BeWARD
SAFETY & SECURITY

User's Manual

8/16/24-Port 10/100Mbps 802.3at PoE + 2-Port Gigabit TP/SFP Combo Managed PoE+ Switch

► **STW-822HP / STW-1622HP / STW-2422HP**

SEC.RU | Короткий путь к информации

Скачано с sec.ru

Trademarks

Copyright © BEWARD Co., Ltd. 2023.
Contents are subject to revision without prior notice.
BEWARD is a registered trademark of BEWARD Co., Ltd. All other trademarks belong to their respective owners.

Disclaimer

BEWARD does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose. BEWARD has made every effort to ensure that this User's Manual is accurate; BEWARD disclaims liability for any inaccuracies or omissions that may have occurred.

Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of BEWARD. BEWARD assumes no responsibility for any inaccuracies that may be contained in this User's Manual. BEWARD makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements to this User's Manual and/or to the products described in this User's Manual, at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

FCC Warning

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

CE Mark Warning

This device is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

Energy Saving Note of the Device

This power required device does not support Standby mode operation. For energy saving, please remove the power cable to disconnect the device from the power circuit. In view of saving the energy and reducing the unnecessary power consumption, it is strongly suggested to remove the power connection for the device if this device is not intended to be active.

WEEE Warning

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

TABLE OF CONETNTS

1. INTRODUCTION 8

1.1 Packet Contents 8

1.2 Product Description 9

1.3 How to Use This Manual 13

1.4 Product Features 14

1.5 Product Specifications 17

2. INSTALLATION 23

2.1 Hardware Description 23

2.1.1 Switch Front Panel 23

2.1.2 LED Indications 25

2.1.3 Switch Rear Panel 28

2.2 Install the Switch 29

2.2.1 Desktop Installation 29

2.2.2 Rack Mounting 30

2.2.3 Installing the SFP Transceiver 31

3. SWITCH MANAGEMENT 33

3.1 Requirements 33

3.2 Management Access Overview 34

3.3 Administration Console 35

3.4 Web Management 37

3.5 SNMP-Based Network Management 38

3.6 BEWARD Smart Discovery Utility 39

4. WEB CONFIGURATION 41

4.1 Main Web Page 44

4.2 System 48

4.2.1 System Information 49

4.2.2 User Configuration 50

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.2.3 IP Configuration 51
4.2.3.1 IPv4 51
4.2.3.2 IPv6 51
4.2.4 SNMP Settings 52
4.2.4.1 SNMP View Table 54
4.2.4.2 SNMP Group Table 55
4.2.4.3 SNMP User Table 56
4.2.4.4 SNMP Community Table 57
4.2.4.5 SNMP Host Table 58
4.2.4.6 SNMP Configuration 59
4.2.5 NTP Settings 60
4.2.6 Syslog Settings 61
4.2.7 Factory Default 62
4.2.8 Configuration 63
4.2.8.1 Backup 63
4.2.8.2 Restoration 63
4.2.9 Firmware Update 64

4.3 PoE Configuration 65
4.3.1 PoE Port Settings 66
4.3.2 PoE Alive Check 67
4.3.3 PoE Port Sequential 69
4.3.4 PoE Schedule 70

4.4 Basic Configuration 72
4.4.1 Port Configuration 73
4.4.2 Port Mirroring 75
4.4.3 Broadcast Storm Control 77
4.4.4 Bandwidth Control 79

4.5 VLAN Configuration 80
4.5.1 VLAN Overview 80
4.5.2 IEEE 802.1Q VLAN 82
4.5.3 VLAN Mode 87
4.5.4 VLAN Group-based Entry Config 88
4.5.5 VLAN Tag-based Entry Config 89
4.5.6 VLAN Port Config 92
4.5.7 Protocol VLAN Config 95
4.5.8 Q-in-Q Port Config 96
4.5.9 Q-in-Q Index Config 98

4.6 QoS Configuration 100

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.6.1 Understanding QoS 100
4.6.2 QoS Group Member 102
4.6.3 QoS Mode Set 103
4.6.4 QoS Out Queue Aging 104
4.6.5 QoS Remap 105
4.6.6 Class of Service 106
4.6.7 802.1p-based QoS 107
4.6.8 DSCP-based Priority 108
4.6.9 TCP/UDP Port-based QoS 109

