concatenated with the 6-byte MAC address of the switch forms a <i>Bridge Identifier</i> . For MSTP operation, this is the priority of the CIST. Otherwise, this is the priority of the STP/RSTP bridge.
Forward Delay	The delay used by STP bridges to transit root and designated ports to forwarding (used in STP compatible mode). The range of valid values is 4 to 30 seconds.
Max Age	The maximum time the information transmitted by the root bridge is considered valid. The range of valid values is 6 to 40 seconds, and Max Age must be $\leq (\text{FwdDelay}-1)*2$.
Maximum Hop Count	This defines the initial value of remaining hops for MSTI information generated at the boundary of an MSTI region. It defines how many bridges a root bridge can distribute its BPDUs to. The range of valid values is 4 to 30 seconds, and MaxAge must be $\leq (\text{FwdDelay}-1)*2$.
Transmit Hold Count	The number of BPDUs a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. The range of valid values is 1 to 10 BPDUs per second.
Edge Port BPDU Filtering	Control whether a port <i>explicitly</i> configured as Edge will transmit and receive BPDUs.
Edge Port BPDU Guard	Control whether a port <i>explicitly</i> configured as Edge will disable itself upon reception of a BPDU. The port will enter the <i>error-disabled</i> state, and will be removed from the active topology.
Port Error Recovery	Control whether a port in the <i>error-disabled</i> state automatically will be enabled after a certain time. If recovery is not enabled, ports must be disabled and re-enabled for normal STP operation. The condition is also cleared by a system reboot.
Port Error Recovery Timeout	The time to pass before a port in the <i>error-disabled</i> state can be enabled. Valid values are between 30 and 86400 seconds (24 hours).
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.4.5.2 MSTI Mapping

This page allows you to examine and change the configurations of current STP MSTI bridge instances.

MSTI Configuration

Add VLANs separated by spaces or comma.

Unmapped VLANs are mapped to the CIST. (The default bridge instance).

Configuration Identification

Configuration Name	e8-e8-75-00-01-b1
Configuration Revision	0

MSTI Mapping

MSTI	VLANs Mapped
MSTI1	
MSTI2	
MSTI3	
MSTI4	
MSTI5	
MSTI6	
MSTI7	

Save

Reset

Figure 64 - MSTI Configuration interface

The following table describes the labels for the **MSTI Configuration** screen.

Label	Description
Configuration Name	The name which identifies the VLAN to MSTI mapping. Bridges must share the name and revision (see below), as well as the VLAN-to-MSTI mapping configurations to share spanning trees for MSTI's (intra-region). The name should not exceed 32 characters.
Configuration Revision	Revision of the MSTI configuration named above. This must be an integer between 0 and 65535.
MSTI	This id for the Bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped.
VLANs Mapped	The list of VLAN's mapped to the MSTI. The VLAN's must be separated with commas and/or a space. A VLAN can only be mapped to one MSTI. An unused MSTI will be left empty (e.g. without any mapped VLANs).
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previous values.

5.4.5.3 MSTI Priorities

This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

MSTI Configuration

MSTI Priority Configuration

MSTI	Priority
*	<>
CIST	32768
MSTI1	32768
MSTI2	32768
MSTI3	32768
MSTI4	32768
MSTI5	32768
MSTI6	32768
MSTI7	32768

Save

Reset

Figure 65 - MSTI Configuration interface

The following table describes the labels for the **MSTI Configuration** screen.

Label	Description
MSTI	This is the bridge instance. CIST is the default instance, which is always active.
Priority	Indicates bridge priority. The lower the value, the higher the priority. The bridge priority, MSTI instance number, and the 6-byte MAC address of the switch forms a bridge identifier.
Save	Click Save to save changes
Reset	Click Reset to undo any changes made locally and revert to previously saved values

5.4.5.4 CIST Ports

This page allows the user to inspect the current STP CIST port configurations, and possibly change them as well. The page contains settings for physical and aggregated ports.

CIST Aggregated Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
-	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced True

CIST Normal Port Configuration

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted Role	TCN	BPDU Guard	Point-to-point
*	<input type="checkbox"/>	<>	<>	<>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<>
1	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
2	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
3	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
4	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
5	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
6	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
7	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
8	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
9	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
10	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
11	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
12	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
13	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
14	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
15	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
16	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
17	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
18	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
19	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
20	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
21	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
22	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
23	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
24	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
25	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto
26	<input type="checkbox"/>	Auto	128	Non-Edge	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto

Save Reset

Figure 66 - CIST Aggregated Port Configuration interface

The following table describes the labels for the **CIST Aggregated Port Configuration** screen.

Label	Description
Port	The switch port number to which the following settings will be applied.
STP Enabled	Check to enable STP for the port
Path Cost	Configures the path cost incurred by the port. Auto will set the path cost according to the physical link speed by using the 802.1D-recommended values. Specific allows you to enter a user-defined value. The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. The range of valid values is 1 to 200000000.
Priority	Configures the priority for ports having identical port costs. (See above).
Admin Edge	Configures the Oper Edge flag to start as set or cleared (the initial Oper Edge state when a port is initialized).
Auto Edge	Check to enable the bridge to detect edges at the bridge port automatically. This allows Oper Edge to be derived from whether BPDUs are received on the port or not.
Restricted Role	When enabled, the port will not be selected as root port for CIST or any MSTI, even if 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. If set, spanning trees will lose connectivity. It can be set by a network administrator to prevent bridges outside a core region of the network from influencing the active spanning tree topology because those bridges are not under the full control of the administrator. This feature is also known as Root Guard.
Restricted TCN	When enabled, the port will not propagate received topology change notifications and topology changes to other ports. If set, it will cause temporary disconnection after changes in an active spanning trees topology because of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges outside a core region of the network from causing address flushing in that region because those bridges are not under the full control of the administrator or is the physical link state for the attached LANs transitions frequently.
Point-to-Point	Configures whether the port connects to a point-to-point LAN rather than a shared medium. This can be configured automatically or set to true or false manually. Transitioning to forwarding state is faster for point-to-point LANs than for shared media.
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.4.5.5 MSTI Ports

This page allows the user to inspect the current STP MSTI port configurations, and possibly change them as well.

An MSTI port is a virtual port, which is instantiated separately for each active CIST (physical) port for each MSTI instance configured on and applicable to the port. The MSTI instance must be selected before displaying actual MSTI port configuration options.

This page contains the MSTI port settings for physical and aggregated ports.

MSTI Port Configuration

Select MSTI

MST1
MST2
MST3
MST4
MST5
MST6
MST7

Get

MSTI Aggregated Ports Configuration (Stack Global)

Port	Path Cost	Priority
-	Auto	128

MSTI Normal Ports Configuration

Port	Path Cost	Priority
*	<>	<>
1	Auto	128
2	Auto	128
3	Auto	128
4	Auto	128

Figure 67 – MST1 MSTI Port Configuration interface

The following table describes the labels for the **MST1 MSTI Port Configuration** screen.

Label	Description
Port	The switch port number of the corresponding STP CIST (and MSTI) port
Path Cost	Configures the path cost incurred by the port. Auto will set the path cost according to the physical link speed by using the 802.1D-recommended values. Specific allows you to enter a user-defined value. The path cost is used when establishing an active topology for the network. Lower path cost ports are chosen as forwarding ports in favor of higher path cost ports. The range of valid values is 1 to 200000000.
Priority	Configures the priority for ports having identical port costs. (See above).
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.4.5.6 Bridge Status

This page shows the status for all STP Bridge instances.

STP Bridges

Auto-refresh ☐ Refresh

MSTI	Bridge ID	Root			Topology Flag	Topology Change Last
		ID	Port	Cost		
CIST	32768.E8-E8-75-00-01-B1	32768.E8-E8-75-00-01-B1	-	0	Steady	-

Figure 68 - STP Bridges interface

The following table describes the labels for the **STP Bridges** screen.

Label	Description
MSTI	This is the bridge instance. It can also be linked to the STP detailed bridge status.
Bridge ID	The bridge ID of this bridge instance.
Root ID	The bridge ID of the currently selected root bridge.
Root Port	The switch port currently assigned the root port role.
Root Cost	Root path cost. For a root bridge, this is zero. For other bridges, it is the sum of port path costs on the least cost path to the Root Bridge.
Topology Flag	The current state of the Topology Change Flag for the bridge instance.
Topology Change Last	The time since last Topology Change occurred.
Refresh	Click to refresh the page immediately.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.

5.4.5.7 Port Status

This page displays the STP port status for the currently selected switch.

STP Port Status

Auto-refresh ☐ Refresh

Port	CIST Role	CIST State	Uptime
1	Non-STP	Forwarding	-
2	Non-STP	Forwarding	-
3	Non-STP	Forwarding	-
4	Non-STP	Forwarding	-
5	Non-STP	Forwarding	-
6	Non-STP	Forwarding	-
7	Non-STP	Forwarding	-
8	Non-STP	Forwarding	-
9	Non-STP	Forwarding	-

Figure 69 - STP Port Status interface

The following table describes the labels for the **STP Port Status** screen.

Label	Description
Port	The switch port number to which the following settings will be applied.
CIST Role	The current STP port role of the CIST port. The values include: AlternatePort , BackupPort , RootPort , DesignatedPort , and Non-STP .
IST State	The current STP port state of the CIST port. The values include: Blocking , Learning , and Forwarding .
Uptime	The time since the bridge port was last initialized
Refresh	Click Refresh to refresh the page immediately.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.

5.4.5.8 Port Statistics

This page displays the STP port statistics for the currently selected switch.

STP Statistics

Auto-refresh ☐ Refresh Clear

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
No ports enabled										

Figure 70 - STP Statistics interface

The following table describes the labels for the **STP Statistics** screen.

Label	Description
Port	The switch port number to which the following settings will be applied.
Transmitted / Received	
MSTP	The number of MSTP configuration BPDU's received/transmitted on the port.
RSTP	The number of RSTP configuration BPDU's received/transmitted on the port
STP	The number of legacy STP configuration BPDU's received/transmitted on the port
TCN	The number of (legacy) topology change notifications BPDU's received/transmitted on the port.
Discarded	
Unknown	The number of unknown spanning tree BPDUs received (and discarded) on the port.
Illegal	The number of illegal spanning tree BPDU's received (and discarded) on the port.
Refresh	Click Refresh to refresh the page immediately.
Auto-refresh	Check this to enable an automatic refresh of the page at regular intervals.

5.4.6 MRP

MRP

<input checked="" type="checkbox"/> Enable		
<input type="checkbox"/> Manager	<input type="checkbox"/> React on Link Change	
1st Ring Port	Port 7 ▼	LinkDown
2nd Ring Port	Port 8 ▼	LinkDown

Apply

Figure 71 - MRP

Label	Description
Enable	Enables the MRP function.
Manager	Every MRP topology needs a MRP manager, and can only have one manager. If two or more switches are set to be Managers at the same time, the MRP topology will fail.

Label	Description
React on Link Change (Advanced mode)	Faster mode. Enabling this function will ensure MRP topology a more rapid converge. This function only can be set by the MRP manager switch.
1st Ring Port	Chooses the port that connects to the MRP ring.
2nd Ring Port	Chooses the port that connects to the MRP ring.

5.4.7 Fast Recovery

Fast Recovery

<input type="checkbox"/> Enable	Recovery Priority
1	Not included ▼
2	Not included ▼
3	Not included ▼
4	Not included ▼
5	Not included ▼
6	Not included ▼
7	Not included ▼
8	Not included ▼
9	Not included ▼
10	Not included ▼
11	Not included ▼
12	Not included ▼
13	Not included ▼
14	Not included ▼
15	Not included ▼
16	Not included ▼
17	Not included ▼
18	Not included ▼
19	Not included ▼
20	Not included ▼
21	Not included ▼
22	Not included ▼
23	Not included ▼
24	Not included ▼
25	Not included ▼
26	Not included ▼

Fast Recovery is disabled.

Save

Figure 72 - Fast Recovery interface

The following table describes the labels for the **Fast Recovery** screen.

Label	Description
Enable	Enable Fast Recovery function
Recovery Priority	Ports can be set to 26 priorities. Only the port with the highest priority will be the active port. The port with the highest recovery priority (the lowest number) will be the active port, others will be blocked (if included). Choose the Recovery Priority number from the drop-down list.
Save	Click Save to save the configurations.

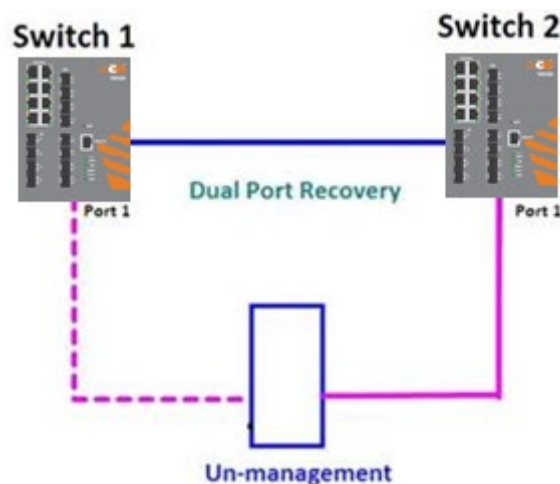
5.4.8 Dual Port Recovery

Dual Port Recovery mode is defined to work with unmanaged devices/switches or ring of switches. This feature can be set to on single port of switches on both sides of unmanaged ring. The iES22GF with Dual Port Recovery mode will provide redundant links.

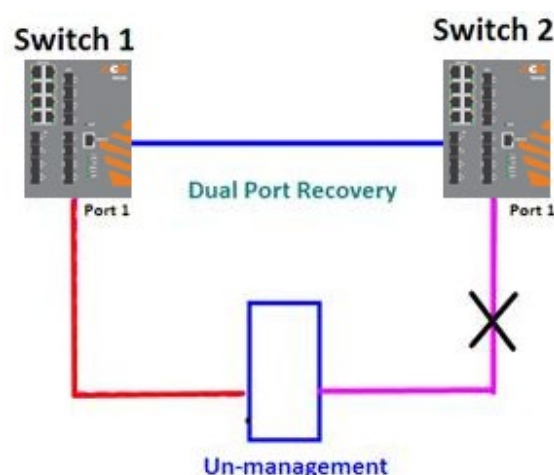
5.4.8.1 Introduction

Dual Port Recovery is an iS5 Com's Proprietary solution for interoperability issues with unmanaged devices such as unmanaged switches. Dual Port Recovery allows Ethernet switches in ring configuration with unmanaged devices to recover from failure rapidly to ensure seamless data transmission. A Dual Port Recovery ring can support up to 5 unmanaged devices and will enable a back-up link in 40ms (adjustable to min 20ms (recommended is 40ms)).

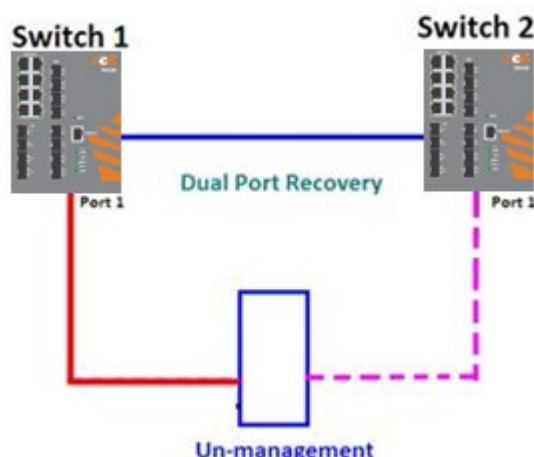
This protocol is based on sending specific messages (BPDU format) from each port on both sides of unmanaged chain. The Dual Port Recovery feature can be executed with other redundancy protocols on same device.



In Dual Port Recovery function if link of port in "Forwarding" state goes down, the "backup" port is changing its state to be forwarding, like in picture below. The disconnected port changes its status to "No Link".



When link of port 1 on switch 2 returns to be linked up, the switch 1 port 1 is in “Forwarding” state and in this case the “No Link” port is changing its status to be “Blocking” port.



5.4.8.2 Configuration of Dual Port Recovery

Dual Port Recovery

<input type="checkbox"/> Enable		
Active Port	Port 1 ▾	LinkDown
Test Interval	10	10~5000ms
Test Max Retry	3	1~500

Save Refresh

Figure 73 - Dual Port Recovery interface

The following table describes the labels for the **Dual Port Recovery** screen.

Label	Description
Enable	Activate the Dual Port Recovery mode.
Active Port	Choosing the port which connects to the unmanaged switch/ring of switches. Note: User needs to select one port to be Active Port on each of two devices of each side.
Test Interval	Setting Interval time for sending keep alive messages (10-5000ms default 10) Note: Test interval should be the same on both sides.
Test Max Retry	Set the maximum number of lost frames to start Dual Port Recovery mechanism (1-500 retries default 3) Note: Test Max Retry should be the same on both sides.
Apply	Click Apply to activate the configurations.

5.5 VLAN

5.5.1 VLAN Membership

You can view and change VLAN membership configurations for a selected switch stack in this page. Up to 64 VLAN's are supported. This page allows for adding and deleting VLAN's as well as adding and deleting port members of each VLAN.

VLAN Membership Configuration

Refresh |<< >>

Start from VLAN with entries per page.

Delete	VLAN ID	VLAN Name	Port Members																									
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
<input type="checkbox"/>	1	default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add New VLAN

Save Reset

Figure 74- VLAN Membership Configuration interface

The following table describes the labels for the **VLAN Membership Configuration** screen.

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
VLAN Name	Indicates the name of the VLAN. The VLAN Name is a string that is 0 to 32 characters in length. Alpha and numeric characters are valid.
Port Members	<p>Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry. The Status of each port can be:</p> <p><input checked="" type="checkbox"/> : To include a port in the VLAN.</p> <p><input type="checkbox"/> : To include a port in a forbidden port list in the VLAN.</p> <p><input type="checkbox"/> : To remove or exclude the port from the VLAN.</p> <p>By default, no ports are members of a newly created VLAN.</p>
Add New VLAN	<p>Click to add a new VLAN ID. An empty row is added to the table, and the VLAN can be configured as needed. Valid values for a VLAN ID are 1 through 4095.</p> <p>After clicking Save, the new VLAN will be enabled on the selected switch stack but contains no port members.</p> <p>A VLAN without any port members on any stack will be deleted when you click Save.</p> <p>Click Delete to undo the addition of new VLANs.</p>
Save	Click to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.5.2 Port Configurations

This page allows you to set up VLAN ports individually.

Auto-refresh ☐ Refresh

Ethertype for Custom S-ports 0x88A8

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN		Tx Tag
				Mode	ID	
*	<>	<input type="checkbox"/>	<>	<>	1	<>
1	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
2	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
3	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
4	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
5	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid

Figure 75 - VLAN Port Configuration interface

The following table describes the labels for the **VLAN Port Configuration** screen.

Label	Description
Ethertype for custom S-Ports	This field specifies the Ether type used for custom S-ports. This is a global setting for all custom S-ports.
Port	The switch port number to which the following settings will be applied.
Port Type	Port can be one of the following types: Unaware , Custom (C-port) , Service (S-port) , Custom Service (S-custom-port) . If the Port Type is Unaware , all frames are classified to the port VLAN ID and tags are not removed.
Ingress Filtering	Enable Ingress Filtering on a port by checking the box. This parameter affects VLAN ingress processing. If ingress filtering is enabled and the ingress port is not a member of the classified VLAN of the frame, the frame will be discarded. By default, Ingress Filtering is disabled (no check mark).
Frame Type	Determines whether the port accepts all frames or only tagged/untagged frames. This parameter affects VLAN ingress processing. The Values are All , Tagged , and Untagged . If the port only accepts Tagged frames, all received by the port Untagged frames will be discarded. By default, the field is set to All .
Port VLAN Mode	The allowed values are None or Specific . This parameter affects VLAN ingress and egress processing. If None is selected, a VLAN tag with the classified VLAN ID is inserted in frames transmitted on the port. This mode is normally used for ports connected to VLAN-aware switches. Tx tag should be set to Untag_pvid when this mode is used. If Specific (the default value) is selected, a port VLAN ID can be configured (see below). Untagged frames received on the port are classified to the port VLAN ID. If VLAN awareness is disabled, all frames received on the port are classified to the port VLAN ID. If the classified VLAN ID of a frame transmitted on the port is different from the port VLAN ID, a VLAN tag with the classified VLAN ID will be inserted in the frame.
Port VLAN ID	Configures the VLAN identifier for the port. The allowed range of the values is 1 through 4095. The default value is 1. The port must be a member of the same VLAN as the port VLAN ID.
Tx Tag	Determines egress tagging of a port. Untag_pvid : all VLANs except the configured PVID will be tagged. Tag_all : all VLANs are tagged. Untag_all : all VLANs are untagged.

5.5.2.1 More Details on Port Types

Below is a detailed description of every port type, including **Unaware**, **C-port**, **S-port**, and **S-custom-port**. TPID stands for the modified tag protocol identifier (TPID) value of VLAN Tags.

Description	Ingress action	Egress action
Unaware The function of Unaware can be used for 802.1QinQ (double tag).	When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded. When the port receives tagged frames: <ul style="list-style-type: none"> If the tagged frame contains a TPID of 0x8100, it will become a double-tag frame and will be forwarded. If the TPID of tagged frame is not 0x8100 (e.g. 0x88A8), it will be forwarded. 	The TPID of a frame transmitted by Unaware port will be set to 0x8100. The final status of the frame after egressing will also be affected by the Egress Rule.
C-port	When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded. When the port receives tagged frames: <ul style="list-style-type: none"> If the tagged frame contains a TPID of 0x8100, it will be forwarded. 	The TPID of a frame transmitted by C-port will be set to 0x8100.
S-port	When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded. When the port receives tagged frames: <ul style="list-style-type: none"> If the tagged frame contains a TPID of 0x8100, it will be forwarded. If the TPID of tagged frame is not 0x88A8 (ex. 0x8100), it will be discarded. 	The TPID of a frame transmitted by S-port will be set to 0x88A8.
S-custom-port	When the port receives untagged frames, an untagged frame obtains a tag (based on PVID) and is forwarded. When the port receives tagged frames: <ul style="list-style-type: none"> If the tagged frame contains a TPID of 0x8100, it will be forwarded. If the TPID of tagged frame is not 0x88A8 (e.g. 0x8100), it will be discarded. 	The TPID of a frame transmitted by S-custom-port will be set to a Self-customized value, which can be set by the user via Ethertype for Custom S-ports .