4.7 ACL Configuration 110
4.7.1 Understanding ACL 110
4.7.2 ACL Profile List 111
4.7.2.1 MAC 113
4.7.2.2 IP 115
4.7.2.3 IP_EXT 116
4.7.2.4 IPv6 118
4.7.2.5 Advanced 119
4.7.3 ACL Ctag Settings 121
4.7.4 ACL Stag Settings 122
4.7.5 ACL VLAN Settings 123
4.7.6 ACL Bandwidth Settings 124
4.7.7 ACL DSCP Settings 125

4.8 Security 126
4.8.1 Access Security 127
4.8.2 Port-MAC-IP Binding 128
4.8.2.1 Port-MAC-IP Port Setting 128
4.8.2.2 Port-MAC-IP Entry Setting 130
4.8.2.3 DHCP Snooping Entry Setting 132
4.8.3 MAC Address Binding 133

4.9 Advanced Features 136
4.9.1 Spanning Tree Protocol 137
4.9.1.1 STP Global Settings 144
4.9.1.2 STP Port Settings 145
4.9.1.3 MST Configuration Identification 146
4.9.1.4 STP Instance Settings 147
4.9.1.5 MSTP Port Information 148
4.9.1.6 STP Loop Detect Settings 149
4.9.2 Trunk & Link Aggregation 150

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.3 IGMP Snooping 154
4.9.3.1 IGMP Snooping Settings 158
4.9.3.2 IGMP Snooping Router Ports Settings 159
4.9.3.3 IGMP Snooping Groups 160
4.9.3.4 IGMP Snooping Ports 161
4.9.4 MLD Snooping 162
4.9.4.1 MLD Snooping Settings 162
4.9.4.2 MLD Snooping Router Ports Settings 163
4.9.4.3 MLD Snooping Groups 164
4.9.4.4 MLD Snooping Ports 165
4.9.5 DHCP Relay Agent 166
4.9.6 Loop Detect 169
4.9.7 GVRP 171
4.9.8 Neighbor MAC ID Settings 172
4.9.9 Voice VLAN Setting 173
4.9.9.1 Voice VLAN State 173
4.9.9.2 Voice VLAN Port Setting 174
4.9.9.3 OUI List 175
4.9.10 LLDP 176
4.9.10.1 LLDP Global Setting 176
4.9.10.2 LLDP Port Setting 178

4.10 Monitoring 180
4.10.1 MIB Counter 181
4.10.2 Scan MAC ID Lookup Table 184
4.10.3 LLDP Remote MIB 185
4.10.4 Syslog 186
4.10.5 CPU Resource Utilization 187

5. COMMAND LINE INTERFACE 188

5.1 Accessing the CLI 188
Logging on to the Console 188
Configure IP Address 188

5.2 Telnet Login 190

6. Command Line Mode 191

6.1 Clear Command 192

6.2 Config Command 192

SEC.RU | Короткий путь к информации
Скачано с sec.ru

6.3 Create Command 193

6.4 Default Command 193

6.5 Delete Command 194

6.6 Disable Command 194

6.7 Enable Command 195

6.8 Exit Command 195

6.9 Reboot Command 195

6.10 Restart Command 196

6.11 Save Command 196

6.12 Show Command 196

7. SWITCH OPERATION 198

7.1 Address Table 198

7.2 Learning 198

7.3 Forwarding & Filtering 198

7.4 Store-and-Forward 198

7.5 Auto-Negotiation 199

8. Power over Ethernet Overview 200

9. TROUBLESHOOTING 201

APPENDIX A: Networking Connection 203

A.1 PoE RJ45 Port Pin Assignments 203

A.2 Switch's Data RJ45 Pin Assignments -- 1000Mbps, 1000BASE-T 203

A.3 10/100Mbps, 10/100BASE-TX 203

APPENDIX B: GLOSSARY 205

SEC.RU | Короткий путь к информации
Скачано с sec.ru

1. INTRODUCTION

BEWARD 8/16/24-port 10/100Mbps 802.3at PoE + 2-port Gigabit TP/SFP Combo Managed PoE+ Switch Series, STW-822HP, STW-1622HP, STW-2422HP, comes with the multi-port Fast Ethernet Switch and SFP fiber optic connectibility and robust Layer 2 features. The descriptions of this series are shown below:

STW-822HP	8-Port 10/100TX 802.3at PoE + 2-Port Gigabit TP/SFP Combo Managed Ethernet Switch (120W)
STW-1622HP	16-Port 10/100TX 802.3at PoE + 2-Port Gigabit TP/SFP Combo Managed Ethernet Switch (240W)
STW-2422HP	24-Port 10/100TX 802.3at PoE + 2-Port Gigabit TP/SFP Combo Managed Ethernet Switch (240W)

"**Managed PoE+ Switch**" is used as an alternative name in this user's manual.

1.1 Packet Contents

Open the box of the Managed PoE+ Switch and carefully unpack it. The box should contain the following items:

- ☑ **The Managed PoE+ Switch** x 1
- ☑ **Quick Installation Guide** x 1
- ☑ **RS232 to RJ45 Console Cable** x 1
- ☑ **Rubber Feet** x 4
- ☑ **Rack Mount Accessory Kit** x 1
- ☑ **Power Cord** x 1
- ☑ **SFP Dust-proof Caps** x 2

If any of these are missing or damaged, please contact your dealer immediately;.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

1.2 Product Description

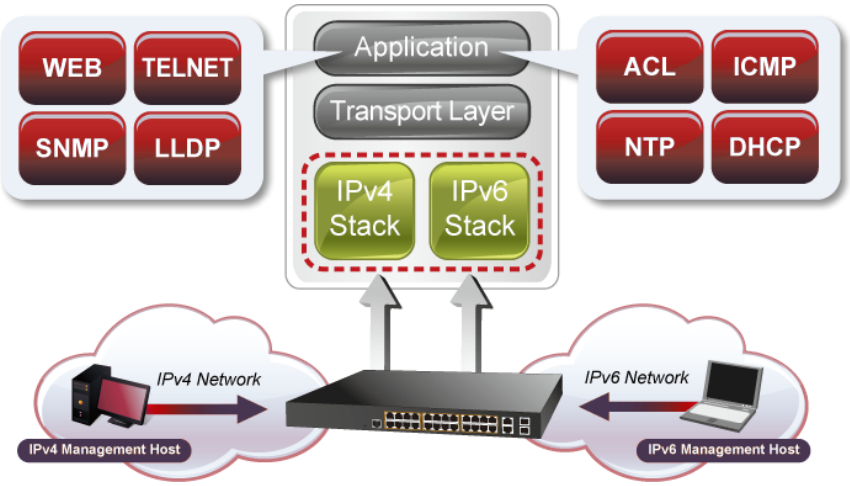
BEWARD's newly-revised Layer 2 Managed PoE+ Switch series is designed for enterprises and industries where a network of PDs can be centrally managed. The Switch's management functions have been enhanced to include intelligent PoE management, IPv6 management, ACL, GVRP, and more.

Cost-optimized Managed PoE+ Switch with L2/L4 Switching and Security

BEWARD Managed PoE+ Switch series is an ideal model which provides cost-effective advantage to local area network and is widely accepted in the SMB office network. It offers **intelligent Layer 2 data packet switching and management functions**, **user-friendly web user interface** and **stable operation**. The Managed PoE+ Switch series complies with **IEEE 802.3at Power over Ethernet Plus (PoE+)** at an affordable price; the Managed PoE+ Switch series is equipped with **8/16/24 10/100BASE-TX** Fast Ethernet ports and **2 Gigabit TP/SFP combo** interfaces with inner power system. With its **8/16/24** Fast Ethernet ports integrated with 802.3at PoE+ injector function and total power budget of up to **240 watts**, it offers a rack-mountable, affordable, safe and reliable power solution for SMBs deploying Power over Ethernet networks, or requiring enhanced data security and network traffic management.

Solution for IPv6 Networking

With the support for IPv6/IPv4 protocol, and easy and user-friendly management interfaces, the Managed PoE+ Switch is the ideal choice for IP surveillance, VoIP and wireless service providers to connect with the IPv6 network. It also helps SMBs to step in the IPv6 era with the lowest investment and without having to replace the network facilities even though ISPs establish the IPv6 FTTx edge network.