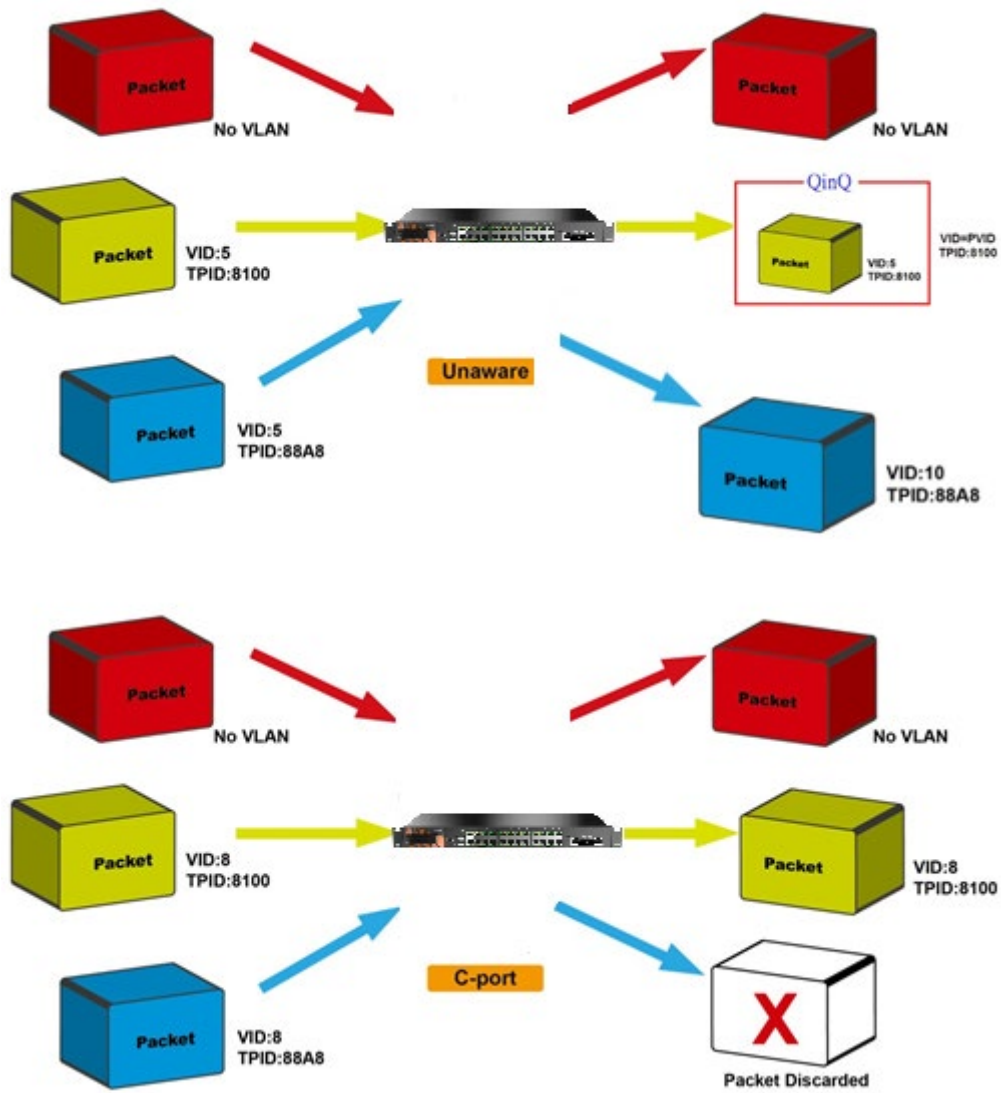


Figure 76 - Unaware and C-port Port Types

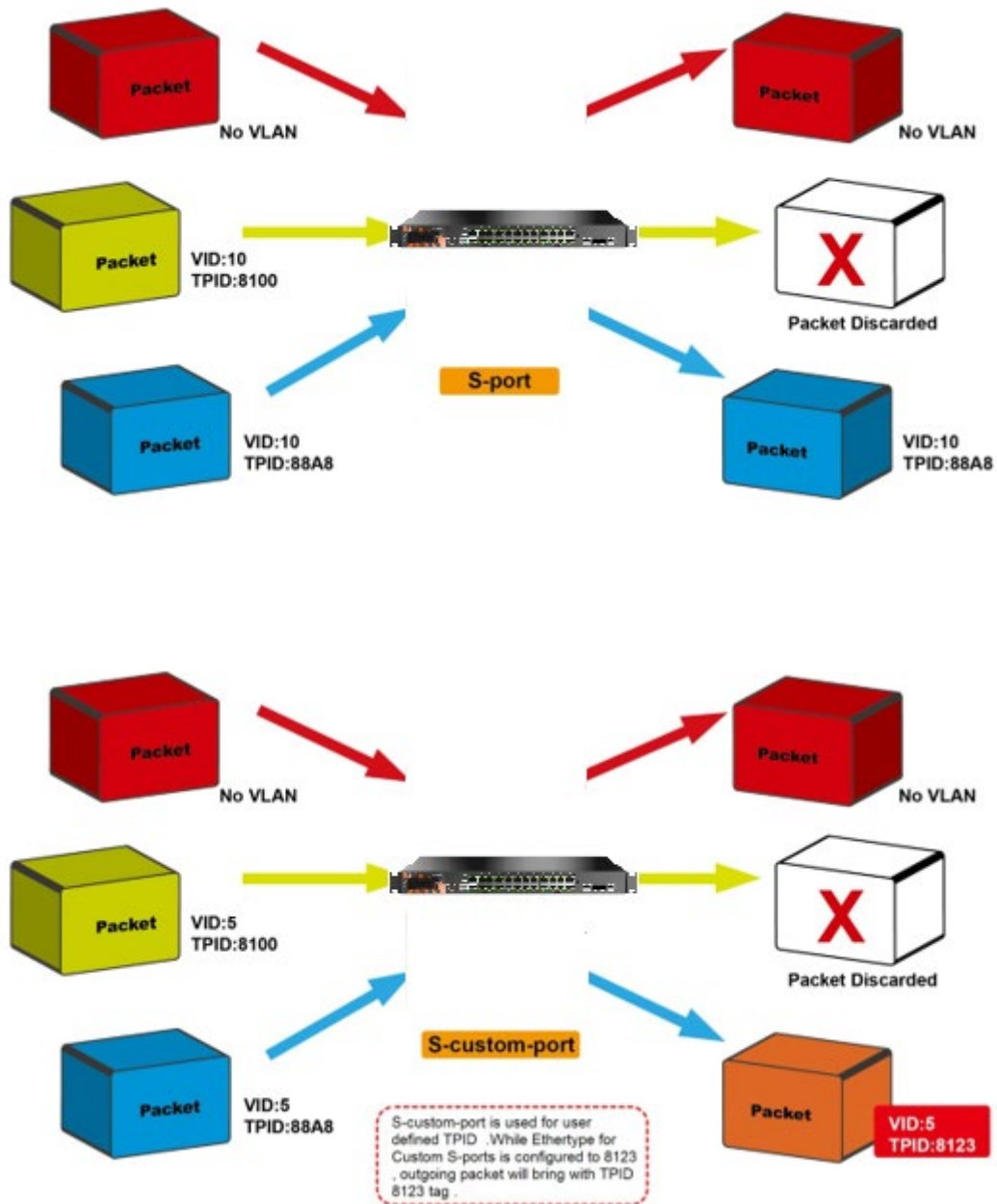


Figure 77 - S-port and S-custom Port Types

5.5.2.2 Examples of VLAN Settings

1) VLAN Access Mode

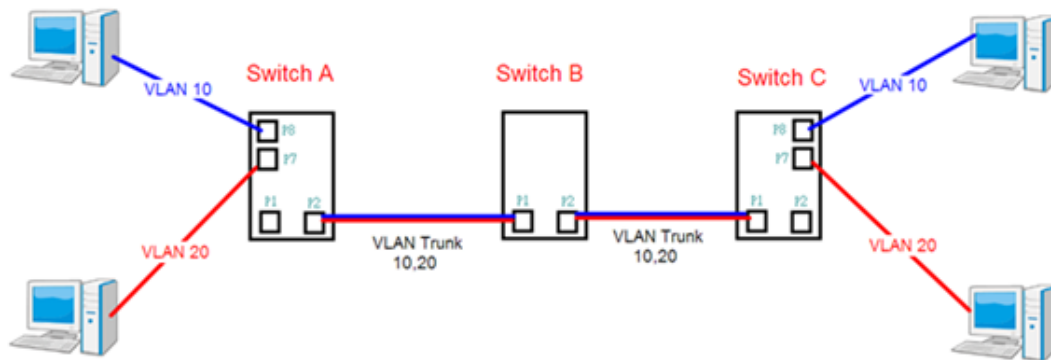


Figure 78 - VLAN Access Mode topology

For Switch A:

Port 7 is VLAN Access mode = Untagged 20

Port 8 is VLAN Access mode = Untagged 10

Below are the switch's settings.

VLAN Membership Configuration

Refresh |<< >>

Start from VLAN with entries per page.

Delete	VLAN ID	VLAN Name	Port Members																											
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
<input type="checkbox"/>	1	default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	10	VLAN10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	20	VLAN20	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add New VLAN

Save Reset

For port 1 VLAN trunk setting

For port 7 & 8 VLAN Access

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN		Tx Tag
				Mode	ID	
*	<>	<input type="checkbox"/>	<>	<>	1	<>
1	C-port	<input type="checkbox"/>	Tagged	Specific	1	Tag_all
2	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
3	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
4	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
5	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
6	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
7	Unaware	<input type="checkbox"/>	Untagged	Specific	20	Untag_pvid
8	Unaware	<input type="checkbox"/>	Untagged	Specific	10	Untag_pvid
9	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid

2) VLAN 1Q Trunk Mode

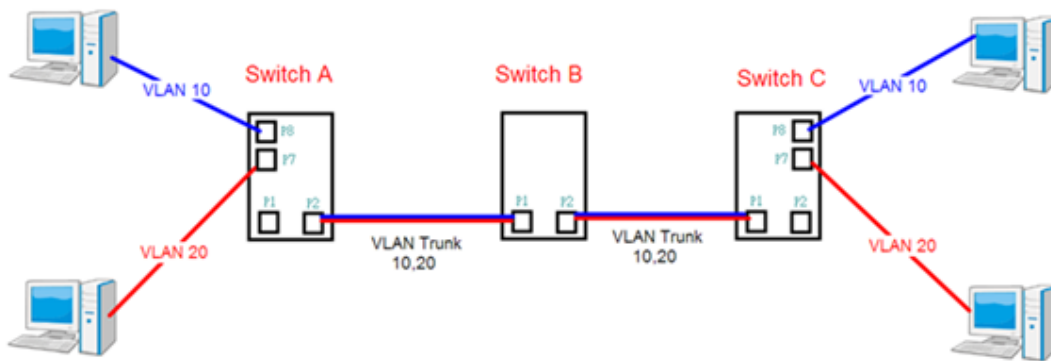


Figure 79 - VLAN 1Qtrunk Mode topology

For Switch B:

Port 1 = VLAN 1Qtrunk mode = tagged 10, 20

Port 2 = VLAN 1Qtrunk mode = tagged 10, 20

Below are the switch settings.

VLAN Membership Configuration

Refresh |<< >>|

Start from VLAN with entries per page.

Delete	VLAN ID	VLAN Name	Port Members																									
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
<input type="checkbox"/>	1	default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	10	VLAN10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	20	VLAN20	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add New VLAN

Save Reset

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN		Tx Tag
				Mode	ID	
*	<input type="text" value="C-port"/>	<input type="checkbox"/>	<input type="text" value="Tagged"/>	<input type="text" value="Specific"/>	<input type="text" value="1"/>	<input type="text" value="Tag_all"/>
1	C-port	<input type="checkbox"/>	Tagged	Specific	1	Tag_all
2	C-port	<input type="checkbox"/>	Tagged	Specific	1	Tag_all
3	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
4	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid

3) VLAN Hybrid Mode

For VLAN Hybrid Mode:

Port 1 VLAN Hybrid mode = untagged 10

Tagged 10, 20

Below are the switch settings.

VLAN Membership Configuration

Refresh |<< >>

Start from VLAN 1 with 20 entries per page.

Delete	VLAN ID	VLAN Name	Port Members																									
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
<input type="checkbox"/>	1	default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	10	VLAN10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	20	VLAN20	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add New VLAN

Save Reset

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN		Tx Tag
				Mode	ID	
*	<>	<input type="checkbox"/>	<>	<>	1	<>
1	C-port	<input type="checkbox"/>	All	Specific	1	Untag_all
2	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
3	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
4	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid

4) VLAN QinQ Mode

VLAN QinQ mode is usually adopted when there are unknown VLANs, as shown in the figure below.

VLAN "X" = Unknown VLAN

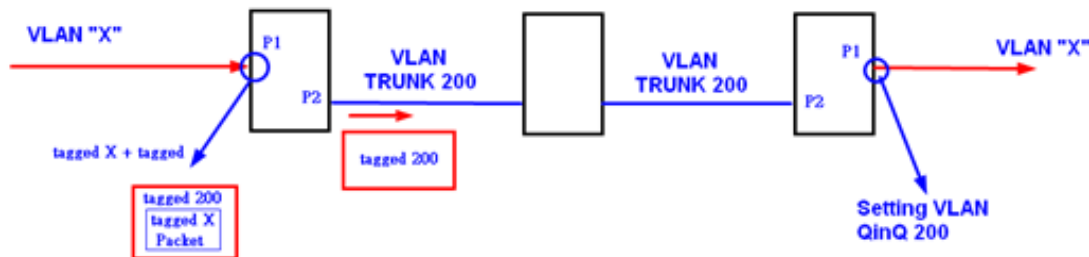


Figure 80 - VLAN QinQ Mode topology

5) iES26GF Port 1 VLAN Settings

VLAN Membership Configuration

Refresh |<< >>

Start from VLAN with entries per page.

Delete	VLAN ID	VLAN Name	Port Members																									
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
<input type="checkbox"/>	1	default	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	200	QinQ	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Add New VLAN

Save Reset

VLAN Port Configuration

Port	Port Type	Ingress Filtering	Frame Type	Port VLAN		Tx Tag
				Mode	ID	
*	<>	<input type="checkbox"/>	<>	<>	1	<>
1	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_all
2	C-port	<input type="checkbox"/>	Tagged	None	1	Tag_all
3	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
4	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid
5	Unaware	<input type="checkbox"/>	All	Specific	1	Untag_pvid

VLAN ID Settings

When setting the management VLAN, only the same VLAN ID port can be used to control the switch.

iES26GF VLAN Settings:

IP Configuration

Mode Router ▾

IP Interfaces

Delete	VLAN	IPv4 DHCP			IPv4	
		Enable	Fallback	Current Lease	Address	Mask Length
<input type="checkbox"/>	1	<input type="checkbox"/>	0		192.168.10.1	24

Add Interface

IP Routes

Delete	Network	Mask Length	Gateway	Next Hop VLAN
--------	---------	-------------	---------	---------------

Add Route

Save Reset

5.5.3 Private VLAN

5.5.3.1 Private VLAN Membership Configuration

The private VLAN membership configuration for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each private VLAN can be added or removed here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and private VLAN IDs can be identical. A port must be a member of both a VLAN and a private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and private VLAN 1.

A VLAN-unaware port can only be a member of one VLAN, but it can be a member of multiple private VLANs.

Auto-refresh ☐ Refresh

Private VLAN Membership Configuration

Delete	PVLAN ID	Port Members																									
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
<input type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add New Private VLAN

Save Reset

Figure 81 - Private VLAN Membership Configuration interface

The following table describes the labels for the **Private VLAN Membership Configuration** screen.

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Private VLAN ID	Indicates the ID of this private VLAN.
Port Members	A row of check boxes for each port is displayed for each private VLAN ID. You can check the box to include a port in a private VLAN. To remove or exclude the port from the private VLAN, make sure the box is unchecked. By default, no ports are members, and all boxes are unchecked.
Adding New Private VLAN	Click Add New Private VLAN to add a new private VLAN ID. An empty row is added to the table, and the private VLAN can be configured as needed. The allowed range for a private VLAN ID is the same as the switch port number range. Any values outside this range are not accepted, and a warning message appears. Click OK to discard the incorrect entry, or click Cancel to return to the editing and make a correction. The private VLAN is enabled when you click Save . The Delete button can be used to undo the addition of new private VLANs.
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.5.3.2 Port Isolation Configuration

This page is used for enabling or disabling port isolation on ports in a Private VLAN.

A port member of a VLAN can be isolated to other isolated ports on the same VLAN and Private VLAN.

Auto-refresh ☐

Port Isolation Configuration

Port Number																									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 82 - Port Isolation Configuration interface

The following table describes the labels for the **Port Isolation Configuration** screen.

Label	Description
Port Number	A check box is provided for each port of a private VLAN. When checked, port isolation is enabled for that port. When unchecked, port isolation is disabled for that port. By default, port isolation is disabled for all ports.
Refresh	Click Refresh to refresh the page immediately.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular Intervals.
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.6 SNMP

5.6.1 SNMP System Configuration

Configure the Simple Network Management Protocol (SNMP) on this page.

SNMP System Configuration

Mode	Enabled
Version	SNMP v2c
Read Community	public
Write Community	private
Engine ID	800007e5017f000001

Save Reset

Figure 83 - SNMP System Configuration interface

The following table describes the labels for the **SNMP System Configuration** screen.

Label	Description
Mode	Indicates existing SNMP mode. Possible modes include: Enabled: enable SNMP mode Disabled: disable SNMP mode
Version	Indicates the supported SNMP version. Possible versions include: SNMP v1: supports SNMP version 1. SNMP v2c: supports SNMP version 2c. SNMP v3: supports SNMP version 3.
Read Community	Indicates the read community string to permit access to SNMP agent. The allowed string length is 0 to 255, and only ASCII characters from 33 to 126 are allowed. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 uses USM for authentication and privacy and the community string will be associated with SNMPv3 community table.
Write Community	Indicates the write community string to permit access to SNMP agent. The allowed string length is 0 to 255, and only ASCII characters from 33 to 126 are allowed. The field only suits to SNMPv1 and SNMPv2c. SNMPv3 uses USM for authentication and privacy and the community string will be associated with SNMPv3 community table.
Engine ID	Indicates the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-F's are not allowed. Change of the Engine ID will clear all original local users.

5.6.2 SNMP Trap Configuration

Configure SNMP Trap on this page.

SNMP Trap Configuration

Trap Mode	Trap Version	Trap Community	Trap Destination Address	Trap Destination IPv6 Address	Trap Probe Security Engine ID	Trap Security Engine ID	Trap Security Name
Disabled	SNMP v1	public			Enabled	Probe Fail	None
Disabled	SNMP v1	public			Enabled	Probe Fail	None
Disabled	SNMP v1	public			Enabled	Probe Fail	None
Disabled	SNMP v1	public			Enabled	Probe Fail	None
Disabled	SNMP v1	public			Enabled	Probe Fail	None

Save Reset

Figure 84 - SNMP Trap Configuration interface

The following table describes the labels for the **SNMP Trap Configuration** screen.

Label	Description
Trap Mode	Indicates the trap destination mode operation. Possible modes are: Enabled: Enable SNMP trap mode operation. Disabled: Disable SNMP trap mode operation.
Trap Version	Indicates the supported SNMP trap version. Possible versions include: SNMP v1: supports SNMP trap version 1 SNMP v2c: supports SNMP trap version 2c SNMP v3: supports SNMP trap version 3
Trap Community	Indicates the community access string when sending SNMP trap packets. The allowed string length is 0 to 255, and only ASCII characters from 33 to 126 are allowed.
Trap Destination Address	Indicates the SNMP trap destination address. It allows a valid IP address in dotted decimal notation ('x.y.z.w').
Trap Destination IPv6 Address	Indicates the Trap Destination IPv6 Address . It allows a valid IP address in dotted decimal notation ('x.y.z.w').
Trap Probe Security Engine ID	Indicates the SNMP trap probe security engine ID mode of operation. Possible values are: Enabled: Enable SNMP trap probe security engine ID mode of operation. Disabled: Disable SNMP trap probe security engine ID mode of operation.
Trap Security Engine ID	Indicates the SNMP trap security engine ID. SNMPv3 sends traps and informs using USM for authentication and privacy. A unique engine ID for these traps and informs is needed. When "Trap Probe Security Engine ID" is enabled, the ID will be probed automatically. Otherwise, the ID specified in this field is used. The string must contain an even number (in hexadecimal format) with number of digits between 10 and 64, but all-zeroes and all-F's are not allowed.
Trap Security name	Indicates the SNMP trap security name. SNMPv3 traps and informs using USM for authentication and privacy. A unique security name is needed when traps and informs are enabled.
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.6.3 SNMPv3 Communities Configuration

This page allows you to configure SNMPv3 community table. The entry index key is **Community**.

SNMPv3 Community Configuration

Delete	Community	Source IP	Source Mask
<input type="checkbox"/>	public	0.0.0.0	0.0.0.0
<input type="checkbox"/>	private	0.0.0.0	0.0.0.0

Figure 85 - SNMPv3 Community Configuration interface

The following table describes the labels for the **SNMPv3 Community Configuration** screen.

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Community	Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
Source IP	Indicates the SNMP source address.
Source Mask	Indicates the SNMP source address mask.
Add New Entry	Click to add a new community configuration.
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.6.4 SNMP Users Configuration

This page allows you to configure SNMPv3 user table. The entry index keys are **Engine ID** and **User Name**.

SNMPv3 User Configuration

Delete	Engine ID	User Name	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
<input type="checkbox"/>	800007e5017f000001	default_user	NoAuth, NoPriv	None	None	None	None
<input type="button" value="Add New Entry"/> <input type="button" value="Save"/> <input type="button" value="Reset"/>							

Figure 86 - SNMPv3 User Configuration

The following table describes the labels for the **SNMPv3 User Configuration** screen.

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Engine ID	An octet string identifying the engine ID that this entry should belong to. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-F's are not allowed. The SNMPv3 architecture uses User-based Security Model (USM) for message security and View-based Access Control Model (VACM) for access control. For the USM entry, the <code>usmUserEngineID</code> and <code>usmUserName</code> are the entry keys. In a simple agent, <code>usmUserEngineID</code> is always that agent's own <code>snmpEngineID</code> value. The value can also take the value of the <code>snmpEngineID</code> of a remote SNMP engine with which this user can communicate. In other words, if user engine ID is the same as system engine ID, then it is local user; otherwise it's remote user.
User Name	A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
Security Level	Indicates the security model that this entry should belong to. Possible security models include: NoAuth, NoPriv: no authentication and none privacy Auth, NoPriv: Authentication and no privacy Auth, Priv: Authentication and privacy The value of security level cannot be modified if the entry already exists, which means the value must be set correctly at the time of entry creation.
Authentication Protocol	Indicates the authentication protocol that this entry should belong to. Possible authentication protocols include: None: no authentication protocol MD5: an optional flag for indicating that this user is using MD5 authentication protocol SHA: an optional flag to indicate that this user is using SHA authentication protocol The value of security level cannot be modified if the entry already exists, which means the value must be set correctly at the time of entry creation.
Authentication Password	A string identifying the authentication pass phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40. Only ASCII characters from 33 to 126 are allowed.
Privacy Protocol	Indicates the privacy protocol that this entry should belong to. Possible privacy protocols include: None: no privacy protocol DES: an optional flag indicating that this user is using DES authentication protocol
Privacy Password	A string identifying the privacy pass phrase. The allowed string length is 8 to 32 and only ASCII characters from 33 to 126 are allowed.

5.6.5 SNMP Group Configuration

This page allows you to configure SNMPv3 group table.

SNMPv3 Group Configuration

Delete	Security Model	Security Name	Group Name
<input type="checkbox"/>	v1	public	default_ro_group
<input type="checkbox"/>	v1	private	default_rw_group
<input type="checkbox"/>	v2c	public	default_ro_group
<input type="checkbox"/>	v2c	private	default_rw_group
<input type="checkbox"/>	usm	default_user	default_rw_group

Figure 87 - SNMPv3 Group Configuration interface

The following table describes the labels for the **SNMPv3 Group Configuration** screen.

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Security Model	Indicates the security model that this entry should belong to. Possible security models included: v1 : Reserved for SNMPv1. v2c : Reserved for SNMPv2c. usm : User-based Security Model (USM).
Security Name	A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
Add New Entry	Click Add New Entry to add a new group configuration.
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.6.6 SNMP View Configuration

This page allows you to configure SNMPv3 view table. The entry index keys are **View Name** and **OID Subtree**.

SNMPv3 View Configuration

Delete	View Name	View Type	OID Subtree
<input type="checkbox"/>	default_view	included ▼	.1

Figure 88 - SNMPv3 View Configuration interface

The following table describes the labels for the **SNMPv3 View Configuration** screen.

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
View Name	A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
View Type	Indicates the view type that this entry should belong to. Possible view types include: Included: an optional flag to indicate that this view subtree should be included. Excluded: An optional flag to indicate that this view subtree should be excluded. Generally, if an entry's view type is Excluded , it should exist in another entry whose view type is Included , and its OID subtree oversteps the Excluded entry.
OID Subtree	The OID defining the root of the subtree to be added to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk (*).
Add New Entry	Click Add New Entry to add a new view configuration.
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.6.7 SNMP Access Configuration

This page allows you to configure SNMPv3 access table. The entry index keys are **Group Name**, **Security Model**, and **Security Level**.

SNMPv3 Access Configuration

Delete	Group Name	Security Model	Security Level	Read View Name	Write View Name
<input type="checkbox"/>	default_ro_group	any	NoAuth, NoPriv	default_view ▼	None ▼
<input type="checkbox"/>	default_rw_group	any	NoAuth, NoPriv	default_view ▼	default_view ▼

Figure 89 - SNMPv3 Access Configuration interface

The following table describes the labels for the **SNMPv3 Community Configuration** screen.

Label	Description
Delete	Check to delete the entry. It will be deleted during the next save.
Group Name	A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and only ASCII characters from 33 to 126 are allowed.
Security Model	Indicates the security model that this entry should belong to. Possible security models include: any : Accepted any security model (v1 v2c usm). v1 : Reserved for SNMPv1. v2c : Reserved for SNMPv2c. usm : User-based Security Model (USM).
Security Level	Indicates the security model that this entry should belong to. Possible security models include: NoAuth, NoPriv : no authentication and no privacy Auth, NoPriv : Authentication and no privacy Auth, Priv : Authentication and privacy
Read View Name	The names of the MIB view define the MIB objects for which this request may request the current values. The options to be selected from a drop-down list are None and default_view .
Write View Name	The names of the MIB view defining the MIB objects for which this request may potentially SET new values. The options to be selected from a drop-down list are None and default_view .

5.7 Traffic Prioritization

5.7.1 Storm Control

This page allows you to configure the storm control settings for all switch ports. There is a storm rate control for unicast, multicast (unknown), and broadcast ingress traffic.

Storm Control Configuration

Frame Type	Enable	Rate (pps)
Unicast	<input type="checkbox"/>	1
Multicast	<input type="checkbox"/>	1
Broadcast	<input type="checkbox"/>	1

Save Reset

Figure 90 - Storm Control Configuration interface

The following table describes the labels for the **Storm Control Configuration** screen.

Label	Description
Frame Type	There are three types of frame type listed here: unicast, broadcast, or unknown.
Enable	Check this box to enable the storm control status for the given frame type and port.
Rate	Controls the rate for the storm control. The rate unit is packets per second (pps). Valid values are: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K or 1024K.
Save	Click Save to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.7.2 Port Classification

QoS is an acronym for Quality of Service. This is a method for achieving efficient bandwidth utilization between individual applications or protocols. This page allows you to configure the basic [QoS](#) Ingress Classification settings for all switch ports.

QoS Ingress Port Classification

Port	QoS class	DP level	PCP	DEI	Tag Class.	DSCP Based
*	<>	<>	<>	<>		<input type="checkbox"/>
1	0	0	0	0	Disabled	<input type="checkbox"/>
2	0	0	0	0	Disabled	<input type="checkbox"/>
3	0	0	0	0	Disabled	<input type="checkbox"/>
4	0	0	0	0	Disabled	<input type="checkbox"/>
5	0	0	0	0	Disabled	<input type="checkbox"/>
6	0	0	0	0	Disabled	<input type="checkbox"/>
7	0	0	0	0	Disabled	<input type="checkbox"/>
8	0	0	0	0	Disabled	<input type="checkbox"/>

Figure 91 - QoS Ingress Port Classification interface

The following table describes the labels for the **QoS Ingress Port Classification** screen.

Label	Description
Port	The port number for which the configuration below applies
QoS Class	<p>It controls the default QoS class All frames are classified to a QoS class. There is a one to one mapping between QoS class, queue, and priority. A QoS class of 0 (zero) has the lowest priority.</p> <ul style="list-style-type: none"> If the port is VLAN aware and the frame is tagged, then the frame is classified to a QoS class that is based on the PCP value in the tag as shown below. Otherwise the frame is classified to the default QoS class. PCP value: 0 1 2 3 4 5 6 7; QoS class: 1 0 2 3 4 5 6 7 If the port is VLAN aware, the frame is tagged, and Tag Class is enabled, then the frame is classified to a QoS class that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default QoS class. <p>The classified QoS class can be overruled by a QCL entry. Note: if the default QoS class has been dynamically changed, then the actual default QoS class is shown in parentheses after the configured default QoS class.</p>
DP level	<p>Controls the default Drop Precedence Level All frames are classified to a DP Level.</p> <ul style="list-style-type: none"> If the port is VLAN aware and the frame is tagged, then the frame is classified to a DP level that is equal to the DEI value in the tag. Otherwise the frame is classified to the default DP level. If the port is VLAN aware, the frame is tagged, and Tag Class is enabled, then the frame is classified to a DP level that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DP level. <p>The classified DP level can be overruled by a QCL entry.</p>
PCP	<p>Controls the default PCP value All frames are classified to a PCP value.</p> <ul style="list-style-type: none"> If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value.
DEI	<p>Controls the default DEI value All frames are classified to a DEI value.</p> <ul style="list-style-type: none"> If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value.
Tag Class	<p>Shows the classification mode for tagged frames on this port.</p> <ul style="list-style-type: none"> Disabled: Use default QoS class and DP level for tagged frames. Enabled: Use mapped versions of PCP and DEI for tagged frames. <p>Click on the mode to configure the mode and/or mapping. Note: this setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN-unaware ports are always classified to the default QoS class and DP level.</p>
DSCP Based	Add a check mark to enable DSCP Based QoS Ingress Port Classification
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

Note: DSCP stands for Differentiated Services (DiffServ) Code Point. The six most significant bits of the DiffServ field are called DSCP.

5.7.3 Port Tag Remarking

This page provides an overview of QoS Egress Port Tag Remarking for all switch ports.

QoS Egress Port Tag Remarking

Port	Mode
1	Classified
2	Classified
3	Classified
4	Classified
5	Classified
6	Classified
7	Classified
8	Classified
9	Classified
10	Classified
11	Classified
12	Classified
13	Classified
14	Classified
15	Classified
16	Classified
17	Classified
18	Classified
19	Classified
20	Classified
21	Classified
22	Classified
23	Classified
24	Classified
25	Classified
26	Classified

Figure 92 - QoS Egress Port Tag Remarking interface

The following table describes the labels for the **QoS Egress Port Tag Remarking** screen.

Label	Description
Port	The switch port number to which the following settings will be applied. Click on the port number to configure tag remarking.
Mode	Shows the tag remarking mode for this port: Classified: use classified PCP/DEI values. Default: uses default PCP/DEI values. Mapped: uses mapped versions of QoS class and DP level.

5.7.4 Port DSCP

This page allows you to configure basic QoS Port DSCP Configuration settings for all switch ports.

QoS Port DSCP Configuration

Port	Ingress		Egress
	Translate	Classify	Rewrite
*	<input type="checkbox"/>	<> ▼	<> ▼
1	<input type="checkbox"/>	Disable ▼	Disable ▼
2	<input type="checkbox"/>	Disable ▼	Disable ▼
3	<input type="checkbox"/>	Disable ▼	Disable ▼
4	<input type="checkbox"/>	Disable ▼	Disable ▼
5	<input type="checkbox"/>	Disable ▼	Disable ▼
6	<input type="checkbox"/>	Disable ▼	Disable ▼
7	<input type="checkbox"/>	Disable ▼	Disable ▼
8	<input type="checkbox"/>	Disable ▼	Disable ▼
9	<input type="checkbox"/>	Disable ▼	Disable ▼
10	<input type="checkbox"/>	Disable ▼	Disable ▼

Figure 93 - QoS Port DSCP Configuration interface

The following table describes the labels for the **QoS Port DSCP Configuration** screen.

Label	Description
Port	Shows the list of ports for which you can configure DSCP Ingress and Egress settings.
Ingress	<p>Ingress settings allow you to change ingress translation and classification settings for individual ports.</p> <p>There are two configuration parameters available in Ingress:</p> <ol style="list-style-type: none"> Translate Classify
1. Translate	Check to enable ingress translation
2. Classify	<p>Classification has 4 different values.</p> <p>Disable: no Ingress DSCP classification</p> <p>DSCP=0: choose if incoming (or translated if enabled) DSCP is 0.</p> <p>Selected: chooses only selected DSCP whose classification is enabled as specified in DSCP Translation window for the specific DSCP.</p> <p>All: choose to select all DSCP</p>
Egress Rewrite	<p>Port egress rewriting can be one of the following options:</p> <p>Disable: no Egress Rewrite</p> <p>Enable: rewrite enabled without remapping.</p> <p>Remap DP Unaware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table.</p> <p>Remap DP Aware: DSCP from analyzer is remapped and frame is remarked with remapped DSCP value. Depending on the DP level of the frame, the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table</p>
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.7.5 Port Policing

This page allows you to configure Policers settings for all switch ports.

QoS Ingress Port Policers

Port	Enabled	Rate	Unit	Flow Control
*	<input type="checkbox"/>	500	<> ▾	<input type="checkbox"/>
1	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>
2	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>
3	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>
4	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>
5	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>
6	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>
7	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>
8	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>
9	<input type="checkbox"/>	500	kpbs ▾	<input type="checkbox"/>

Figure 94 - QoS Ingress Port Policers interface

The following table describes the labels for the **QoS Ingress Port Policers** screen

Label	Description
Port	The port number for which the configuration below applies.
Enable	Check to enable the policer for individual switch ports.
Rate	Configures the rate of each policer. The default value is 500 . This value is restricted to 100 to 1000000 when the Unit is kpbs or fps , and to 1 to 3300 when the Unit is Mbps or kfps .
Unit	Configures the unit of measurement for each policer rate as kpbs , Mbps , fps , or kfps . The default value is kpbs .
Flow Control	If flow control is enabled and the port is in flow control mode, then pause frames are sent instead of discarding frames.
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.7.6 Queue Policing

This page allows you to configure Queue Policer settings for all switch ports.

QoS Ingress Queue Policers

Port	Queue 0 Enable	Queue 1 Enable	Queue 2 Enable	Queue 3 Enable	Queue 4 Enable	Queue 5 Enable	Queue 6 Enable	Queue 7 Enable
*	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 95 - QoS Ingress Queue Policers interface

The following table describes the labels for the **QoS Ingress Queue Policers** screen.

Label	Description
Port	The port number for which the configuration below applies.
Enable(E)	Check to enable queue policer for individual switch ports
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.7.7 Port Scheduler

This page provides an overview of QoS Egress Port Schedulers for all switch ports.

QoS Egress Port Schedulers

Port	Mode	Weight					
		Q0	Q1	Q2	Q3	Q4	Q5
1	Strict Priority	-	-	-	-	-	-
2	Strict Priority	-	-	-	-	-	-
3	Strict Priority	-	-	-	-	-	-
4	Strict Priority	-	-	-	-	-	-
5	Strict Priority	-	-	-	-	-	-
6	Strict Priority	-	-	-	-	-	-
7	Strict Priority	-	-	-	-	-	-
8	Strict Priority	-	-	-	-	-	-
9	Strict Priority	-	-	-	-	-	-

Figure 96 - QoS Egress Port Schedulers interface

The following table describes the labels for the **QoS Egress Port Schedulers** screen.

Label	Description
Port	The logical port for the settings contained in the same row. Click on the port number to configure the schedulers. Details for configuration can be found in the QoS Egress Port Scheduler and Shapers section.
Mode	Shows the scheduling mode for this port.
Qn	Shows the weight for this queue and port.

5.7.7.1 QoS Egress Port Scheduler and Shapers

This page allows you to configure Scheduler and Shapers for a specific port. This is accessed by selecting specific port on the **Port Scheduler** or **Port Shaping** screens.

1) Strict Priority

Port 1

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode: **Strict Priority**

Queue Shaper			
Enable	Rate	Unit	Excess
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>
<input type="checkbox"/>	500	kbps	<input type="checkbox"/>

STRICT

Port Shaper		
Enable	Rate	Unit
<input type="checkbox"/>	500	kbps

Save Reset Cancel

Figure 97 - QoS Egress Port Scheduler and Shapers Port 1

This table describes the labels for the **QoS Egress Port Scheduler and Shapers Policers** screen.

Label	Description
Scheduler Mode	Controls whether the scheduler mode is Strict Priority or Weighted on this switch port
Queue Shaper Enable	Check to enable queue shaper for individual switch ports.
Queue Shaper Rate	Configures the rate of each queue shaper. The default value is 500 . This value is restricted to 100 to 1000000 when the Unit is kbps , and it is restricted to 1 to 3300 when the Unit is Mbps .
Queues Shaper Unit	Configures the rate for each queue shaper. The default value is 500 . This value is restricted to 100 to 1000000 when the Unit is kbps , and it is restricted to 1 to 3300 when the Unit is Mbps .
Queue Shaper Excess	Allows the queue to use excess bandwidth.
Port Shaper Enable	Check to enable port shaper for individual switch ports.
Port Shaper Rate	Configures the rate of each port shaper. The default value is 500 . This value is restricted to 100 to 1000000 when the Unit is kbps , and it is restricted to 1 to 3300 when the Unit is Mbps .
Port Shaper Unit	Configures the unit of measurement for each port shaper rate as kbps or M bps . The default value is kbps .
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previous values.
Cancel	Click Cancel to undo any changes made locally and return to the previous page.

2) Weighted

Port 1 ▾

QoS Egress Port Scheduler and Shapers Port 1

Scheduler Mode Weighted ▾

Queue Shaper				Queue Scheduler		Port Shaper		
Enable	Rate	Unit	Excess	Weight	Percent	Enable	Rate	Unit
<input checked="" type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	17	17%	D W R R S T R I C T	<input checked="" type="checkbox"/>	500 kbps ▾
<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	17	17%			
<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	17	17%			
<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	17	17%			
<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	17	17%			
<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	17	17%			
<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	17	17%			
<input type="checkbox"/>	500	kbps ▾	<input type="checkbox"/>	17	17%			

Save Reset Cancel

Figure 98 - QoS Egress Port Scheduler and Shapers Port 1

This table describes the labels for the **QoS Egress Port Scheduler and Shapers Port 1** screen.

Label	Description
Scheduler Mode	Controls whether the scheduler mode is Strict Priority or Weighted on this switch port.
Queue Shaper Enable	Check to enable queue shaper for individual switch ports.
Queue Shaper Rate	Configures the rate of each queue shaper. The default value is 500 . This value is restricted to 100 to 1000000 when the Unit is kbps , and it is restricted to 1 to 3300 when the Unit is Mbps .
Queues Shaper Unit	Configures the rate of each queue shaper. The default value is 500 . This value is restricted to 100 to 1000000 when the Unit is kbps , and it is restricted to 1 to 3300 when the Unit is Mbps .
Queue Shaper Excess	Allows the queue to use excess bandwidth
Queue Scheduler Weight	Configures the weight of each queue. The default value is 17 . This value is restricted to 1 to 100. This parameter is only shown if Scheduler Mode is set to Weighted .
Queue Scheduler Percent	Shows the weight of the queue in percentage. This parameter is only shown if Scheduler Mode is set to Weighted .
Port Shaper Enable	Check to enable port shaper for individual switch ports

Port Shaper Rate	Configures the rate of each port shaper. The default value is 500 . This value is restricted to 100 to 1000000 when the Unit is kbps , and it is restricted to 1 to 3300 when the Unit is Mbps .
Port Shaper Unit	Configures the unit of measurement for each port shaper rate as kbps or M bps . The default value is kbps .
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.
Cancel	Click Cancel to undo any changes made locally and return to the previous page.

3) Port Shaping

This page provides an overview of QoS Egress Port Shapers for all switch ports.

QoS Egress Port Shapers

Port	Shapers								
	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Port
1	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
2	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
3	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
4	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
5	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
6	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
7	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
8	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled
9	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled	disabled

Figure 99 - QoS Egress Port Shapers interface

The following table describes the labels for the **QoS Egress Port Shapers** screen.

Label	Description
Port	The switch port number to which the following settings will be applied. Click on the port number to configure the shapers. Details for configuration can be found in the QoS Egress Port Scheduler and Shapers section.
Qn	Shows disabled or actual port shaper rate - e.g. 800 Mbps

5.7.8 DSCP Based QoS

This page allows you to configure basic QoS DSCP-based QoS Ingress Classification settings for all switches.

DSCP-Based QoS Ingress Classification

DSCP	Trust	QoS Class	DPL
*	<input type="checkbox"/>	<> v	<> v
0 (BE)	<input type="checkbox"/>	0 v	0 v
1	<input type="checkbox"/>	0 v	0 v
2	<input type="checkbox"/>	0 v	0 v
3	<input type="checkbox"/>	0 v	0 v
4	<input type="checkbox"/>	0 v	0 v
5	<input type="checkbox"/>	0 v	0 v
6	<input type="checkbox"/>	0 v	0 v
7	<input type="checkbox"/>	0 v	0 v
8 (CS1)	<input type="checkbox"/>	0 v	0 v
9	<input type="checkbox"/>	0 v	0 v
10 (AF11)	<input type="checkbox"/>	0 v	0 v
11	<input type="checkbox"/>	0 v	0 v
12 (AF12)	<input type="checkbox"/>	0 v	0 v

Figure 100 - DSCP-Based QoS Ingress Classification interface

The following table describes the labels for the **DSCP-Based QoS Ingress Classification** screen.

Label	Description
DSCP	Maximum number of supported DSCP values is 64
Trust	Check to trust a specific DSCP value. Only frames with trusted DSCP values are mapped to a specific QoS class and drop precedence level. Frames with untrusted DSCP values are treated as a non-IP frame.
QoS Class	QoS class value can be any number from 0-7.
DPL	Drop Precedence Level (0-1)
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.7.9 DSCP Translation

This page allows you to configure basic QoS DSCP translation settings for all switches. DSCP translation can be done in **Ingress** or **Egress**.

DSCP Translation

DSCP	Ingress		Egress	
	Translate	Classify	Remap DP0	Remap DP1
*	<> ▾	<input type="checkbox"/>	<> ▾	<> ▾
0 (BE)	0 (BE) ▾	<input type="checkbox"/>	0 (BE) ▾	0 (BE) ▾
1	1 ▾	<input type="checkbox"/>	1 ▾	1 ▾
2	2 ▾	<input type="checkbox"/>	2 ▾	2 ▾
3	3 ▾	<input type="checkbox"/>	3 ▾	3 ▾
4	4 ▾	<input type="checkbox"/>	4 ▾	4 ▾
5	5 ▾	<input type="checkbox"/>	5 ▾	5 ▾
6	6 ▾	<input type="checkbox"/>	6 ▾	6 ▾
7	7 ▾	<input type="checkbox"/>	7 ▾	7 ▾
8 (CS1)	8 (CS1) ▾	<input type="checkbox"/>	8 (CS1) ▾	8 (CS1) ▾
9	9 ▾	<input type="checkbox"/>	9 ▾	9 ▾
10 (AF11)	10 (AF11) ▾	<input type="checkbox"/>	10 (AF11) ▾	10 (AF11) ▾
11	11 ▾	<input type="checkbox"/>	11 ▾	11 ▾
12 (AF12)	12 (AF12) ▾	<input type="checkbox"/>	12 (AF12) ▾	12 (AF12) ▾
13	13 ▾	<input type="checkbox"/>	13 ▾	13 ▾
14 (AF13)	14 (AF13) ▾	<input type="checkbox"/>	14 (AF13) ▾	14 (AF13) ▾
15	15 ▾	<input type="checkbox"/>	15 ▾	15 ▾
16 (CS2)	16 (CS2) ▾	<input type="checkbox"/>	16 (CS2) ▾	16 (CS2) ▾

Figure 101 - DSCP Translation interface

The following table describes the labels for the **DSCP Translation** screen.