SEC.RU | Короткий путь к информации
Скачано с sec.ru

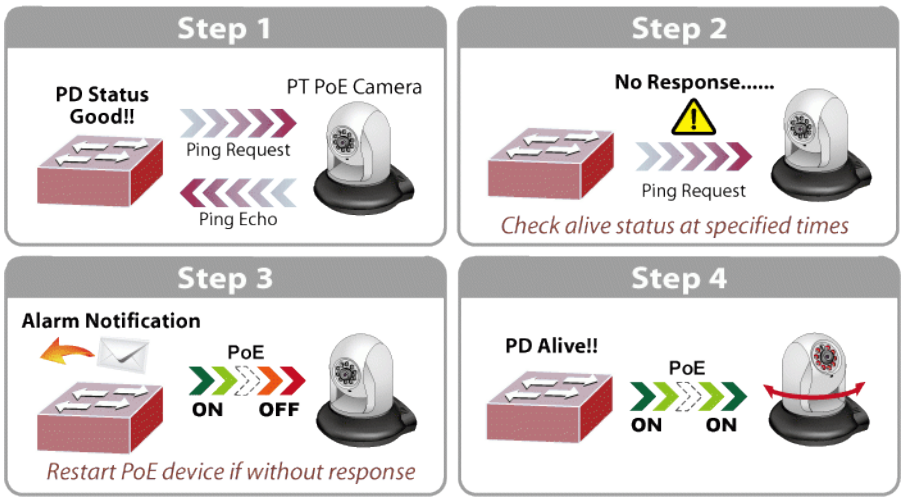
Built-in Unique PoE Functions for Surveillance Management

As the managed PoE+ Switch for surveillance network, it features the following intelligent PoE management functions:

- **PD Alive Check**
- **PoE Port Sequence**
- **PoE Schedule**

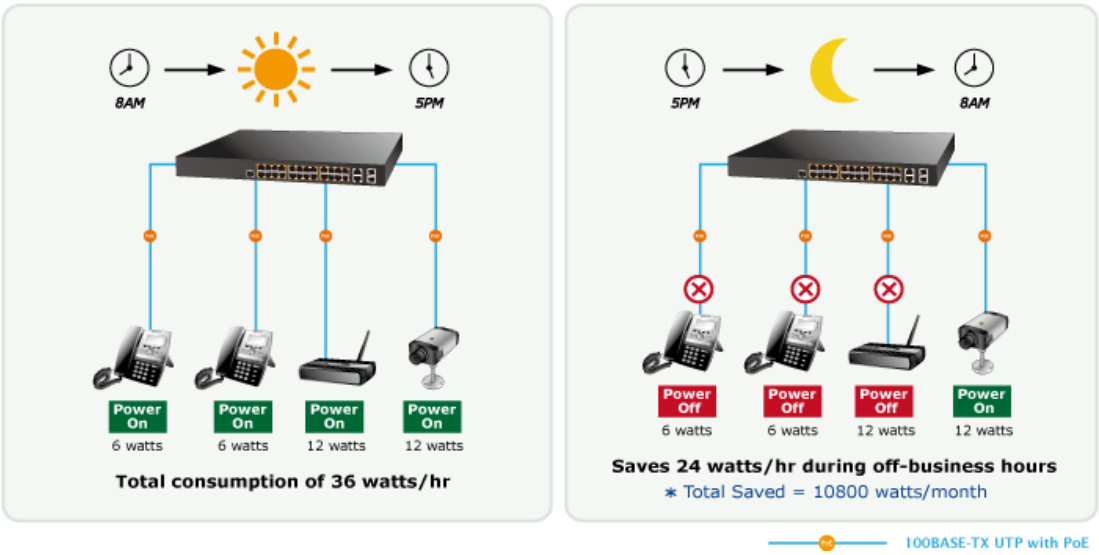
Intelligent Powered Device Alive Check

The Managed PoE+ Switch can be configured to monitor a connected PD status in real time via ping action. Once the PD stops working and it is without response, the Managed PoE+ Switch will resume the PoE port power and bring the PD back to work. It will greatly enhance the network reliability through the PoE port resetting the PD's power source, thus reducing administrator management burden.