Label	Description
DSCP	Maximum number of supported DSCP values is 64 and valid DSCP values range is from 0 to 63.
Ingress	Ingress DSCP can be first translated to new DSCP before using the DSCP for QoS class and DPL map. There are two configuration parameters for DSCP Translation - Translate: DSCP can be translated to any of (0-63) DSCP values. Choose one of them from the drop-down list. Classify: check to enable Ingress classification
Egress	There are the following configurable parameters for Egress side - 1. Remap DP0 Controls the remapping for frames with DP level 0. 2. Remap DP1 Controls the remapping for frames with DP level 1. Remap DP0: Select the DSCP value from the drop-down list. DSCP value ranges from 0 to 63. Remap DP1: Select the DSCP value from the drop-down list. DSCP value ranges from 0 to 63.
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.7.10 DSCP Classification

This page allows you to configure the mapping of QoS class to DSCP value.

DSCP Classification

QoS Class	DPL	DSCP
*	*	<>
0	0	0 (BE)
0	1	0 (BE)
1	0	0 (BE)
1	1	0 (BE)
2	0	0 (BE)
2	1	0 (BE)
3	0	0 (BE)
3	1	0 (BE)
4	0	0 (BE)
4	1	0 (BE)
5	0	0 (BE)
5	1	0 (BE)
6	0	0 (BE)
6	1	0 (BE)
7	0	0 (BE)
7	1	0 (BE)

Save

Reset

Figure 102 - DSCP Classification interface

The following table describes the labels for the **DSCP Classification** screen.

Label	Description
QoS Class	Actual QoS class
DPL	Drop Precedence Level. For every QoS Class, there is a row with DPL=0 and another one with DPL=1.
DSCP	Select the classified DSCP value (0-63) from the drop-down list.
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.7.11 QoS Control List

This page shows the QoS Control List ([OCL](#)), which is made up of the [QCEs](#). Each row describes a QCE that is defined. The maximum number of QCEs is 256 on each switch. Click on the lowest plus sign to add a new QCE to the list.

QoS Control List Configuration

QCE#	Port	Frame Type	SMAC	DMAC	VID	PCP	DEI	Action		
								Class	DPL	DSCP



Figure 103 - QoS Control List Configuration interface

To see the QCE Configuration dialog box, click on the + sign (marked by a rectangle outlined in red)

QCE Configuration

Port Members																									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Key Parameters

Tag	Any
VID	Any
PCP	Any
DEI	Any
SMAC	Any
DMAC Type	Any
Frame Type	Any

Action Parameters

Class	0
DPL	Default
DSCP	Default

Figure 104 - QCE Configuration interface

The following table describes the labels for the **QCE Configuration** screen.

Label	Description
Port Members	Check to include the port in the QCL entry. By default, all ports are included.
Key Parameters	<p>Key configurations include:</p> <p>Tag: value of tag; it can be Any, Untag, or Tag.</p> <p>VID: valid value of VLAN ID, can be any value from 1 to 4095 Any: user can enter either a specific value or a range of VIDs.</p> <p>PCP: Priority Code Point, can be specific numbers (0, 1, 2, 3, 4, 5, 6, 7), a range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or Any</p> <p>DEI: Drop Eligible Indicator, can be 0, 1 or Any</p> <p>SMAC: Source MAC Address, can be specific (xx-xx-xx, 24 MS bits OUI) or Any</p> <p>DMAC Type: Destination MAC type, can be unicast (UC), multicast(MC), broadcast (BC) or Any</p> <p>Frame Type can be Any Ethernet LLC SNAP IPv4 or IPv6</p> <p>Note: all frame types are explained below.</p>
Any	Allow all types of frames
Ethernet	Valid Ethernet values can range from 0x600 to 0xFFFF or Any but excluding 0x800(IPv4) and 0x86DD(IPv6). The default value is Any .
LLC	<p>SSAP Address: valid SSAP (Source Service Access Point) values can range from 0x00 to 0xFF or Any. The default value is Any.</p> <p>DSAP Address: valid DSAP (Destination Service Access Point) values can range from 0x00 to 0xFF or Any. The default value is Any.</p> <p>Control Valid Control: valid values can range from 0x00 to 0xFF or Any. The default value is Any.</p>
SNAP	PID: valid PID (a.k.a. Ethernet type); its values can range from 0x00 to 0xFFFF or Any . The default value is Any .
IPv4	<p>Protocol IP Protocol Number: (0-255, TCP or UDP) or Any</p> <p>Source IP: specific Source IP address in value/mask format or Any. IP and mask are in the format of x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255. When the mask is converted to a 32-bit binary string and read from left to right, all bits following the first zero must also be zero.</p> <p>IP Fragment: Ipv4 frame fragmented options include yes, no, and any.</p> <p>DSCP (Differentiated Code Point): can be a specific value, a range, or Any. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.</p>
IPv6	<p>Protocol IP protocol number: Other (0-255), TCP, UDP, or Any</p> <p>Source IP IPv6 source address: (a.b.c.d) or Any, 32 LS bits</p> <p>DSCP (Differentiated Code Point): can be a specific value, a range, or Any. DSCP values are in the range 0-63 including BE, CS1-CS7, EF or AF11-AF43.</p>
Action Parameters	<p>Class QoS class: (0-7) or Default</p> <p>Valid Drop Precedence Level value can be (0-3) or Default.</p> <p>Valid DSCP value can be (0-63, BE, CS1-CS7, EF or AF11-AF43) or Default. Default means that the default classified value is not modified by this QCE.</p>

5.7.12 QoS Statistics

This page provides the statistics of individual queues for all switch ports.

Queuing Counters

Auto-refresh ☐ Refresh Clear

Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	10633	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1039
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 105 - Queuing Counters

The following table describes the labels for the **Queuing Counters** screen.

Label	Description
Port	The logical port number for the statistics displayed. Click on the port number to see Detailed Port Statistics.
Qn	There are 8 QoS queues per port. Q0 is the lowest priority.
Rx / Tx	The number of received and transmitted packets per queue.
Refresh	Click Refresh to refresh the page immediately.
Clear	Click Clear all statistics counters.
Auto-refresh	Check Auto-refresh box to enable an automatic refresh of the page at regular intervals.

5.7.13 QCL Status

This page shows the QCL status for different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

Combined Auto-refresh ☐

QoS Control List Status

User	QCE#	Frame Type	Port	Action			Conflict
				Class	DPL	DSCP	
No entries							

Figure 106 - QoS Control List Status interface

The following table describes the labels for the **QoS Control List Status** screen.

Label	Description
User	Indicates the QCL user.
QCE#	Indicates the index of QCE.
Frame Type	Indicates the type of frame to look for incoming frames. Possible frame types are: Any : the QCE will match all frame type. Ethernet : Only Ethernet frames (with Ether Type 0x600-0xFFFF) are allowed. LLC : Only (LLC) frames are allowed. SNAP : Only (SNAP) frames are allowed. IPv4 : the QCE will match only IPV4 frames. IPv6 : the QCE will match only IPV6 frames.
Port	Indicates the list of ports configured with the QCE.
Action	Indicates the classification action taken on ingress frame if parameters configured are matched with the frame's content. There are three action fields: Class , DPL , and DSCP . Class : Classified QoS; if a frame matches the QCE, it will be put in the queue. DPL : Drop Precedence Level; if a frame matches the QCE, then DP level will be set to a value displayed under DPL column. DSCP : if a frame matches the QCE, then DSCP will be classified with the value displayed under DSCP column.
Conflict	Displays the conflict status of QCL entries. As hardware resources are shared by multiple applications, resources required to add a QCE may not be available. In that case, it shows conflict status as Yes , otherwise it is always No . Please note that conflict can be resolved by releasing the hardware resources required to add the QCL entry by pressing Resolve Conflict button.
QCL status	Select one of the following to be displayed: Combined : Show both static and conflict entries. Static : Show static entries. Conflict : Show conflict entries.
Clear	Click Clear to reset all statistics counters.
Auto-refresh	Check Auto-refresh box to enable an automatic refresh of the page at regular intervals.

5.8 Multicast

The Internet Group Management Protocol (IGMP) is used by IP hosts to register their dynamic multicast group membership. IGMP has 3 versions: IGMP v1, v2 and v3. For details, refer to RFC 1112, 2236 and 3376. IGMP Snooping improves the performance of networks that carry multicast traffic. It provides the ability to trim multicast traffic so that it travels only to its intended end destinations. This reduces the amount of traffic on the Ethernet LAN.

5.8.1 IGMP Snooping Basic Configuration

This page provides IGMP Snooping related configurations.

IGMP Snooping Configuration

Global Configuration	
Snooping Enabled	<input type="checkbox"/>
Unregistered IPMCv4 Flooding Enabled	<input checked="" type="checkbox"/>

Port Related Configuration

Port	Router Port	Fast Leave
*	<input type="checkbox"/>	<input type="checkbox"/>
1	<input type="checkbox"/>	<input type="checkbox"/>
2	<input type="checkbox"/>	<input type="checkbox"/>
3	<input type="checkbox"/>	<input type="checkbox"/>
4	<input type="checkbox"/>	<input type="checkbox"/>
5	<input type="checkbox"/>	<input type="checkbox"/>
6	<input type="checkbox"/>	<input type="checkbox"/>
7	<input type="checkbox"/>	<input type="checkbox"/>
8	<input type="checkbox"/>	<input type="checkbox"/>
9	<input type="checkbox"/>	<input type="checkbox"/>

Figure 107 - IGMP Snooping Configuration interface

The following table describes the labels for the **IGMP Snooping Configuration** screen.

Label	Description
Snooping Enabled	Check to enable global IGMP snooping
Unregistered IPMCv4 Flooding enabled	Check to enable unregistered IPMCv4 traffic flooding. The flooding control takes effect only when IGMP Snooping is enabled. When IGMP Snooping is disabled, unregistered IPMCv4 traffic flooding is always active despite this setting.
Router Port	Specifies which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP Snooping Querier. If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.
Fast Leave	Check to enable Fast Leave on the port
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.8.2 IGMP Snooping VLAN Configuration

Each page shows up to 99 entries from the VLAN table, with a default value of 20, selected by the **Entries Per Page** input field. When first visited, the web page will show the first 20 entries from the beginning of the VLAN Table. The first displayed will be the one with the lowest VLAN ID found in the VLAN Table.

The **VLAN** input field allows the user to select the starting point in the VLAN Table. Clicking **Refresh** will update the displayed table starting from that or the next closest VLAN Table match.

The **>>** will use the last entry of the currently displayed entry as a basis for the next lookup. When the end is reached, the text **No more entries** is shown in the displayed table. Use the **|<<** button to start over.

IGMP Snooping VLAN Configuration

Figure 108 - IGMP Snooping VLAN Configuration

The following table describes the labels for the **IGMP Snooping VLAN Configuration** screen.

Label	Description
Delete	Check to delete the entry. The designated entry will be deleted during the next save.
VLAN ID	The VLAN ID of the entry
Snooping Enabled	Check to enable IGMP snooping for individual VLAN. Up to 32 VLAN's can be selected.
IGMP Querier	<p>Enable the IGMP Querier in the VLAN.</p> <p>Defines the IPv4 address as source address used in IP header for IGMP Querier election.</p> <ul style="list-style-type: none"> When the Querier address is not set, system uses IPv4 management address of the IP interface associated with this VLAN. When the IPv4 management address is not set, the system uses the first available IPv4 management address. <p>Otherwise, the system uses a pre-defined value. By default, this value will be 192.0.2.1.</p>
Add New IGMP VLAN	Click to add new IGMP VLAN. Specify the VID and configure the new entry. Click Save . The specific IGMP VLAN starts working after the corresponding static VLAN is also created.
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.8.3 IGMP Snooping Status

This page provides IGMP snooping status.

Auto-refresh ☐

IGMP Snooping Status

Statistics

VLAN ID	Querier Version	Host Version	Querier Status	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
---------	-----------------	--------------	----------------	---------------------	------------------	---------------------	---------------------	---------------------	--------------------

Router Port

Port	Status
1	-
2	-
3	-
4	-
5	-
6	-
7	-
8	-
9	-
10	-
11	-
12	-
13	-
14	-
15	-
16	-
17	-
18	-

Figure 109 - IGMP Snooping Status

The following table describes the labels for the **IGMP Snooping Status** screen.

Label	Description
VLAN ID	The VLAN ID of the entry
Querier Version	Active Querier version
Host Version	Active Host version
Querier Status	Shows the Querier status as ACTIVE or DISABLE
Querier Transmitted	The number of transmitted Queries
Querier Received	The number of transmitted Queries
V1 Reports Received	The number of received V1 reports
V2 Reports Received	The number of received V2 reports
V3 Reports Received	The number of received V3 reports
V2 Leaves Received	The number of received V2 leave packets
Refresh	Click to refresh the page immediately
Clear	Clear all statistics counters
Auto-refresh	Check Auto-refresh box to enable an automatic refresh of the page at regular intervals.
Router Port	Port number on the switch
Router Port Status	It indicates whether a specific port is a router port or not.

5.8.4 IGMP Snooping Group Information

Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group.

Each page shows up to 99 entries from the IGMP Group table, by default being 20, selected through the **entries per page input** field. When first visited, the web page will show the first 20 entries from the beginning of the IGMP Group Table.

The **Start from VLAN** and **Groups** input fields allow the user to select the starting point in the IGMP Group Table.

Clicking **Refresh** will update the displayed table starting from that or the next closest IGMP Group Table match. In addition, the two input fields will—after clicking **Refresh**—assume the value of the first displayed entry, allowing for continuous refresh with the same start address.

The “>>” button will use the last entry of the currently displayed table as a basis for the next lookup. When the end is reached the text "No more entries" is shown in the displayed table. Use the “<<” button to start over.

IGMP Snooping Group Information

Auto-refresh ☐ Refresh |<< >>|

Start from VLAN and group address with entries per page.

		Port Members																									
VLAN ID	Groups	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
No more entries																											

Figure 110 - IGMP Snooping Group Information interface

The following table describes the labels for the **IGMP Snooping Group Information** screen.

Label	Description
VLAN ID	The VLAN ID of the group.
Groups	The group address of the group displayed.
Port Members	Selected ports under this group.

5.9 Security

5.9.1 Remote Control Security Configurations

Remote Control Security allows you to limit remote access to the management interface. When enabled, client requests which are not allowed will be rejected.

Remote Control Security Configuration

Mode Enable ▾

Delete Port IP Web Telnet SNMP

Add new entry Save Reset

Figure 111 - Remote Control Security Configuration interface

The following table describes the labels for the **Remote Control Security Configuration** screen

Label	Description
Port	Port number of the remote client
IP	IP address of the remote client. 0.0.0.0 means any IP.
Web	Enables management via a Web interface
Telnet	Enables management via a Telnet interface
SNMP	Enables management via a SNMP interface
Delete	Check to delete entries
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.9.2 Device Binding

This page provides device binding configurations. Device binding is a powerful way to monitor devices and network security.

5.9.2.1 Configuration

Device Binding

Function State Enable ▾

Port	Mode	Alive Check		Stream Check		DDOS Prevention		Device	
		Active	Status	Active	Status	Active	Status	IP Address	MAC Address
1	Scan ▾	<input type="checkbox"/>	---	<input type="checkbox"/>	---	<input type="checkbox"/>	---	0.0.0.0	00-00-00-00-0
2	Binding ▾	<input type="checkbox"/>	---	<input type="checkbox"/>	---	<input type="checkbox"/>	---	0.0.0.0	00-00-00-00-0
3	Shutdown ▾	<input type="checkbox"/>	---	<input type="checkbox"/>	---	<input type="checkbox"/>	---	0.0.0.0	00-00-00-00-0
4	--- ▾	<input type="checkbox"/>	---	<input type="checkbox"/>	---	<input type="checkbox"/>	---	0.0.0.0	00-00-00-00-0
5	--- ▾	<input type="checkbox"/>	---	<input type="checkbox"/>	---	<input type="checkbox"/>	---	0.0.0.0	00-00-00-00-0

Figure 112 - Device Binding interface

The following table describes the labels for the **Device Binding** screen.

Label	Description
Mode	Indicates the device binding operation for each port. Possible modes are: ---: disable Scan : scans IP/MAC automatically, but no binding function Binding : enables binding. Under this mode, any IP/MAC that does not match the entry will not be allowed to access the network. Shutdown : shuts down the port (No Link)
Alive Check Active	Check to enable alive check. When enabled, switch will ping the device continually.
Alive Check Status	Indicates alive check status. Possible statuses are: ---: disable Got Reply : receive ping reply from device, meaning the device is still alive Lost Reply : not receiving ping reply from device, meaning the device might have been dead.
Stream Check Active	Check to enable stream check. When enabled, the switch will detect the stream change (getting low) from the device.
Stream Check Status	Indicates stream check status. Possible statuses are: ---: disable Normal : the stream is normal. Low : the stream is getting low.
DDoS Prevention Acton	Check to enable DDOS prevention. When enabled, the switch will monitor the device against DDOS attacks.
DDoS Prevention Status	Indicates DDOS prevention status. Possible statuses are: ---: disable Analyzing : analyzes packet throughput for initialization Running : analysis completes and ready for next move Attacked : DDOS attacks occur
Device IP Address	Specifies IP address of the device
Device MAC Address	Specifies MAC address of the device

1) Advanced Configurations

5.9.2.2 Alias IP Address

This page provides Alias IP Address configuration. Some devices might have more than one IP addresses. You could specify the other IP address here.

Alias IP Address

Port	Alias IP Address
1	0.0.0.0
2	0.0.0.0
3	0.0.0.0
4	0.0.0.0
5	0.0.0.0

Figure 113 - Alias IP Address interface

The following table describes the labels for the **Alias IP Address** screen.

Label	Description
Alias IP Address	Specifies alias IP address. Keep 0.0.0.0 if the device does not have an alias IP address.
Save	Click Save to save all changes.

5.9.2.3 Alive Check

You can use ping commands to check port link status. If port link fails, you can set actions from the list.

Alive Check

Port	Mode	Action	Status
1	---	---	---
2	---	---	---
3	---	Link Change	---
4	---	Only Log it	---
5	---	Shunt Down the Port	---
6	---	---	---
7	---	---	---
8	---	---	---
9	---	---	---
10	---	---	---
11	---	---	---
12	---	---	---

Figure 114 - Alive Check interface

The following table describes the labels for the **Alive Check** screen

Label	Description
Mode	Enables or disables Alive Check of the port
Action	Actions to be taken; the options are: ---, Link Change , Only Log it , and Shunt Down the Port .
Link Change	Disables or enables the port
Only Log it	Simply sends logs to the log server
Shunt Down the Port	Disables the port
Status	Indicates the Alive Check status. Possible statuses are: ---: Disable. Analysing : Analyze the packet throughput for initialization. Running : Function ready. Attacked : DDOS attack happened.
Save	Click Save to save all changes.

5.9.2.4 DDoS Prevention

This page provides DDOS Prevention configurations. The switch can monitor ingress packets and perform actions when DDOS attack occurred on this port. You can configure the setting to achieve maximum protection.

DDOS Prevention

Port	Mode	Sensibility	Packet Type	Socket Number		Filter	Action	Status
				Low	High			
1	---	Normal	TCP	80	80	Destination	---	---
2	---	Normal	UDP	80	80	Destination	---	---
3	---	Normal	RX Total	80	80	Destination	---	---
4	---	Normal	TCP	80	80	Destination	---	---
5	---	Normal	TCP	80	80	Destination	---	---
6	---	Normal	TCP	80	80	Destination	---	---
7	---	Normal	TCP	80	80	Destination	---	---
8	---	Normal	TCP	80	80	Destination	---	---
9	---	Normal	TCP	80	80	Destination	---	---
10	---	Normal	TCP	80	80	Destination	---	---
11	---	Normal	TCP	80	80	Destination	---	---
12	---	Normal	TCP	80	80	Destination	---	---

Figure 115 - DDOS Prevention interface

The following table describes the labels for the **DDOS Prevention** screen.

Label	Description
Mode	Enables or disables DDOS prevention of the port
Sensibility	Indicates the level of DDOS detection. Possible levels are: Low: low sensibility Normal: normal sensibility Medium: medium sensibility High: high sensibility
Packet Type	Indicates the types of DDOS attack packets to be monitored. Possible types are: RX Total: all ingress packets RX Unicast: unicast ingress packets RX Multicast: multicast ingress packets RX Broadcast: broadcast ingress packets TCP: TCP ingress packets UDP: UDP ingress packets
Socket Number	If the packet type is UDP or TCP, specify the socket number here. The socket number can be a range of numbers, from low to high, or a single number. In this case, insert the same number in both Low and High fields. For Socket Numbers other than UDP or TCP, the Socket number cannot be specified.
Filter	If the packet type is UDP or TCP, choose the socket direction. The options are Destination and Source .
Action	Indicates the action to be taken when DDOS attacks occur. Possible actions are: --- : no action Blocking 1 minute: blocks forwarding for 1 minute and logs the event Blocking 10 minute: blocks forwarding for 10 minutes and logs the event Blocking: blocks and logs the event Shunt Down the Port: shuts down the port (No Link) and logs the event Only Log it: simply logs the event
Status	Indicates the DDOS prevention status. Possible statuses are: --- : disables DDOS prevention Analyzing: analyzes packet throughput for initialization Running: analysis completes and ready for next move Attacked: DDOS attacks occur

5.9.2.5 Device Description

This page allows you to configure device description settings.

Device Description

Port	Device		
	Type	Location Address	Description
1	---		
2	IP Camera		
3	IP Phone		
4	Access Point		
5	PC		
6	PLC		
7	Network Video Recorder		
8	---		
9	---		
10	---		
11	---		
12	---		
13	---		
14	---		
15	---		
16	---		
17	---		
18	---		
19	---		
20	---		
21	---		
22	---		
23	---		
24	---		
25	---		
26	---		

Save

Figure 116 - Device Description interface

The following table describes the labels for the **Device Description** screen.

Label	Description
Device Type	Indicates device types. Possible types are: --- (no specification), IP Camera , IP Phone , Access Point , PC , PLC , and Network Video Recorder
Location Address	Indicates location information of the device. The information can be used for Google Mapping.
Description	Enter Device descriptions

5.9.2.6 Stream Check

This page allows you to configure stream check settings.

Stream Check

Port	Mode	Action	Status
1	Enabled ▼	Log it ▼	Normal
2	--- ▼	--- ▼	---
3	--- ▼	--- ▼	---
4	--- ▼	--- ▼	---
5	--- ▼	--- ▼	---
6	--- ▼	--- ▼	---
7	--- ▼	--- ▼	---
8	--- ▼	--- ▼	---
9	--- ▼	--- ▼	---
10	--- ▼	--- ▼	---
11	--- ▼	--- ▼	---
12	--- ▼	--- ▼	---

Figure 117 - Steam Check interface

The following table describes the labels for the **Stream Check** screen.

Label	Description
Mode	Enables or disables Stream Monitoring of the port
Action	Indicates the action to take when the stream gets low. Possible actions are: ---: no action, or Log it : simply logs the event
Status	Indicates the Status of the port. The Mode has to be enabled for the Status to be indicated.

5.9.3 ACL

5.9.3.1 ACL Ports Configuration

This page allows you to configure the Access Control List (ACL) parameters or access control entries (ACE) of each switch port. These parameters will affect the frames received on a port unless the frame matches a specific ACE.

ACL Ports Configuration

Port	Policy ID	Action	Rate Limiter ID	Port Redirect	Mirror	Logging	Shutdown	State	Counter
*	0	<>	<>	Disabled	<>	<>	<>	<>	*
1	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0
2	0	Permit	Disabled	Disabled	Disabled	Disabled	Disabled	Enabled	0

Figure 118 - ACL Ports Configuration

The following table describes the labels for the **ACL Ports Configuration** screen.

Label	Description
Port	The switch port number to which the following settings will be applied.
Policy ID	Select the policy to apply to this port. The allowed values are 0 through 255. The default value is 0.
Action	Select to Permit or Deny forwarding. The default value is Permit .
Rate Limiter ID	Select a Rate Limiter ID for the port. The allowed values are Disabled or numbers from 1 to 16. The default value is Disabled.
Port Redirect	Select which port frames are copied to. The allowed values are Disabled or a specific port number. The default value is Disabled .
Mirror	Specify the mirror operation of this port. The allowed values are: Enabled : Frames received on the port are mirrored. Disabled : Frames received on the port are not mirrored. The default value is "Disabled".
Logging	Specifies the logging operation of the port. The allowed values are: Enabled : frames received on the port are stored in the system log. Disabled : frames received on the port are not logged. The default value is Disabled . Please note that system log memory capacity and logging rate are limited.
Shutdown	Specifies the shutdown operation of this port. The allowed values are: Enabled : if a frame is received on the port, the port will be disabled. Disabled : if port shut down is disabled. The default value is Disabled .
State	Specify the state of this port. The allowed values are: Enabled : To re-open ports by changing the volatile port configuration of the ACL user module. Disabled : To close ports by changing the volatile port configuration of the ACL user module. The default value is Enabled .
Counter	Counts the number of frames that match this ACE.
Refresh	Click Refresh to refresh the page immediately.
Clear	Click Clear to clear all statistics counters.
Save	Click Save to save changes.
Reset	Click Reset to undo any changes and revert to previously saved values.

5.9.3.2 ACL Rate Limiter Configuration

This page allows you to configure the rate limiter for the ACL of the switch.

ACL Rate Limiter Configuration

Rate Limiter ID	Rate	Unit
*	1	<> ▾
1	1	pps ▾
2	1	pps ▾
3	1	kbps ▾
4	1	pps ▾
5	1	pps ▾
6	1	pps ▾
7	1	pps ▾
8	1	pps ▾
9	1	pps ▾
10	1	pps ▾
11	1	pps ▾
12	1	pps ▾
13	1	pps ▾
14	1	pps ▾
15	1	pps ▾
16	1	pps ▾

Save Reset

Figure 119 - ACL Rate Limiter Configuration

The following table describes the labels for the **ACL Rate Limiter Configuration** screen.

Label	Description
Rate Limiter ID	The rate limiter ID for the settings contained in the same row.
Rate	The ACL Rate . The allowed values are: 0-3276700 in pps or 0, 100, 200, 300, ..., 1000000 in kbps.
Unit	It specifies the unit type. The available options are pps (packet per second) and kbps (Kbits per second.).
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.9.3.3 Access Control List

This page shows the Access Control List ([ACL](#)), which is made up of the [ACEs](#) defined on this switch. Each row describes an ACE that is defined. The maximum number of ACEs is 512 on each switch. To add a new ACE to the list, click the plus sign (shown circled by a rectangle with a red outline on Figure 120). The reserved ACEs, used for internal protocol, cannot be edited or deleted, the order sequence cannot be changed, and the priority is highest.

Auto-refresh ☐ Refresh Clear Remove All

Access Control List Configuration

Ingress Port	Policy / Bitmask	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	Counter

Figure 120 - Access Control List Configuration interface

An ACE consists of several parameters. These parameters vary with the frame type you have selected. First select the ingress port for the ACE, and then the frame type. Different parameter options are displayed according to the frame type you have selected. A frame matching the ACE can be configured here.

ACE Configuration

Ingress Port	All Port 1 Port 2 Port 3 Port 4
Policy Filter	Specific
Policy Value	0
Policy Bitmask	0x0
Frame Type	Any Any Ethernet Type ARP IPv4

Action	Permit
Rate Limiter	Disabled
Port Redirect	Disabled Port 1 Port 2 Port 3 Port 4
Mirror	Disabled
Logging	Disabled
Shutdown	Disabled
Counter	0

VLAN Parameters

802.1Q Tagged	Any
VLAN ID Filter	Any
Tag Priority	Any

Save Reset Cancel

Figure 121 - ACE Configuration interface

The following table describes the labels for the **ACE Configuration** screen.

Label	Description
Ingress Port	Indicates the ingress port of the ACE. Possible values are: All: The ACE will match all ingress port. Port: The ACE will match a specific ingress port.
Policy Filter	Specify the policy number filter for this ACE. Any: No policy filter is specified. (policy filter status is "don't-care".) Specific: If you want to filter a specific policy with this ACE, choose this value. When Specific is chosen, two fields for entering a policy value and bitmask appear: Policy Value and Policy Bitmask . Policy Value: Enter a range between 0 and 255. Policy Bitmask: Enter a range between 0x0 and 0xff.
Frame Type	Indicates the frame type of the ACE. Choose one of the options provided in the drop-down list. These frame types are mutually exclusive. Any: any frame can match the ACE. Ethernet Type: only Ethernet type frames can match the ACE. The IEEE 802.3 describes the value of length/types should be greater than or equal to 1536 decimal (equal to 0600 hexadecimal). ARP: only ARP frames can match the ACE. Notice the ARP frames will not match the ACE with Ethernet type. IPv4: The ACE will match all IPv4 frames. IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol. IPv4/UDP: The ACE will match IPv4 frames with UDP protocol. IPv4/TCP: The ACE will match IPv4 frames with TCP protocol. IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. IPv6: The ACE will match all IPv6 standard frames.
Action	Specifies the action to take when a frame matches the ACE. Permit: takes action when the frame matches the ACE. Deny: drops the frame matching the ACE.
Rate Limiter	Specifies the rate limiter in number of base units. The allowed range is 1 to 16. Disabled means that the Rate Limiter operation is disabled.
Port Redirect	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
Mirror	Specify the mirror operation of this port. Frames matching the ACE are mirrored to the destination mirror port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is Disabled .
Logging	Specifies the logging operation of the ACE. The allowed values are: Enabled: frames matching the ACE are stored in the system log. Disabled: frames matching the ACE are not logged. Please note that system log memory capacity and logging rate is limited.
Shutdown	Specifies the shutdown operation of the ACE. The allowed values are: Enabled: if a frame matches the ACE, the ingress port will be disabled. Disabled: port shutdown is disabled for the ACE.
Counter	Indicates the number of times the ACE is matched by a frame.

5.9.3.4 ACL Status

This page shows the ACL status of the different ACL users. Each row describes the ACE that is defined. It is a conflict if a specific ACE is not applied to the hardware due to hardware limitations. The maximum number of ACEs is 512 on each switch.

Combined ☐ Auto-refresh ☐ Refresh

ACL Status

User	Ingress Port	Frame Type	Action	Rate Limiter	Port Redirect	Mirror	CPU	CPU Once	Counter	Conflict
No entries										

Figure 122 - ACL Status interface

The following table describes the labels for the **ACL Status** screen.

Label	Description
User	Indicates the ACL user.
Ingress Port	Indicates the ingress port to which the ACE will apply. All: the ACE will match all ports. Port n: the ACE applies to this port number, where n is the number of the switch port.
Frame Type	Indicates the frame type of the ACE. Any: The ACE will match any frame type. EType: The ACE will match Ethernet Type frames. Note that an Ethernet Type based ACE will not get matched by IP and ARP frames. ARP: The ACE will match ARP/ RARP frames. IPv4: The ACE will match all IPv4 frames. IPv4/ICMP: The ACE will match IPv4 frames with ICMP protocol. IPv4/UDP: The ACE will match IPv4 frames with UDP protocol. IPv4/TCP: The ACE will match IPv4 frames with TCP protocol. IPv4/Other: The ACE will match IPv4 frames, which are not ICMP/UDP/TCP. IPv6: The ACE will match all IPv6 standard frames.
Action	Indicates the forwarding action of the ACE. Permit: Frames matching the ACE may be forwarded and learned. Deny: Frames matching the ACE are dropped.
Rate Limiter	Indicates the rate limiter number of the ACE. The allowed range is 1 to 16. When Disabled is displayed, the rate limiter operation is disabled.
Port Redirect	Frames that match the ACE are copied to the port number specified here. The allowed range is the same as the switch port number range. Disabled indicates that the port copy operation is disabled.
Mirror	Specify the mirror operation of this port. The allowed values are: Enabled: Frames received on the port are mirrored. Disabled: Frames received on the port are not mirrored. The default value is Disabled .
CPU	Forward packet that matched the specific ACE to CPU.
CPU Once	Forward first packet that matched the specific ACE to CPU.
Counter	The counter indicates the number of times the ACE was hit by a frame.
Conflict	Indicates the hardware status of the specific ACE. The specific ACE is not applied to the hardware due to hardware limitations.
Select ACL	Select one of the following (choose from the drop-down list next to Auto Refresh box: Combined: Shows both static and conflict entries in the ACL. Static: Shows static entries in the ACL. IPMC: Shows IPMC entries in the ACL. DHCP: Shows DHCP entries in the ACL. Loop Protect: Shows Loop Protect entries in the ACL Conflict: Show conflict entries in the ACL.
Refresh	Click Refresh to refresh the page.
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals.

5.9.4 AAA

5.9.4.1 AAA – Authentication Server Configuration

Authentication, Authorization and Accounting (AAA)—this page allows you to configure the AAA server.

Authentication Server Configuration

Common Server Configuration

Timeout	15	seconds
Dead Time	300	seconds

RADIUS Authentication Server Configuration

#	Enabled	IP Address	Port	Secret
1	<input type="checkbox"/>		1812	
2	<input type="checkbox"/>		1812	
3	<input type="checkbox"/>		1812	
4	<input type="checkbox"/>		1812	
5	<input type="checkbox"/>		1812	

RADIUS Accounting Server Configuration

#	Enabled	IP Address	Port	Secret
1	<input type="checkbox"/>		1813	
2	<input type="checkbox"/>		1813	
3	<input type="checkbox"/>		1813	
4	<input type="checkbox"/>		1813	
5	<input type="checkbox"/>		1813	

Save Reset

Figure 123 - Authentication Server Configuration interface

The following table describes the labels for the **Authentication Server Configuration** screen.

Label	Description
Timeout	The Timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server. If the server does not reply within this time frame, we will consider it to be dead and continue with the next enabled server (if any). RADIUS servers are using the UDP protocol, which is unreliable by design. To cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered to be dead.
Dead Time	The Dead Time , which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead. Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.
Radius Authentication Server Configuration	
#	The RADIUS Authentication Server number for which the configuration below applies.
Enabled	Enable the RADIUS Authentication Server by checking this box.
IP Address	The IP address of the RADIUS Authentication Server. IP address is expressed in dotted decimal notation .
Port	The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.

Secret	The Secret —up to 29 characters long—shared between the RADIUS Authentication Server and the switch.
Radius Accounting Server Configuration	
#	The RADIUS Accounting Server number for which the configuration below applies.
Enabled	Enable the RADIUS Accounting Server by checking this box.
IP Address	The IP address of the RADIUS Accounting Server. IP address is expressed in dotted decimal notation .
Port	The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.
Secret	The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.
Save	Click Save to save changes.
Reset	Click to undo any changes made locally and revert to previously saved values.

5.9.4.2 RADIUS Overview

This page provides an overview of the status of the RADIUS servers configurable on the authentication configuration page.

RADIUS Authentication Server Status Overview

Auto-refresh ☐ Refresh

#	IP Address	Status
1	0.0.0.0:1812	Disabled
2	0.0.0.0:1812	Disabled
3	0.0.0.0:1812	Disabled
4	0.0.0.0:1812	Disabled
5	0.0.0.0:1812	Disabled

RADIUS Accounting Server Status Overview

#	IP Address	Status
1	0.0.0.0:1813	Disabled
2	0.0.0.0:1813	Disabled
3	0.0.0.0:1813	Disabled
4	0.0.0.0:1813	Disabled
5	0.0.0.0:1813	Disabled

Figure 124 - Radius Authentication Server Status Overview interface

The following table describes the labels for the **Radius Authentication Server Status Overview**.

Label	Description
#	The RADIUS server number. Click to navigate to detailed statistics of the server.
IP Address	The IP address and UDP port number (in <IP Address>: <UDP Port> notation) of the server.
Status	The current status of the server. This field takes one of the following values: Disabled: The server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Refresh	Click to refresh the page immediately.
Auto-refresh	Check to enable an automatic refresh of the page at regular intervals.

5.9.4.3 RADIUS Details

This page provides detailed statistics for a specific RADIUS server.

RADIUS Authentication Statistics for Server #1

Server #1 ▾	Auto-refresh <input type="checkbox"/>	Refresh	Clear
Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address	0.0.0.0:1812		
State	Disabled		
Round-Trip Time	0 ms		

RADIUS Accounting Statistics for Server #1

Receive Packets		Transmit Packets	
Responses	0	Requests	0
Malformed Responses	0	Retransmissions	0
Bad Authenticators	0	Pending Requests	0
Unknown Types	0	Timeouts	0
Packets Dropped	0		
Other Info			
IP Address	0.0.0.0:1813		
State	Disabled		
Round-Trip Time	0 ms		

Figure 125 - RADIUS Authentication Statistics for Server #1 interface

This table describes the labels for the **RADIUS Authentication Statistics for Server #1** screen.

Label	Description
Server #n ↓	Use the server's drop-down box to determine which server's information will be shown by selecting server #n. 'n' is from 1 to 5.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click Refresh to refresh the page immediately.
Clear	Click Clear to clear the counters for the selected server. Note that the "Pending Requests" counter will not be cleared by this operation.

5.9.4.4 Packet Counters—RADIUS authentication server packet counter

There are seven receive and three transmit counters (as shown below).

Rx / Tx	Name	RFC4668 Name	Description
Rx	Access Accepts	radiusAuthClientExtAccessAccepts	The number of RADIUS Access-Accept packets (valid or invalid) received from the server.
Rx	Access Rejects	radiusAuthClientExtAccessRejects	The number of RADIUS Access-Reject packets (valid or invalid) received from the server.
Rx	Access Challenges	radiusAuthClientExtAccessChallenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from the server.
Rx	Malformed Access Responses	radiusAuthClientExtMalformedAccessResponses	The number of malformed RADIUS Access-Response packets received from the server. Malformed packets include packets with an invalid length. Bad authenticators or Message Authenticator attributes or unknown types are not included as malformed access responses.
Rx	Bad Authenticators	radiusAuthClientExtBadAuthenticators	The number of RADIUS Access-Response packets containing invalid authenticators or Message Authenticator attributes received from the server.
Rx	Unknown Types	radiusAuthClientExtUnknownTypes	The number of RADIUS packets that were received with unknown types from the server on the authentication port and dropped.
Rx	Packets Dropped	radiusAuthClientExtPacketsDropped	The number of RADIUS packets that were received from the server on the authentication port and dropped for some other reason.
Tx	Access Requests	radiusAuthClientExtAccessRequests	The number of RADIUS Access-Request packets sent to the server. This does not include retransmissions.
Tx	Access Retransmissions	radiusAuthClientExtAccessRetransmissions	The number of RADIUS Access-Request packets retransmitted to the RADIUS authentication server.
Tx	Pending Requests	radiusAuthClientExtPendingRequests	The number of RADIUS Access-Request packets destined for the server that have not yet timed out or received a response. This variable is incremented when an Access-Request is sent and decremented due to receipt of an Access-Accept, Access-Reject, Access-Challenge, timeout, or retransmission.

Tx	Timeouts	radiusAuthClientExtTimeouts	The number of authentication timeouts to the server. After a timeout, the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
-----------	-----------------	-----------------------------	---

For more information about the state of the server and the latest round-trip time, see the tables and other information as follows.

Name	RFC4668 Name	Description
IP Address	-	IP address and UDP port for the authentication server in question.
State	-	Shows the state of the server. It takes one of the following values: Disabled: The selected server is disabled. Not Ready: The server is enabled, but IP communication is not yet up and running. Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept access attempts. Dead (X seconds left): Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.
Round-Trip Time	radiusAuthClientExtRoundTripTime	The time interval (measured in milliseconds) between the most recent Access-Reply/Access-Challenge and the Access-Request that matched it from the RADIUS authentication server. The granularity of this measurement is 100 ms. A value of 0 ms indicates that there hasn't been round-trip communication with the server yet.

5.9.5 NAS (802.1x)

5.9.5.1 Overview

This page allows you to configure the IEEE 802.1X and MAC-based authentication system and port settings.

The IEEE 802.1X standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. One or more central servers (the backend servers) determine whether the user is allowed access to the network. These backend (RADIUS) servers are configured on the **Security** → **AAA** → **AAA** page.

MAC-based authentication allows for authentication of more than one user on the same port, and does not require the users to have special 802.1X software installed on their system. The switch uses the users' MAC addresses to authenticate against the backend server. As intruders can create counterfeit MAC addresses, which makes MAC-based authentication is less secure than 802.1 X authentications.

1) Overview of 802.1X (Port-Based) Authentication

In an 802.1X network environment, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The switch acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server. Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (Extensible Authentication Protocol (EAP) Over LANs) frames which encapsulate EAP PDUs (Protocol Data Units) (RFC3748). Frames sent between the switch and the RADIUS server are RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible as it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) does not need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.

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

Note: in an environment where two backend servers are enabled, the server timeout is configured to X seconds (using the authentication configuration page), and the first server in the list is currently down (but not considered dead), if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, it will never be authenticated because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant.

Since the server has not failed (because the X seconds have not expired), the same server will be contacted when the next back-end authentication server requests from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.

2) Overview of MAC-Based Authentication

Unlike 802.1X, MAC-based authentication is not a standard, but merely a best -practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string in the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.

When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using static entries into the MAC Table. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC -based authentication has nothing to do with the 802.1X standard.

The advantage of MAC-based authentication over 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients do not need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users, equipment whose MAC address is a valid RADIUS user can be used by anyone, and only the MD5-Challenge method is supported.

802.1X and MAC-Based authentication configurations consist of two sections: system- and port-wide.

5.9.5.2 Configuration

1) Network Access Server (NAS) Configuration

Network Access Server Configuration

System Configuration

Mode	Disabled ▾	
Reauthentication Enabled	<input type="checkbox"/>	
Reauthentication Period	3600	seconds
EAPOL Timeout	30	seconds
Aging Period	300	seconds
Hold Time	10	seconds

Port Configuration

Port	Admin State	Port State	Restart	
*	<> ▾			
1	Force Authorized ▾	Globally Disabled	Reauthenticate	Reinitialize
2	Force Authorized ▾	Globally Disabled	Reauthenticate	Reinitialize
3	Force Authorized ▾	Globally Disabled	Reauthenticate	Reinitialize
4	Force Authorized ▾	Globally Disabled	Reauthenticate	Reinitialize
5	Force Authorized ▾	Globally Disabled	Reauthenticate	Reinitialize
6	Force Authorized ▾	Globally Disabled	Reauthenticate	Reinitialize
7	Force Authorized ▾	Globally Disabled	Reauthenticate	Reinitialize
8	Force Authorized ▾	Globally Disabled	Reauthenticate	Reinitialize

Figure 126 - Network Access Server Configuration interface

The following table describes the labels for the **Network Access Server Configuration** screen.

Label	Description
Mode	Indicates if 802.1X and MAC-based authentication is globally enabled or disabled on the switch. If globally disabled, all ports are allowed to forward frames.
Re-authentication Enabled	If checked, clients are re-authenticated after the interval specified by the Re-authentication Period. Re-authentication for 802.1X-enabled ports can be used to detect if a new device is plugged into a switch port. For MAC-based ports, re-authentication is only useful if the RADIUS server configuration has changed. It does not involve communication between the switch and the client, and therefore does not imply that a client is still present on a port (see Age Period below).
Re-authentication Period	Determines the period, in seconds, after which a connected client must be re-authenticated. This is only active if the Re-authentication is Enabled. Valid range of the value is 1 to 3600 seconds.
EAPOL Timeout	Determines the time for retransmission of Request Identity EAPOL frames. Valid range of the value is 1 to 65535 seconds. This has no effect for MAC-based ports.