PoE Schedule for Energy Saving

Besides being used for IP surveillance, the Managed PoE+ Switch is certainly applicable to build any PoE network including VoIP and wireless LAN. Under the trend of energy saving worldwide and contributing to the environmental protection on the Earth, the Managed PoE+ Switch can effectively control the power supply besides its capability of giving high watts power. The **"PoE schedule"** function helps you to enable or disable PoE power feeding for each PoE port during specified time intervals and it is a powerful function to help SMBs and enterprises save energy and budget.



SEC.RU | Короткий путь к информации
Скачано с sec.ru

PoE Port Sequence

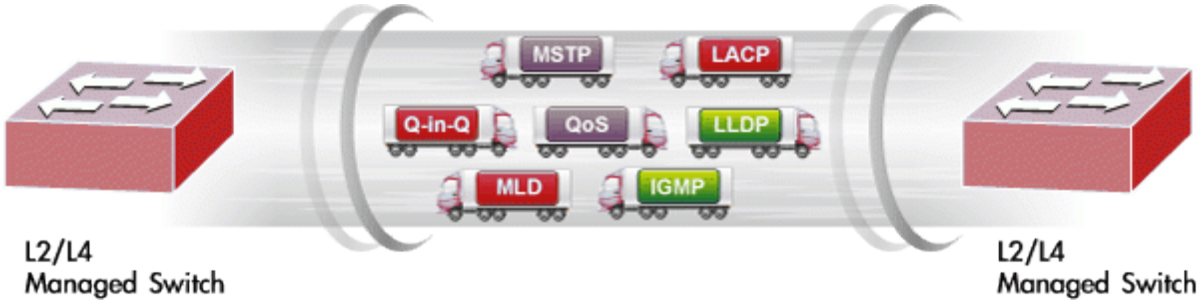
To prevent all the PoE ports of the Managed PoE+ Switch from being active at the same time when the Switch has booted up, the PoE ports of the Managed PoE+ Switch can be configured to allow each port to be activated at an interval time. In addition, the **"Delay"** setting is to delay power feeding on each port when the Managed PoE+ Switch has completely booted up.

Ethernet Data Transmission Distance Extension

In the "Extended" operation mode, the Managed PoE+ Switch operates on a per-port basis at 10Mbps duplex operation but can support PoE power output over a distance of up to 250 meters overcoming the 100 meters limit on Ethernet UTP cable.

Robust Layer 2 Features

The Managed PoE+ Switch can be programmed for advanced switch management functions, such as **Multiple Spanning Tree Protocol (MSTP)**, BPDU filtering, BPDU Guard, dynamic port link aggregation, **IGMP/MLD snooping**, DHCP relay agent, loop detection and **GVRP**, voice VLAN and the **Link Layer Discovery Protocol (LLDP)**. The Layer 2 protocol included is to help discover basic information about neighboring devices in the local broadcast domain. Other features included are the port-based/802.1Q VLAN and Q-in-Q VLAN, Layer 2/4 QoS, port mirroring, broadcast storm control and bandwidth control.



Enhanced Security and Traffic Control

The Managed PoE+ Switch offers the comprehensive **Layer 2 to Layer 4 access control list (ACL)** for enforcing security to the edge. It can be used to restrict network access by denying packets based on source and destination IP/MAC address or defined typical network applications. The Managed PoE+ Switch also provides **DHCP Snooping**, **ARP Inspection** and **MAC Verification** functions to prevent IP snooping from attack and discard ARP packets with invalid MAC address. Also included are per port MAC/IP address binding and MAC address binding. The network administrator can now build highly-secure corporate networks with considerably less time and effort than before.

Cybersecurity Network Solution to Minimize Security Risks

The cybersecurity features that virtually need no effort and cost to have included the protection of the switch management and the enhanced security of the mission-critical network. Both SSH and SSL protocols are utilized to provide strong protection against advanced threats. The network administrator can now construct highly-secure corporate networks with considerably less time and effort than before.