Aging Period	<p>This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:</p> <p>MAC-Based Auth.:</p> <p>When the NAS module uses the Port Security module to secure MAC addresses, the Port Security module needs to check for activity on the MAC address in question at regular intervals and free resources if no activity is seen within a given period of time. This parameter controls exactly this period and can be set to a number between 10 and 1000000 seconds.</p> <p>For ports in MAC-based Auth. mode, reauthentication does not cause direct communications between the switch and the client, so this will not detect whether the client is still attached or not, and the only way to free any resources is to age the entry.</p>
Hold Time	<p>This setting applies to the following modes, i.e. modes using the Port Security functionality to secure MAC addresses:</p> <p>MAC-Based Auth.:</p> <p>If a client is denied access - either because the RADIUS server denies the client access or because the RADIUS server request times out (according to the timeout specified on the "Security→AAA→AAA" page) – the client is put on hold in Unauthorized state. The hold timer does not count during an on-going authentication.</p> <p>The switch will ignore new frames coming from the client during the hold time. The hold time can be set to a number between 10 and 1000000 seconds.</p>

2) Port Configuration

The following table describes the labels for the **Port Configuration** screen.

Label	Description
Port	The port number for which the configuration below applies.
Admin State	<p>If NAS is globally enabled, this selection controls the port's authentication mode. The following modes are available:</p> <p>Force Authorized (1) Force Unauthorized (2) 802.1X (3) MAC-based Auth. (4)</p> <p>All of them are explained below.</p>
1. Force Authorized	In this mode, the switch will send one EAPOL Success frame when the port link is up, and any client on the port will be allowed network access without authentication.
2. Force Unauthorized	In this mode, the switch will send one EAPOL Failure frame when the port link is up, and any client on the port will be disallowed network access.
3. 802.1X	<p>In an 802.1X network environment, the user is called the supplicant, the switch is the authenticator, and the RADIUS server is the authentication server. The authenticator acts as the man-in-the-middle, forwarding requests and responses between the supplicant and the authentication server.</p> <p>EAPOL (EAP Over LANs)</p> <p>Frames sent between the supplicant and the switch are special 802.1X frames, known as EAPOL (EAP Over LANs) frames which encapsulate EAP PDUs (RFC3748). Frames sent between the switch and the RADIUS server is RADIUS packets. RADIUS packets also encapsulate EAP PDUs together with other attributes like the switch's IP address, name, and the supplicant's port number on the switch. EAP is very flexible as it allows for different authentication methods, like MD5-Challenge, PEAP, and TLS. The important thing is that the authenticator (the switch) does not need to know which authentication method the supplicant and the authentication server are using, or how many information exchange frames are needed for a particular method. The switch simply</p>

	<p>encapsulates the EAP part of the frame into the relevant type (EAPOL or RADIUS) and forwards it.</p> <p>When authentication is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding the result to the supplicant, the switch uses it to open up or block traffic on the switch port connected to the supplicant.</p> <p>Note: in an environment where two backend servers are enabled, the server timeout is configured to X seconds (using the authentication configuration page), and the first server in the list is currently down (but not considered dead), if the supplicant retransmits EAPOL Start frames at a rate faster than X seconds, it will never be authenticated because the switch will cancel on-going backend authentication server requests whenever it receives a new EAPOL Start frame from the supplicant. Since the server has not failed (because the X seconds have not expired), the same server will be contacted when the next backend authentication server request from the switch. This scenario will loop forever. Therefore, the server timeout should be smaller than the supplicant's EAPOL Start frame retransmission rate.</p>
Single 802.1X	<p>In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they are not authenticated individually. To overcome this security breach, use the Single 802.1X variant.</p> <p>Single 802.1X is not yet an IEEE standard, but features many of the same characteristics as port-based 802.1X. In Single 802.1X, at most one supplicant can get authenticated on the port at a time. Normal EAPOL frames are used in the communications between the supplicant and the switch. If more than one supplicant is connected to a port, the one that comes first when the port's link is connected will be the first one considered. If that supplicant does not provide valid credentials within a certain amount of time, the chance will be given to another supplicant. Once a supplicant is successfully authenticated, only that supplicant will be allowed access. This is the most secure of all the supported modes. In this mode, the Port Security module is used to secure a supplicant's MAC address once successfully authenticated.</p>
4. Multi 802.1X	<p>In port-based 802.1X authentication, once a supplicant is successfully authenticated on a port, the whole port is opened for network traffic. This allows other clients connected to the port (for instance through a hub) to piggy-back on the successfully authenticated client and get network access even though they are not authenticated individually. To overcome this security breach, use the Multi 802.1X variant.</p> <p>Multi 802.1X is not yet an IEEE standard, but features many of the same characteristics as port-based 802.1X. In Multi 802.1X, one or more supplicants can be authenticated on the same port at the same time. Each supplicant is authenticated individually and secured in the MAC table using the Port Security module.</p> <p>In Multi 802.1X it is not possible to use the multicast BPDU MAC address as the destination MAC address for EAPOL frames sent from the switch to the supplicant, since that would cause all supplicants attached to the port to reply to requests sent from the switch. Instead, the switch uses the supplicant's MAC address, which is obtained from the first EAPOL Start or EAPOL Response Identity frame sent by the supplicant. An exception to this is when no supplicants are attached. In this case, the switch sends EAPOL Request Identity frames using the BPDU multicast MAC address as destination - to wake up any supplicants that might be on the port.</p> <p>The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.</p>

4.MAC-based Auth.	<p>Unlike port-based 802.1X, MAC-based authentication is not a standard, but merely a best-practices method adopted by the industry. In MAC-based authentication, users are called clients, and the switch acts as the supplicant on behalf of clients. The initial frame (any kind of frame) sent by a client is snooped by the switch, which in turn uses the client's MAC address as both username and password in the subsequent EAP exchange with the RADIUS server. The 6-byte MAC address is converted to a string in the following form "xx-xx-xx-xx-xx-xx", that is, a dash (-) is used as separator between the lower-cased hexadecimal digits. The switch only supports the MD5-Challenge authentication method, so the RADIUS server must be configured accordingly.</p> <p>When authentication is complete, the RADIUS server sends a success or failure indication, which in turn causes the switch to open up or block traffic for that particular client, using the Port Security module. Only then will frames from the client be forwarded on the switch. There are no EAPOL frames involved in this authentication, and therefore, MAC-based authentication has nothing to do with the 802.1X standard.</p> <p>The advantage of MAC-based authentication over port-based 802.1X is that several clients can be connected to the same port (e.g. through a 3rd party switch or a hub) and still require individual authentication, and that the clients don't need special supplicant software to authenticate. Another advantage of MAC-based authentication over 802.1X-based authentication is that the clients do not need special supplicant software to authenticate. The disadvantage is that MAC addresses can be spoofed by malicious users - equipment whose MAC address is a valid RADIUS user can be used by anyone. Also, only the MD5-Challenge method is supported. The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality.</p>
Port State	<p>The current state of the port. It can undertake one of the following values:</p> <p>Globally Disabled: NAS is globally disabled.</p> <p>Link Down: NAS is globally enabled, but there is no link on the port.</p> <p>Authorized: the port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.</p> <p>Unauthorized: the port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.</p> <p>X Auth/Y Unauth: the port is in a multi-supplicant mode. Currently X clients are authorized and Y are unauthorized.</p>
Restart	<p>Two buttons are available for each row. The buttons are only enabled when authentication is globally enabled and the port's Admin State is in an EAPOL-based or MAC-based mode.</p> <p>Clicking these buttons will not cause settings changed on the page to take effect.</p> <p>Reauthenticate: schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication). For MAC-based authentication, reauthentication will be attempted immediately.</p> <p>The button only has effect on successfully authenticated clients on the port and will not cause the clients to be temporarily unauthorized.</p> <p>Reinitialize: forces a reinitialization of the clients on the port and hence a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress.</p>

5.9.5.3 NAS Switch

This page provides an overview of the current NAS port states.

Network Access Server Switch Status

Auto-refresh ☐ Refresh

Port	Admin State	Port State	Last Source	Last ID
1	Force Authorized	Globally Disabled		
2	Force Authorized	Globally Disabled		
3	Force Authorized	Globally Disabled		
4	Force Authorized	Globally Disabled		
5	Force Authorized	Globally Disabled		
6	Force Authorized	Globally Disabled		
7	Force Authorized	Globally Disabled		
8	Force Authorized	Globally Disabled		
9	Force Authorized	Globally Disabled		
10	Force Authorized	Globally Disabled		
11	Force Authorized	Globally Disabled		
12	Force Authorized	Globally Disabled		
13	Force Authorized	Globally Disabled		
14	Force Authorized	Globally Disabled		
15	Force Authorized	Globally Disabled		
16	Force Authorized	Globally Disabled		
17	Force Authorized	Globally Disabled		
18	Force Authorized	Globally Disabled		
19	Force Authorized	Globally Disabled		
20	Force Authorized	Globally Disabled		
21	Force Authorized	Globally Disabled		
22	Force Authorized	Globally Disabled		
23	Force Authorized	Globally Disabled		
24	Force Authorized	Globally Disabled		
25	Force Authorized	Globally Disabled		
26	Force Authorized	Globally Disabled		

Figure 127 - Network Access Server Switch Status interface

The following table describes the labels for the **Network Access Server Switch Status** screen.

Label	Description
Port	The switch port number. Click a port number to navigate to detailed 802.1X statistics of each port.
Admin State	The port's current administrative state. Refer to NAS Admin State for more details regarding each value.
Port State	The current state of the port. Refer to NAS Port State for more details regarding each value.
Last Source	The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication.
Last ID	The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication.

5.9.5.4 NAS Port

This page provides detailed IEEE 802.1X statistics for a specific switch port using port-based authentication. For MAC-based ports, only selected backend server (RADIUS Authentication Server) statistics are shown. Use the Port's drop-down list to select details about which Port to be displayed.

NAS Statistics Port 1

Port 1 Auto-refresh ☐

Port State

Admin State	Force Authorized
Port State	Globally Disabled

Figure 128 - NAS Statistics Port 1 interface

The following table describes the labels for the **NAS Statistics Port 1** screen.

Label	Description
Admin State	The port's current administrative state. Refer to NAS Admin State for more details regarding each value.
Port State	The current state of the port. Refer to NAS Port State for more details regarding each value.
Auto-refresh	Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.
Refresh	Click to refresh the page immediately.

1) EAPOL Counters

These supplicant frame counters are available for the following administrative states:

- **Force Authorized**
- **Force Unauthorized**
- **802.1X**

The following table describes the seven receive and three transmit **EAPOL** counters.

Rx/Tx	Name	IEEE Name	Description
Rx	Total	dot1xAuthEapolFramesRx	The number of valid EAPOL frames of any type that have been received by the switch.
Rx	Response ID	dot1xAuthEapolRespIdFramesRx	The number of valid EAPOL Response Identity frames that have been received by the switch.
Rx	Responses	dot1xAuthEapolRespFramesRx	The number of valid EAPOL response frames (other than Response Identity frames) that have been received by the switch.
Rx	Start	dot1xAuthEapolStartFramesRx	The number of EAPOL Start frames that have been received by the switch.
Rx	Logoff	dot1xAuthEapolLogoffFramesRx	The number of valid EAPOL Logoff frames that have been received by the switch.
Rx	Invalid Type	dot1xAuthInvalidEapolFramesRx	The number of EAPOL frames that have been received by the switch in which the frame type is not recognized.
Rx	Invalid Length	dot1xAuthEapolLengthErrorFramesRx	The number of EAPOL frames that have been received by the switch in which the Packet Body Length field is invalid.
Tx	Total	dot1xAuthEapolFramesTx	The number of EAPOL frames of any type that have been transmitted by the switch.
Tx	Request ID	dot1xAuthEapolReqIdFramesTx	The number of EAPOL Request Identity frames that have been transmitted by the switch.
Tx	Requests	dot1xAuthEapolReqFramesTx	The number of valid EAPOL Request frames (other than Request Identity frames) that have been transmitted by the switch.

2) Backend Server Counters

These backend (RADIUS) frame counters are available for the following administrative states:

- **802.1X**
- **MAC-based Auth.**

The following table describes the four receive and one transmit Backend Server counters.

Rx / Tx	Name	IEEE Name	Description
Rx	Access Challenges	dot1xAuthBackend AccessChallenges	<p>802.1X-based: Counts the number of times that the switch receives the first request from the backend server following the first response from the supplicant. Indicates that the backend server has communication with the switch.</p> <p>MAC-based: Counts all Access Challenges received from the backend server for this port (left-most table) or client (right-most table).</p>
Rx	Other Requests	dot1xAuthBackend OtherRequestsToS supplicant	<p>802.1X-based: Counts the number of times that the switch sends an EAP Request packet following the first to the supplicant. Indicates that the backend server chose an EAP-method.</p> <p>MAC-based: Not applicable.</p>
Rx	Auth. Successes	dot1xAuthBackend AuthSuccesses	<p>802.1X- and MAC-based: Counts the number of times that the switch receives a success indication. Indicates that the supplicant/client has successfully authenticated to the backend server.</p>
Rx	Auth. Failures	dot1xAuthBackend AuthFails	<p>802.1X- and MAC-based: Counts the number of times that the switch receives a failure message. This indicates that the supplicant/client has not authenticated to the backend server.</p>
Tx	Responses	dot1xAuthBackend Responses	<p>802.1X-based: Counts the number of times that the switch attempts to send a supplicant's first response packet to the backend server. Indicates the switch attempted communication with the backend server. Possible retransmissions are not counted.</p> <p>MAC-based: Counts all the backend server packets sent from the switch towards the backend server for a given port (left-most table) or client (right-most table). Possible retransmissions are not counted.</p>

3) Last Supplicant/ Client Info

Information about the last supplicant/client that attempted to authenticate. This information is available for the following administrative states:

- **802.1X**
- **MAC-based Auth.**

Name	IEEE Name	Description
MAC Address	dot1xAuthLastEapolFrameSource	The MAC address of the last supplicant/client.
VLAN ID	-	The VLAN ID on which the last frame from the last supplicant/client was received.
Version	dot1xAuthLastEapolFrameVersion	802.1X-based: The protocol version number carried in the most recently received EAPOL frame. MAC-based: Not applicable.
Identity	-	802.1X-based: The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame. MAC-based: Not applicable.

4) Selected Counters

The Selected Counters table is visible when the port is in the MAC-based Auth. state. The table is identical to and is placed next to the [Port Counters](#) table, and will be empty if no MAC address is currently selected. To populate the table, select one of the [attached MAC Addresses](#) from the table below.

Label	Description
MAC Address	For MAC-based Auth., this column holds the MAC address of the attached client. Clicking the link causes the client's Backend Server counters to be shown in the Selected Counters table. If no clients are attached, it shows No clients attached.
VLAN ID	This column holds the VLAN ID that the corresponding client is currently secured through the Port Security module.
State	The client can either be authenticated or unauthenticated. In the authenticated state, it is allowed to forward frames on the port, and in the unauthenticated state, it is blocked. As long as the backend server hasn't successfully authenticated the client, it is unauthenticated. If an authentication fails for one or the other reason, the client will remain in the unauthenticated state for Hold Time seconds.
Last Authentication	Shows the date and time of the last authentication of the client (successful as well as unsuccessful).

5.10 Warning

The Warning function is very important for managing the switch. The switch can be managed using SYSLOG, E-MAIL, and Fault Relay. The function helps the user to monitor the switch's status at a remote site. When events occur, a warning message will be sent to the appointed server, E-MAIL, or relay fault on the switch panel.

5.10.1 Fault Alarm

When any selected fault event happens, the Fault LED on the switch panel will light up and the electric relay will signal at the same time.

Select the events to cause the Fault Alarm, then click **Save** (at the bottom of the screen) to save the changes.

Fault Alarm

Power Failure

☐ PWR 1

☐ PWR 2

Port Link Down/Broken

Port	Active
1	<input type="checkbox"/>
2	<input type="checkbox"/>
3	<input type="checkbox"/>
4	<input type="checkbox"/>
5	<input type="checkbox"/>
6	<input type="checkbox"/>
7	<input type="checkbox"/>
8	<input type="checkbox"/>

Figure 129 - Fault Alarm interface

The following table describes the labels for the **Fault Alarm** screen.

Label	Description
Power Failure	Fault alarm when any selected power failure. This switch support dual powers.
PWR 1	Add a checkmark if you choose the fault alarm LED to appear on PWR 1.
PWR 2	Add a checkmark if you choose the fault alarm LED to appear on PWR 2.
Port Link Down/Broken	Fault alarm when any selected port link down/broken.
Port	Indicates a port number.
Active	Add a checkmark to indicate if the port is Active .
Save	Click Save to save changes.

5.10.2 System Warning

5.10.2.1 SYSLOG Setting

The SYSLOG is a protocol that transmits event notifications across networks. For more details, please refer to RFC 3164 - The BSD SYSLOG Protocol.

System Log Configuration

Server Mode	Disabled ▾
Server Address	0.0.0.0

Figure 130 - System Log Configuration interface

The following table describes the labels for the System Log Configuration screen.

Label	Description
Server Mode	Indicates existing server mode. When the mode operation is enabled, the syslog message will be sent to syslog server. The syslog protocol is based on UDP communications and received on UDP port 514. The syslog server will not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always be sent even if the syslog server does not exist. Possible modes are: Enabled: enables server mode Disabled: disables server mode
SYSLOG Server	Indicates the IPv4 host address of syslog server. If the switch provides DNS functions, it also can be a host name. 0.0.0.0 is shown as default.
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.10.2.2 SMTP Settings

The Simple Mail Transfer Protocol (SMTP) is a protocol for e-mail transmission across the Internet. For details, refer to RFC 821 - Simple Mail Transfer Protocol. To set it up, go to the page below.

SMTP Setting

E-mail Alert : ▾

SMTP Server Address	0.0.0.0
Sender E-mail Address	administrator
Mail Subject	Automated Email Alert
<input type="checkbox"/> Authentication	
Recipient E-mail Address 1	
Recipient E-mail Address 2	
Recipient E-mail Address 3	
Recipient E-mail Address 4	
Recipient E-mail Address 5	
Recipient E-mail Address 6	

Figure 131 - SMTP Setting interface

The following table describes the labels for the **SMTP Setting** screen.

Label	Description
E-mail Alert	Enables or disables transmission of system warnings by e-mail.
SMTP Server Address	The SMTP server IP address (or domain name address). The default is 0.0.0.0
Sender E-mail Address	The sender's E-mail address
Mail Subject	Subject of the mail
Authentication	Username: the authentication username Password: the authentication password Confirm Password: re-enter password
Recipient E-mail Address	The recipient's e-mail address, allows a total number of six recipients.
Save	Click Save to save the settings.

5.10.2.3 Event Selection

There is one warning way supported by system—SYSLOG. Checking the corresponding box will enable specific system event warning to SYSLOG. Note that the checkbox cannot be checked when SYSLOG is disabled.

System Warning - Event Selection

System Events	SYSLOG	SMTP
System Start	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Power Status	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SNMP Authentication Failure	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Redundant Ring Topology Change	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Port	SYSLOG	SMTP
1	Link Up	Disabled
2	Disabled	Disabled
3	Disabled	Disabled
4	Disabled	Disabled
5	Disabled	Disabled
6	Disabled	Disabled
7	Disabled	Disabled
8	Disabled	Disabled
9	Disabled	Disabled
10	Disabled	Disabled
11	Disabled	Disabled

Figure 132 - System Warning - Event Selection

The following table describes the labels for the **System Warning – Event Selection** screen.

Label	Description
System Start	Alerts when the system is restarted.
Power Status	Alerts when power is up or down.
SNMP Authentication Failure	Alerts when SNMP authentication fails.
Redundant Ring Topology Change	Alerts when there is a Ring topology change.

SYSLOG	Select the SYSLOG event for a specific port number. Possible selections are: <ul style="list-style-type: none">• Disable• Link Up• Link Down• Link Up and Link Down
SMTP	Select a SMTP option for a specific port number. Possible selections are: <ul style="list-style-type: none">• Disable• Link Up• Link Down• Link Up and Link Down
Save	Click Save to save changes.
Reset	Click Reset to undo any changes made locally and revert to previously saved values.

5.11 Monitoring and Diagnostic

5.11.1 MAC Table

5.11.1.1 MAC Address Table Configuration

The MAC address table can be configured on this page. Set timeouts for entries in the dynamic MAC table and configure the static MAC table here.

MAC Address Table Configuration

Aging Configuration

Disable Automatic Aging	<input type="checkbox"/>
Aging Time	300 seconds

MAC Table Learning

	Port Members																									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Auto	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Disable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Static MAC Table Configuration

	Port Members																											
Delete	VLAN ID	MAC Address	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Add New Static Entry

Save

Reset

Figure 133 - MAC Address Table Configuration

1) Aging Configuration

By default, dynamic entries are removed from the MAC after 300 seconds (as shown above). This removal is called Aging. You can configure Aging Time by entering a value in the box of **Aging Time**. The allowed range is 10 to 1000000 seconds. You can also disable the automatic aging of dynamic entries by checking **Disable Automatic Aging**.

2) MAC Table Learning

If the learning mode for a given port is grayed out, it means another module is in control of the mode, and thus the user cannot change the configurations. An example of such a module is MAC-Based authentication under 802.1X. You can configure the port to dynamically learn the MAC address based upon the following settings.

Label	Description
Auto	Learning is done automatically as soon as a frame with unknown SMAC is received.
Disable	No learning is done.
Secure	Only static MAC entries are learned, all other frames are dropped. Note: make sure the link used for managing the switch is added to the static Mac table before changing to secure learning mode, otherwise the management link will be lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface.

3) Static MAC Table Configurations

The static entries in the MAC table are shown in this table. The static MAC table can contain up to 64 entries. The entries are for the whole stack, not for individual switches. The MAC table is sorted first by VLAN ID and then by MAC address.

Label	Description
Delete	Check to delete an entry. It will be deleted during the next save.
VLAN ID	The VLAN ID for the entry.
MAC Address	The MAC address for the entry.
Port Members	Checkmarks indicate which ports are members of the entry. Check or uncheck to modify the entry.
Adding New Static Entry	Click to add a new entry to the static MAC table. You can specify the VLAN ID, MAC Address, and Port Members for the new entry. Click Save to save the changes.

5.11.1.2 MAC Address Table

Entries in the MAC Table are shown on this page. The MAC Address Table contains up to 8192 entries, and is sorted first by VLAN ID, then by MAC address.

Each page shows up to 999 entries from the MAC table, with a default value of 20, selected by the **Entries Per Page** input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.

The **Start from MAC address** and **VLAN** fields allow the user to select the starting point in the MAC table. Clicking the **Refresh** button will update the displayed table starting from that or the closest next MAC table match. In addition, the two input fields will – upon clicking **Refresh** - assume the value of the first displayed entry, allows for continuous refresh with the same start address.

The >> will use the last entry of the currently displayed VLAN/MAC address pairs as a basis for the next lookup. When it reaches the end, the text "**no more entries**" is shown in the displayed table. Use the << button to start over.

MAC Address Table

Auto-refresh ☐ Refresh Clear << >>

Start from VLAN and MAC address with entries per page.

			Port Members																											
Type	VLAN	MAC Address	CPU	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	
Static	1	01-80-C2-4A-44-06	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Dynamic	1	54-E1-AD-07-0D-87					✓																							
Static	1	E8-E8-75-00-2C-57	✓																											
Static	1	FF-FF-FF-FF-FF-FF	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	

Figure 134 - MAC Address Table

The following table describes the labels for the **MAC Address Table** screen.

Label	Description
Type	Indicates whether the entry is a static or dynamic entry.
MAC address	The MAC address of the entry.
VLAN	The VLAN ID of the entry.
Port Members	The ports that are members of the entry.

5.11.2 Port Statistics

5.11.2.1 Traffic Overview

This page provides an overview of general traffic statistics for all switch ports.

Port Statistics Overview

Auto-refresh ☐ Refresh Clear

Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	44296	14219	5965478	4013429	1	0	0	0	9585
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	25	0	4792	0	0	0	6	0	19
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0

Figure 135 - Port Statistics Overview interface

The following table describes the labels for the **Ports Statistics Overview** screen.

Label	Description
Port	The logical port for the settings contained in the same row. Click on a port to go to that ports Detailed Statistics page.
Packets	The number of received and transmitted packets per port.
Bytes	The number of received and transmitted bytes per port.
Errors	The number of frames received in error and the number of incomplete transmissions per port.
Drops	The number of frames discarded due to ingress or egress congestion.
Filtered	The number of received frames filtered by the forwarding process.
Auto-refresh	Check to enable an automatic refresh of the page. Automatic refresh occurs every 3 seconds at regular intervals.
Refresh	Click Refresh to refresh the page immediately.
Clear	Clears Clear the counters for all ports.

5.11.2.2 Detailed Statistics

This page provides detailed traffic statistics for a specific switch port. Use the port drop-down list to decide the details of which switch port to be displayed.

The displayed counters include the total number for receive and transmit, the size for receive and transmit, and the errors for receive and transmit.

Detailed Port Statistics Port 1

Port 1	Auto-refresh	Refresh	Clear
Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		Transmit Size Counters	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		Transmit Queue Counters	
Rx Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	0
Receive Error Counters		Transmit Error Counters	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		0
Rx Oversize	0		0
Rx Fragments	0		0
Rx Jabber	0		0
Rx Filtered	0		0

Figure 136 - Detailed Port Statistics Port 1

The following table describes the labels for the **Detailed Ports Statistics Port 1** screen.

Label	Description
Rx and Tx Packets	The number of received and transmitted (good and bad) packets.
Rx and Tx Octets	The number of received and transmitted (good and bad) bytes, including FCS, except framing bits.
Rx and Tx Unicast	The number of received and transmitted (good and bad) unicast packets.
Rx and Tx Multicast	The number of received and transmitted (good and bad) multicast packets.
Rx and Tx Broadcast	The number of received and transmitted (good and bad) broadcast packets.
Rx and Tx Pause	The number of MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation.
Rx and Tx Size Counters	The number of received and transmitted (good and bad) packets split into categories based on their respective frame sizes.
Rx and Tx Queue Counters	The number of received and transmitted packets per input and output queue.
Rx Drops	The number of frames dropped due to insufficient receive buffer or egress congestion.
Rx CRC/Alignment	The number of frames received with CRC or alignment errors.
Rx Undersize	The number of short1 frames received with a valid CRC.
Rx Oversize	The number of long2 frames received with a valid CRC.
Rx Fragments	The number of short1 frames received with an invalid CRC.
Rx Jabber	The number of long2 frames received with an invalid CRC.
Rx Filtered	The number of received frames filtered by the forwarding process.
Tx Drops	The number of frames dropped due to output buffer congestion.
Tx Late / Exc.Coll.	The number of frames dropped due to excessive or late collisions.

Notes: 1. Short frames are frames smaller than 64 bytes.

2. Long frames are frames longer than the maximum frame length configured for this port.

5.11.3 Port Monitoring

To solve network problems, selected traffic can be copied or mirrored to a mirror port where a frame analyzer can be attached to analyze the frame flow. The traffic to be copied to the mirror port is selected as follows:

- All frames received on a given port (also known as Ingress or Source Mirroring).
- All frames transmitted on a given port (also known as Egress or Destination Mirroring).
- Port to mirror is also known as the mirror port. Frames from ports that have either source (Rx) or destination (Tx) mirroring enabled are mirrored to this port.
- Disabled option means disabled mirroring.

You can configure Port Mirroring on this page (as shown below).

Mirror Configuration

Port to mirror to Disabled ▾

Mirror Port Configuration

Port	Mode
*	<> ▾
1	Disabled ▾
2	Disabled ▾
3	Disabled ▾
4	Disabled ▾
5	Disabled ▾
6	Disabled ▾
7	Disabled ▾
8	Disabled ▾
9	Disabled ▾
10	Disabled ▾
11	Disabled ▾

Figure 137 - Mirror Configuration interface

5.11.4 System Log Information

This page provides switch system log information.

System Log Information

Auto-refresh ☐ Refresh Clear |<< << >> >>|

The total number of entries is 0 for the given level.

Start from ID with entries per page.

ID	Time	Message
No system log entries		

Figure 138 - System Log Information interface

The following table describes the labels for the **System Log Information** screen.

Label	Description
ID	The ID (≥ 1) of the system log entry
Level	The level of the system log entry. The following level types are supported: Info : provides general information Warning : provides warning for abnormal operation Error : provides error message
Time	The time of the system log entry.
Message	The MAC address of the switch.
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Updates system log entries, starting from the current entry ID.
Clear	Flushes all system log entries.
<<	Updates system log entries, starting from the first available entry ID.
<<	Updates system log entries, ending at the last entry currently Displayed.
>>	Updates system log entries, starting from the last entry currently displayed.
>>	Updates system log entries, ending at the last available entry ID.

5.11.5 SFP Monitor

SFP modules with DDM (Digital Diagnostic Monitoring) function can measure the temperature of the apparatus, helping you monitor the status of connection and detect errors immediately. You can manage and set up event alarms through DDM Web interface.

SFP Monitor

Auto-refresh ☐

Port No.	Temperature (°C)	Vcc (V)	TX Bias(mA)	TX Power(μW)	RX Power(μW)
25	N/A	N/A	N/A	N/A	N/A
26	N/A	N/A	N/A	N/A	N/A

Warning Temperature :

°C(0~100)

Event Alarm :

☐ Syslog ☐ SMTP ☐ SNMP Trap

Figure 139 - SFP Monitor interface

The following table describes the labels for the **SFP Monitor** screen.

Label	Description
Port no	Port Number.
Temperature (°C)	Temperature of the SFP
Vcc (V)	Transceiver supply voltage
TX Bias (mA)	Transmitted laser bias current
TX Power (μW)	Transmit power of the SFP
RX Power (μW)	Receive power of the SFP
Warning Temperature	The temperature when the warning event is triggered. The warning temperature is 85C
Event Alarm:	
Syslog	Syslog method of notification will be used
SMTP	SMTP method of notification will be used
SNMP Trap	SNMP trap method of notification will be used
Auto-refresh	Check this box to enable an automatic refresh of the page at regular intervals.
Refresh	Updates system log entries, starting from the current entry ID.
Save	Click Save to save the changes

5.11.6 Ping

This page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues.

ICMP Ping

IP Address	0.0.0.0
Ping Length	56
Ping Count	5
Ping Interval	1

Start

Figure 140 - ICMP Ping

After you press **Start**, five ICMP packets will be transmitted, and the sequence number and roundtrip time will be displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

```
PING6 server ::10.10.132.20
```

```
64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms
```

```
64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms
```

64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms

Sent 5 packets, received 5 OK, 0 bad

You can configure the following properties of the issued ICMP packets:

The following table describes the labels for the **ICMP Ping** screen.

Label	Description
IP Address	The destination IP Address
Ping Length	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
Ping Count	The count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval	The interval of the ICMP packet. Values range from 0 second to 30 seconds.

5.11.7 Ping6

This page allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.

After you press **Start**, ICMPv6 packets are transmitted, and the sequence number and round trip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

PING6 server ::10.10.132.20, 56 bytes of data.

64 bytes from ::10.10.132.20: icmp_seq=0, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=1, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=2, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=3, time=0ms

64 bytes from ::10.10.132.20: icmp_seq=4, time=0ms

Sent 5 packets, received 5 OK, 0 bad

You can configure the following properties of the issued ICMP packets:

ICMPv6 Ping

IP Address	0:0:0:0:0:0:0:0
Ping Length	56
Ping Count	5
Ping Interval	1

Figure 141 - ICMPv6 Ping

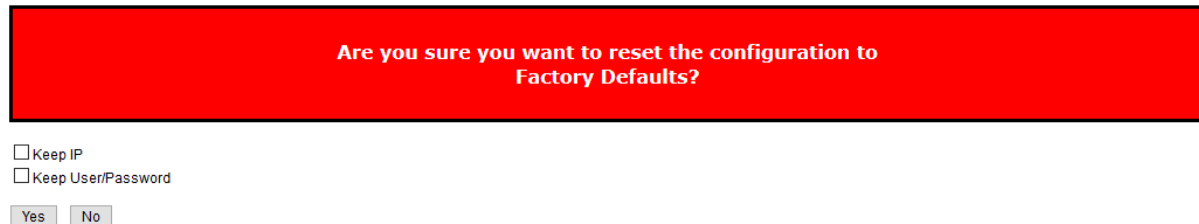
The following table describes the labels for the **ICMPv6 Ping** screen.

Label	Description
IP Address	The destination IP Address
Ping Length	The payload size of the ICMP packet. Values range from 2 bytes to 1452 bytes.
Ping Count	The count of the ICMP packet. Values range from 1 time to 60 times.
Ping Interval	The interval of the ICMP packet. Values range from 0 second to 30 seconds.

5.12 Factory Defaults

You can reset the configuration of the stack switch on this page. The IP configuration and/or User/Password are retained only if the respective boxes are checked when the switch is restored to factory defaults.

Factory Defaults



Are you sure you want to reset the configuration to Factory Defaults?

☐ Keep IP
☐ Keep User/Password

Yes No

Figure 142 - Factory Defaults

The following table describes the labels for the **Factory Defaults** screen.

Label	Description
Yes	Click Yes to reset the configuration to factory defaults.
No	Click No to return to the System Information page without resetting.

5.13 System Reboot

You can reset the stack switch on this page. After reset, the system will boot normally as if you have powered on the devices.

Restart Device



Are you sure you want to perform a Restart?

Yes No

Figure 143 - System Reboot interface

The following table describes the labels for the **System Reboot** screen

Label	Description
Yes	Click Yes to reset the configuration to factory defaults.
No	Click No to return to the System Information page without resetting.

To reset the iES26G switch to the default configuration, click **Reset** and all configurations will be reset to their default value.

You can select “**Keep current IP address setting**” and “**Keep current username & password**” to prevent from changing IP and username and password to the default.

5.14 Command Line Interface Management

Besides Web-based management, the iES6GF also supports Command Line Interface (CLI) management. Use either the Console port or Telnet to manage the switch via the CLI. Details are shown below.

5.14.1 CLI Management by RS-232 Serial Console (115200, 8, none, 1, none)

Before configuring RS-232 serial console, connect the RS-232 port of the switch to your PC Com port using a RJ45 to DB9-F cable.

Follow the steps below to access the console via RS-232 serial cable.

- 1) Start **Tera Term** (or another terminal emulator) application.



- 2) Under **Setup** select **Serial Port**.

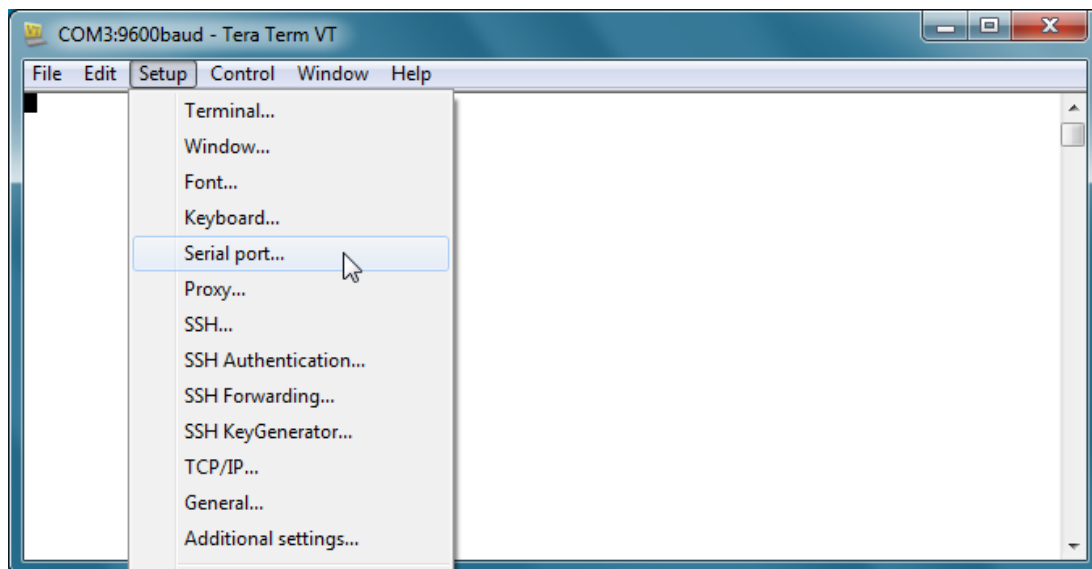


Figure 144 - Tera Term VT interface

- 3) Select the COM Port used by your PC to connect to the Console Port. Set the rest of the properties to: **115200** for Baud rate, **8** for Data bits, **None** for Parity, **1** for Stop bits, and **none** for Flow control. Then, click **OK**.

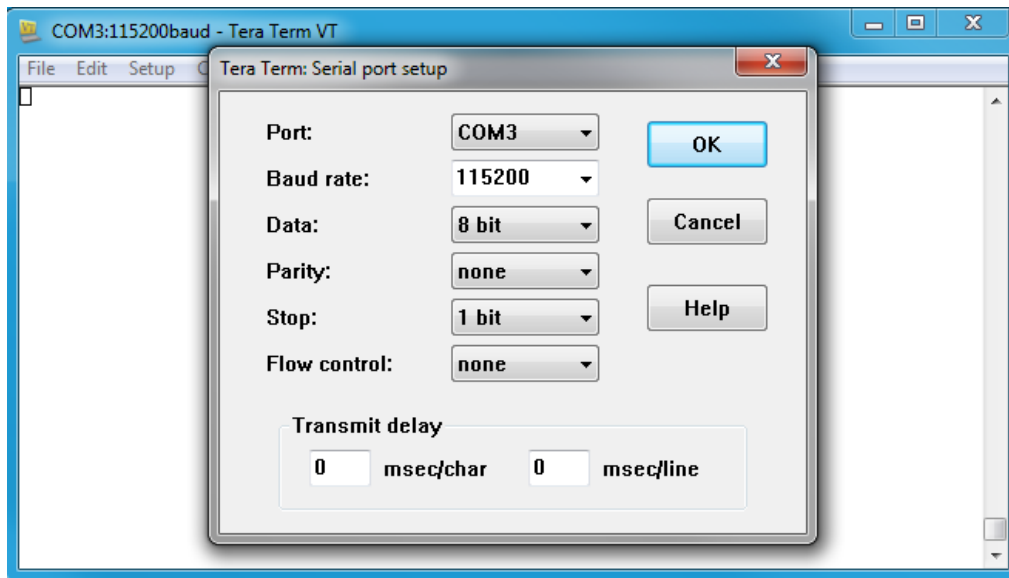


Figure 145 - Tera Term: Serial port setup interface

- 4) Press **Enter** for the **Console login screen** to appear. Use the keyboard to enter the Console Username and Password which is same as the Web Browser password (**admin** for both), then press **Enter**.

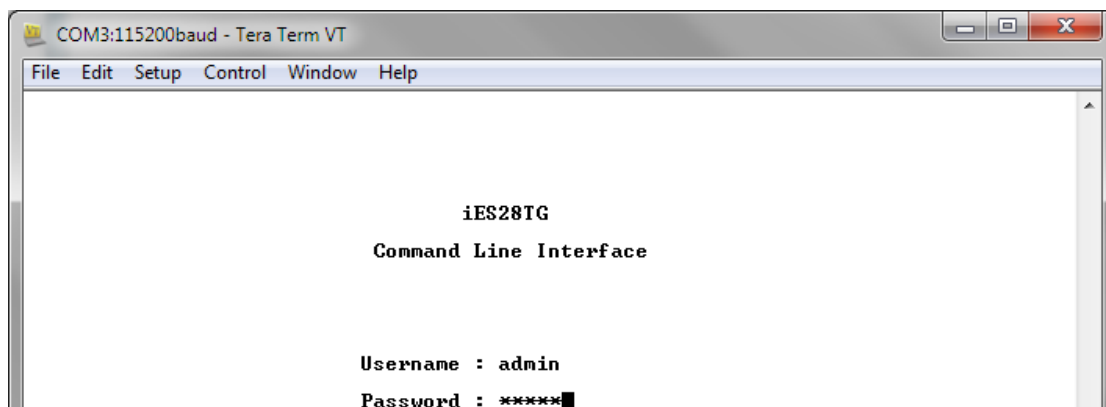


Figure 146 - Console Login Screen

5.14.2 CLI Management by Telnet

You can use **Telnet** to configure the switch. The default values are:

IP Address: **192.168.10.1**

Subnet Mask: **255.255.255.0**

Default Gateway: **192.168.10.254**

User Name: **admin**

Password: **admin**

Follow the steps below to access the console via Telnet.

- 1) Connect your PC to one of the Ethernet ports of the switch via an Ethernet cable.
- 2) Telnet to the IP address of the switch from the Windows **Run** command (or from the MS-DOS prompt).

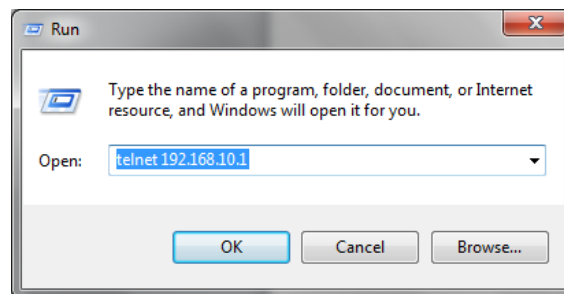


Figure 147 - Windows Run interface

- 3) The Console login screen appears. Use the keyboard to enter the Console's Username and Password, then press Enter. Note that these Username and Password are the same as the ones used for the Web Management. The default Username is "admin" and the default Password is "admin".

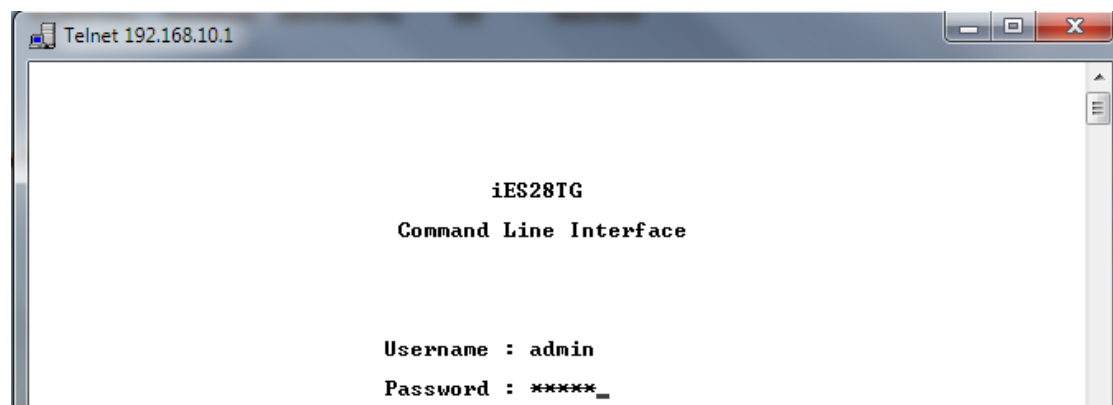


Figure 148 - Telnet Login Screen

1) Command Groups

Welcome to iES26GF Command Line Interface.

Type 'help' or '?' to get help.

>?

General Commands:

Help/?: Get help on a group or a specific command

Up : Move one command level up

Logout: Exit CLI

Command Groups:

System	: System settings and reset options
IP	: IP configuration and Ping
Port	: Port management
MAC	: MAC address table
VLAN	: Virtual LAN
PVLAN	: Private VLAN
Security	: Security management
STP	: Spanning Tree Protocol
Aggr	: Link Aggregation
LACP	: Link Aggregation Control Protocol
LLDP	: Link Layer Discovery Protocol
QoS	: Quality of Service
Mirror	: Port mirroring
Config	: Load/Save of configuration via TFTP
Firmware	: Download of firmware via TFTP
PTP	: IEEE1588 Precision Time Protocol
Loop Protect	: Loop Protection
IPMC	: MLD/IGMP Snooping
Fault	: Fault Alarm Configuration
Event	: Event Selection
DHCP Server	: DHCP Server Configuration
RIP	: Routing Information Protocol
iRing	: iRing Configuration
iChain	: iChain Configuration
iBridge	: iBridge Configuration
RCS	: Remote Control Security
Fastrecovery	: Fast-Recovery Configuration
SFP	: SFP Monitor Configuration
DeviceBinding	: Device Binding Configuration
MRP	: MRP Configuration
Modbus	: Modbus TCP Configuration
RSTP	: RSTP Configuration

Type '<group>' to enter command group, e.g. 'port'.

Type '<group> ?' to get list of group commands, e.g. 'port ?'.

Type '<command> ?' to get help on a command, e.g. 'port mode ?'.

Commands may be abbreviated, e.g. 'por co' instead of 'port configuration'.

2) System

System>	Configuration [all] [<port_list>]
	Name [<name>]
	Description [<description>]
	Contact [<contact>]
	Location [<location>]
	Version
	Log Configuration
	Log Level [info warning error]
	Log Server Mode [enable disable]
	Log Server Address [<ip_addr_string>]
	Log Lookup [<log_id>] [all info warnup]
	Log Lookup [<log_id>] [all info warning error]
	Log Clear [all info warning error]
	Timezone Configuration
	Timezone Offset [<offset>]
	Timezone Acronym [<acronym>]
	DST Configuration
	DST Mode [disable recurring non-recurring]
	DST start <week> <day> <month> <date> <year> <hour>
	DST end <week> <day> <month> <date> <year> <hour> <minute>
	DST Offset [<dst_offset>]
	Reboot
	Restore Default [keep_ip]
	Load

3) IP

IP>	Address <vlan> <ip_ifaddr>
	Address Delete <vlan> <ip_ifaddr>
	Configuration
	DHCP <vlan> [enable disable]
	DHCP fallback timeout <vlan> [<value>]
	DHCP retry <vlan>
	Interface add <vlan_list>
	Interface delete [<vlan_list>]
	Interface list [<vlan_list>]
	Mode [host router]
	Neighbour Clear

	Neighbour List
	Ping <ip_target> [(Length <ping_length>)] [(Count <ping_count>)]
	[(Interval <ping_interval>)]
	Route Add <ip_net> <ip_gateway>
	Route Delete <ip_net> <ip_gateway>
	Route List
	SNTP Configuration
	SNTP Mode [enable disable]
	SNTP Server Add <ip_addr string>
	SNTP Server Delete

4) Port

Port>	Configuration [<port_list>] [up down]
	Mode [<port_list>]
	[auto 10hdx 10fdx 100hdx 100fdx 1000fdx 10gfdx]
	State [<port_list>] [enable disable]
	MaxFrame [<port_list>] [<max_frame>]
	Excessive [<port_list>] [discard restart]
	Statistics [<port_list>] [<command>] [up down]
	VeriPHY [<port_list>]
	SFP [<port_list>]

5) MAC

MAC>	Configuration [<port_list>]
	Add <mac_addr> <port_list> [<vid>]
	Delete <mac_addr> [<vid>]
	Lookup <mac_addr> [<vid>]
	Agetime [<age_time>]
	Learning [<port_list>] [auto disable secure]
	Dump [<mac_max>] [<mac_addr>] [<vid>]
	Statistics [<port_list>]
	Flush

6) VLAN

VLAN >	Configuration [<port_list>]
	PVID [<port_list>] [<vid> none]
	FrameType [<port_list>] [all tagged untagged]
	IngressFilter [<port_list>] [enable disable]
	tx_tag [<port_list>] [untag_pvid untag_all tag_all]
	PortType [<port_list>] [unaware c-port s-port s-custom-port]
	EtypeCustomSport [<etype>]
	Add <vid> <name> [<ports_list>]
	Forbidden Add <vid> <name> [<port_list>]
	Delete <vid> <name>
	Forbidden Delete <vid> <name>
	Forbidden Lookup [<vid>] [(name <name>)]
	Lookup [<vid>] [(name <name>)] [combined static nas all]
	Name Add <name> <vid>
	Name Delete <name>
	Name Lookup [<name>]
	Status [<port_list>] [combined static nas mstp all conflicts]

7) Private VLAN

PVLAN >	Configuration [<port_list>]
	Add <pvlan_id> [<port_list>]
	Delete <pvlan_id>
	Lookup [<pvlan_id>]
	Isolate [<port_list>] [enable disable]

8) Security

Security >	Switch Switch security setting
	Network Network security setting
	AAA Authentication, Authorization and Accounting setting

9) Security Switch

Security/switch>	Password <password>	
	Auth	Authentication
	SSH	Secure Shell
	HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
	RMON	Remote Network Monitoring

10) Security Switch Authentication

Security/switch/auth>	Configuration	
	Console [no local radius] [local radius]	
	Telnet [no local radius] [local radius]	
	SSH [no local radius] [local radius]	
	HTTP [no local radius] [local radius]	

11) Security Switch SSH

Security/switch/SSH>	Configuration	
	Mode [enable disable]	

12) Security Switch HTTPS

Security/switch/HTTPS>	Configuration	
	Mode [enable disable]	
	Redirect [enable disable]	

13) Security Switch RMON

Security/switch/RMON>	Statistics Add <stats_id> <data_source>		
	Statistics Delete <stats_id>		
	Statistics Lookup [<stats_id>]		
	History Add <history_id> <data_source> [<interval>][<buckets>]		
	History Delete <history_id>		
	History Lookup [<history_id>]		
	Alarm Add <alarm_id> <interval> <alarm_variable> [absolute delta] <rising_threshold> <rising_event_index> <falling_threshold> <falling_event_index> [rising falling both]		
	Alarm Delete <alarm_id>		
	Alarm Lookup [<alarm_id>]		
	Event	Add	<event_id> [none log trap log_trap] [<community>][<description>]
	Event Delete <event_id>		
	Event Lookup [<event_id>]		

14) **Security Network**

Security/Network >	Psec	Port Security Status
	NAS	Network Access Server (IEEE 802.1X)
	ACL	Access Control List

15) **Security Network Psec**

Security/Network / Psec>	Switch [<port_list>]
	Port [<port_list>]

16) **Security Network NAS**

Security/Network /NAS>	Configuration [<port_list>]
	Mode [enable disable]
	State [<port_list>] [auto authorized unauthorized macbased]
	Reauthentication [enable disable]
	ReauthPeriod [<reauth period>]
	EapolTimeout [<eapol timeout>]
	Agetime [<age time>]
	Holdtime [<hold time>]
	Authenticate [<port_list>] [now]
	Statistics [<port_list>] [clear eapol radius]

17) **Security Network ACL**

Security/Network/ ACL>	Configuration [<port_list>]
	Action [<port_list>] [permit deny] [<rate_limiter>][<port_redirect>] [<mirror>] [<logging>] [<shutdown>]
	Policy [<port_list>] [<policy>]
	Rate [<rate_limiter_list>] [<rate_unit>] [<rate>]up
	Add [<ace_id>] [<ace_id_next>] [(port <port_list>)] [(policy <policy> <policy_bitmask>)][<tagged>] [<vid>] [<tag_prio>] [<dmac_type>][(etype [<etype>] [<smac>] [<dmac>])] (arp [<sip>] [<dip>] [<smac>] [<arp_opcode>] [<arp_flags>]) (ip [<sip>] [<dip>] [<protocol>] [<ip_flags>]) (icmp [<sip>] [<dip>] [<icmp_type>] [<icmp_code>] [<ip_flags>]) (udp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>]) (tcp [<sip>] [<dip>] [<sport>] [<dport>] [<ip_flags>] [<tcp_flags>]) (ipv6_std [<next_header>] [<sip_v6>] [<sip_v6_mask>])) [permit deny] [<rate_limiter>] [<port_redirect>] [<mirror>] [<logging>][<shutdown>]
	Delete <ace_id>
	Lookup [<ace_id>]
	Clear
	Status [combined static loop_protect dhcp ipmc conflicts]
	Port State [<port_list>] [enable disable]

18) Security Network DHCP

Security/Network /DHCP>	Configuration
	Mode [enable disable]
	19) Server [<ip_addr>]
	Information Mode [enable disable]
	Information Policy [replace keep drop]
	Statistics [clear]

20) Security AAA

Security/AAA>	Configuration
	Radius-server timeout [<timeout>]
	Radius-server retransmit [<retransmit>]
	Radius-server deadtime [<deadtime>]
	radius-server key [<key>]
	radius-server nas-ip-address [<ipv4_addr> disable]
	radius-server nas-identifier [<id>]
	radius-server host add <ip_addr_string> [<auth_port>] [<acct_port>] [<timeout>] [<retransmit>] [<key>]
	radius-server host delete <ip_addr_string> [<auth_port>] [<acct_port>]
	radius-server host show
	radius-server statistics [<host_index>]

21) **STP**

STP>	Configuration
	Version [<stp_version>]
	Txhold [<holdcount>]
	MaxHops [<maxhops>]
	MaxAge [<max_age>]
	FwdDelay [<delay>]
	bpduFilter [enable disable]
	bpduGuard [enable disable]
	recovery [<timeout>]
	CName [<config-name>] [<integer>]
	Status [<msti>] [<port_list>]
	Msti Priority [<msti>] [<priority>]
	Msti Map [<msti>] [clear]
	Msti Add <msti> <vid>
	Port Configuration [<stp_port_list>]
	Port Mode [<stp_port_list>] [enable disable]
	Port Edge [<stp_port_list>] [enable disable]
	Port AutoEdge [<stp_port_list>] [enable disable]
	Port P2P [<stp_port_list>] [enable disable auto]
	Port RestrictedRole [<stp_port_list>] [enable disable]
	Port RestrictedTcn [<stp_port_list>] [enable disable]
	Port bpduGuard [<stp_port_list>] [enable disable]
	Port Statistics [<stp_port_list>] [clear]
	Port Mcheck [<stp_port_list>]
	Msti Port Configuration [<msti>] [<stp_port_list>]
	Msti Port Cost [<msti>] [<stp_port_list>] [<path_cost>]
	Msti Port Priority [<msti>] [<stp_port_list>] [<priority>]

22) **Aggr**

Aggr>	Configuration
	Add <port_list> [<aggr_id>]
	Delete <aggr_id>
	Lookup [<aggr_id>]
	Mode [smac dmac ip port] [enable disable]

23) **LACP**

LACP>	Configuration [<port_list>]
	Mode [<port_list>] [enable disable]
	Key [<port_list>] [<key>]
	Prio [<port_list>] [<prio>]
	System Prio [<sysprio>]
	Role [<port_list>] [active passive]
	Status [<port_list>]
	Statistics [<port_list>] [clear]
	Timeout [<port_list>] [fast slow]

24) **LLDP**

LLDP>	Configuration [<port_list>]
	Mode [<port_list>] [enable disable]
	Optional_TLV [<port_list>]
	[<port_descr> <sys_name> <sys_descr> <sys_capa> <mgmt_addr>]
	Interval [<interval>]
	Hold [<hold>]
	Delay [<delay>]
	Reinit [<reinit>]
	Statistics [<port_list>] [clear]
	Info [<port_list>]

25) **QoS**

QoS>	Configuration [<port_list>]
	Port Classification Class [<port_list>] [<class>]
	Port Classification DPL [<port_list>] [<dpl>]
	Port Classification PCP [<port_list>] [<pcp>]
	Port Classification DEI [<port_list>] [<dei>]
	Port Classification Tag [<port_list>] [enable disable]
	Port Classification Map [<port_list>] [<pcp_list>] [<dei_list>]
	[<class>] [<dpl>]
	Port Classification DSCP [<port_list>] [enable disable]
	Port Policer Mode [<port_list>] [enable disable]
	Port Policer Rate [<port_list>] [<rate>]
	Port Policer Unit [<port_list>] [kbps fps]

Port QueuePolicer Mode	[<port_list>]	[<queue_list>]
Port QueuePolicer Rate	[<port_list>]	[<queue_list>] [<bit_rate>]
Port Scheduler Mode	[<port_list>]	[strict weighted]
Port Scheduler Weight	[<port_list>]	[<queue_list>] [<weight>]
Port Shaper Mode	[<port_list>]	[enable disable]
Port Shaper Rate	[<port_list>]	[<bit_rate>]
Port QueueShaper Mode	[<port_list>]	[<queue_list>]
Port QueueShaper Rate	[<port_list>]	[<queue_list>] [<bit_rate>]
Port QueueShaper Excess	[<port_list>]	[<queue_list>]
Port TagRemarking Mode	[<port_list>]	
Port TagRemarking PCP	[<port_list>]	[<pcp>]
Port TagRemarking DEI	[<port_list>]	[<dei>]
Port TagRemarking DPL	[<port_list>]	[<dpl>] [<dpl>] [<dpl>]
Port TagRemarking Map	[<port_list>]	[<class_list>] [<dpl_list>]
Port DSCP Translation	[<port_list>]	[enable disable]
Port DSCP Classification	[<port_list>]	[none zero selected all]
Port DSCP EgressRemark	[<port_list>]	[disable enable remap]
DSCP Map	[<dscp_list>]	[<class>] [<dpl>]
DSCP Translation	[<dscp_list>]	[<trans_dscp>]
DSCP Trust	[<dscp_list>]	[enable disable]
DSCP Classification Mode	[<dscp_list>]	[enable disable]
DSCP Classification Map	[<class_list>]	[<dpl_list>] [<dscp>]
DSCP EgressRemap	[<dscp_list>]	[<dpl_list>] [<dscp>]
Port Storm Unicast	[<port_list>]	[enable disable] [<rate>]
Storm Multicast	[enable disable]	[<packet_rate>]
Port Storm Broadcast	[<port_list>]	[enable disable] [<rate>] [kbps fps]
Port Storm Unknown	[<port_list>]	[enable disable] [<rate>] [kbps fps]
WRED	[<queue_list>]	[enable disable] [<min_th>] [<mdp_1>] [<mdp_2>] [<mdp_3>]
QCL Add	[<qce_id>]	[<qce_id_next>] [<port_list>] [<tag>] [<vid>] [<pcp>] [<dei>] [<smac>] [<dmac_type>] [(etype [<etype>]) (LLC [<DSAP>] [<SSAP>] [<control>]) (SNAP [<PID>]) (ipv4 [<protocol>] [<sip>] [<dscp>] [<fragment>] [<sport>]

	[<dport>)]
	(ipv6 [<protocol>] [<sip_v6>] [<dscp>] [<sport>] [<dport>])]
	[<class>] [<dp>] [<classified_dscp>]
	QCL Delete <qce_id>
	QCL Lookup [<qce_id>]
	QCL Status [combined static conflicts]
	QCL Refresh

26) **Mirror**

Mirror>	Configuration [<port_list>]
	Port [<port> disable]
	Mode [<port_list>] [enable disable rx tx]

27) **Config**

Config>	Save <ip_server> <file_name>
	Load <ip_server> <file_name> [check]

28) **SNMP**

SNMP>	Configuration
	Mode [enable disable]
	Version [1 2c 3]
	Read Community [<community>]
	Write Community [<community>]
	Engine ID [<engineid>]
	Community Add <community> [<ip_addr>] [<ip_mask>]
	Community Delete <index>
	Community Lookup [<index>]
	User Add <engineid> <user_name> [MD5 SHA] [<auth_password>] [DES AES] [<priv_password>]
	User Delete <index>
	User Changekey <engineid> <user_name> <auth_password> [<priv_password>]

	User Lookup [<index>]
	Group Add <security_model> <security_name> <group_name>
	Group Delete <index>
	Group Lookup [<index>]
	View Add <view_name> [included excluded] <oid_subtree>
	View Delete <index>
	View Lookup [<index>]
	Access Add <group_name> <security_model> <security_level> [<read_view_name>] [<write_view_name>]
	Access Delete <index>
	Access Lookup [<index>]
	Trap Mode [enable disable]
	Trap Lookup [<conf_name>]
	Trap Add <conf_name> [enable disable] [(dip <ipv4v6_addr>)] [(dport <udp_port>)](((1) [(community <comm>))] (((2c [(community <comm>))] [(trap) (informs [<retries> [<timeout>]])) ((3) [(trap) (informs [<retries>] [<timeout>]] [(probe) (engine <engineid>)] [(security <security_name>)]))]
	Trap Delete <conf_name>
	Trap Event Lookup [<conf_name>]
	Trap Event System Warm-start [<conf_name>] [enable disable]
	Trap Event System Cold-start [<conf_name>] [enable disable]
	Trap Event Interface Link-up [<conf_name>] [<port_list> [enable disable]
	Trap Event Interface Link-down [<conf_name>] [<port_list> [enable disable]
	Trap Event Interface LLDP [<conf_name>] [enable disable]
	Trap Event AAA Authentication-Failure [<conf_name> [enable disable]
	Trap Event Switch STP [<conf_name>] [enable disable]
	Trap Event Switch RMON [<conf_name>] [enable disable]

29) **Firmware**

Firmware>	Load <ip_addr_string> <file_name>
	NetLoad <url>
	Information
	Swap

30) **Loop Protect**

Loop Protect> Port	Configuration
	Mode [enable disable]
	Transmit [<transmit-time>]
	Shutdown [<shutdown-time>]
	Configuration [<port_list>]
	Port Mode [<port_list>] [enable disable]
	Port Action [<port_list>] [shutdown shut_log log]
	Port Transmit [<port_list>] [enable disable]
	Status [<port_list>]

31) **IPMC**

IPMC>	Configuration [igmp]
	Mode [igmp] [enable disable]
	Flooding [igmp] [enable disable]
	VLAN Add [igmp] <vid> up
	VLAN Delete [igmp] <vid>
	State [igmp] [<vid>] [enable disable]
	Querier [igmp] [<vid>] [enable disable]
	Fastleave [igmp] [<port_list>] [enable disable]
	Router [igmp] [<port_list>] [enable disable]
	Status [igmp] [<vid>]
	Groups [igmp] [<vid>]
	Version [igmp] [<vid>]

32) **Fault**

Fault>	Alarm PortLinkDown [<port_list>] [enable disable]
	Alarm PowerFailure [pwr1 pwr2 pwr3] [enable disable]

33) **Event**

Event>	Configuration
	Syslog SystemStart [enable disable]
	Syslog PowerStatus [enable disable]
	Syslog SnmpAuthenticationFailure [enable disable]
	Syslog RingTopologyChange [enable disable]
	Syslog Port [<port_list>] [disable linkup linkdown both]

34) **DHCP Server**

DHCP Server>	Mode [enable disable]
	Setup [<ip_start>] [<ip_end>] [<ip_mask>] [<ip_router>]
	[<ip_dns>] [<ip_tftp>] [<lease>] [<bootfile>]

35) **RIP**

RIP>	Configuration
	Mode [enable disable]

36) **Ring**

Ring>	Mode [enable disable]
	Master [enable disable]
	1stRingPort [<port>]
	2ndRingPort [<port>]
	Couple Mode [enable disable]
	Couple Port [<port>]
	Dualhoming Mode [enable disable]
	Dualhoming Port [<port>]

37) **Chain**

Chain>	Configuration
	Mode [enable disable]
	1stUplinkPort [<port>]
	2ndUplinkPort [<port>]
	EdgePort [1st 2nd none]

38) **RCS**

RCS>	Mode [enable disable]
	Add [<ip_addr>] [<port_list>] [web_on web_off] [telnet_on telnet_off] [snmp_on snmp_off]
	Del <index>
	Configuration

39) **FastRecovery**

FastRecovery>	Mode [enable disable]
	Port [<port_list>] [<fr_priority>]

40) **DualPort**

DualPort>	Configuration
	Mode [enable disable]
	Interval <integer>
	Retry <integer>
	TimeoutDelay <integer>
	DebugMessage [enable disable]

41) **O-Ring**

Open-Ring>	Configuration [enable disable]
	Port <port>
	1stUplinkPort [<port>]
	2ndUplinkPort [<port>]
	Vender [moxx advantexx hirschmaxx]

42) **SFP**

SFP>	syslog [enable disable]
	temp [<temperature>]
	Info

43) Device Binding

DeviceBinding>	Mode [enable disable]
	Port Mode [<port_list>] [disable scan binding shutdown]
	Port DDOS Mode [<port_list>] [enable disable]
	Port DDOS Sensibility [<port_list>] [low normal medium high]
	Port DDOS Packet [<port_list>] [rx_total rx_unicast rx_multicast rx_broadcast tcp udp]
	Port DDOS Low [<port_list>] [<socket_number>]
	Port DDOS High [<port_list>] [<socket_number>]
	Port DDOS Filter [<port_list>] [source destination]
	Port DDOS Action [<port_list>] [do_nothing block_1_min block_10_mins block shutdown only_log]
	Port DDOS Status [<port_list>]
	Port Alive Mode [<port_list>] [enable disable]
	Port Alive Action [<port_list>] [do_nothing link_change shutdown only_log]
	Port Alive Status [<port_list>]
	Port Stream Mode [<port_list>] [enable disable]
	Port Stream Action [<port_list>] [do_nothing only_log]
	Port Stream Status [<port_list>]
	Port Addr [<port_list>] [<ip_addr>] [<mac_addr>]
	Port Alias [<port_list>] [<ip_addr>]
	Port DeviceType [<port_list>] [unknown ip_cam ip_phone ap pc plc nvr]
	Port Location [<port_list>] [<device_location>]
	Port Description [<port_list>] [<device_description>]

44) Modbus

Modbus	Status
	Mode [enable disable]

45) **MRP**

MRP	Status
	MRP Mode [enable disable]
	MRP Manager [enable disable]
	MRP React [enable disable]
	MRP 1stRingPort [<mrp_port>]
	MRP 2ndRingPort [<mrp_port>]
	MRP Parameter MRP_TOPchgT [<value>]
	MRP Parameter MRP_TOPNRmax [<value>]
	MRP Parameter MRP_TSTshortT [<value>]
	MRP Parameter MRP_TSTdefaultT [<value>]
	MRP Parameter MRP_TSTNRmax [<value>]
	MRP Parameter MRP_LNKdownT [<value>]
	MRP Parameter MRP_LNKupT [<value>]
	MRP Parameter MRP_LNKNRmax [<value>]

APPENDIX A: IES26GF MODBUS INFORMATION

*Device ID/PLC is 1

*04 Read Input Register (3x) should be used.

*The returned values are in hex format

Address	Description
16	VendorName
48	ProductName
81	Version
85	MacAddress
256	SysName
512	SysDescription
768	SysLocation
1024	SysContact
4096	PortStatus: Port :1~VTSS_PORTS Value :0x0000 Link down 0x0001 Link up 0x0002 Disable 0xffff NoPort
4352	PortSpeed: Port :1~VTSS_PORTS Value :0x0000 10M-Half 0x0001 10M-Full 0x0002 100M-Half 0x0003 100M-Full 0x0004 1G-Half 0x0005 1G-Full 0xffff NoPort
4608	PortFlowCtrl : Port :1~VTSS_PORTS Value :0x0000 Off 0x0001 On 0xffff NoPort