Efficient Management

For efficient management, the Managed PoE+ Switch is equipped with **Web**, **Telnet** and **SNMP** management interfaces. With the built-in Web-based management interface, the Managed PoE+ Switch offers an easy-to-use, platform-independent management and configuration facility. By supporting the standard Simple Network Management Protocol (SNMP), the

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Managed PoE+ Switch can be managed via any standard management software. For text-based management, the switch can be accessed via Telnet. Moreover, the Managed PoE+ Switch offers secure remote management by supporting **SNMPv3** connections which encrypt the packet content at each session.

Flexible and Extendable Uplink Solution

The Managed PoE+ Switch provides **2 extra Gigabit TP/SFP combo** interfaces supporting **10/100/1000BASE-T** RJ45 copper to connect with surveillance network devices such as **NVR**, **Video Streaming Server** or **NAS** to facilitate surveillance management. Or through these fiber SFP slots occupied by the **1000BASE-SX/LX** SFP (small form-factor pluggable) fiber transceivers, it can be uplinked to a backbone switch and monitoring center in long distance. The distance can be extended from 550 meters to 2km (multi-mode fiber) to 10/20/40/80/120 kilometers (single-mode fiber or WDM fiber). They are well-suited for applications within the industrial data centers and distributions.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

1.3 How to Use This Manual

This User's Manual is structured as follows:

Section 2, INSTALLATION

The section explains the functions of the Managed PoE+ Switch and how to physically install the Managed PoE+ Switch.

Section 3, SWITCH MANAGEMENT

The section contains the information about the software function of the Managed PoE+ Switch.

Section 4, WEB CONFIGURATION

The section explains how to manage the Managed PoE+ Switch by Web interface.

Section 5, COMMAND LINE INTERFACE

The section describes how to use the Command Line interface (CLI).

Section 6, CLI CONFIGURATION

The section explains how to manage the Managed PoE+ Switch by Command Line interface.

Section 7, SWITCH OPERATION

The chapter explains how to do the switch operation of the Managed PoE+ Switch.

Section 8, POWER over ETHERNET OVERVIEW

The chapter introduces the IEEE 802.3af / 802.3at PoE standard and PoE provision of the Managed PoE+ Switch.

Section 9, TROUBLESHOOTING

The chapter explains how to do troubleshooting of the Managed PoE+ Switch.

Appendix A

The section contains cable information of the Managed PoE+ Switch.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

1.4 Product Features

- **Physical Port**
  - **8/16/24 10/100BASE-TX** RJ45 copper ports with **IEEE 802.3at/af PoE+** injector function
  - **2 10/100/1000BASE-T** Gigabit RJ45 copper ports (Combo Interface)
  - **2 1000BASE-X mini-GBIC/SFP slots** (Combo Interface)
  - RJ45 console interface for switch basic management and setup
  - Reset button for system factory default

- **Switching**
  - Hardware-based 10/100Mbps, half/full duplex and 1000Mbps full duplex mode, flow control and auto-negotiation, and auto MDI/MDI-X
  - Features Store-and-Forward mode with wire-speed filtering and forwarding rates
  - IEEE 802.3x flow control for full duplex operation and back pressure for half duplex operation
  - Automatic address learning and address aging
  - Supports CSMA/CD protocol

- **Power over Ethernet**
  - Complies with IEEE 802.3at Power over Ethernet Plus
  - Complies with IEEE 802.3af Power over Ethernet
  - Up to 8/16/24 ports of IEEE 802.3af/802.3at devices powered
  - Supports PoE Power up to 30 watts for each PoE port
  - 120/240-watt PoE budget
  - Auto detects powered device (PD)
  - Circuit protection prevents power interference between ports
  - Remote power feeding up to 250m via extend mode
  - PoE Management
    - Per port PoE function enable/disable
    - Per Port PoE operation mode selection
    - Per PoE port power budget control
    - PD classification detection and PoE consumption usage status
  - Intelligent PoE features
    - PD alive check
    - PoE port sequence
    - PoE schedule

- **Layer 2 Features**
  - Prevents packet loss with back pressure (half-duplex) and IEEE 802.3x pause frame flow control (full-duplex)
  - High performance Store and Forward architecture, runt/CRC filtering eliminates erroneous packets to optimize the network bandwidth
  - Supports **VLAN**
    - Port-based VLAN, up to 10/18/26 VLAN groups
    - IEEE 802.1Q tagged VLAN

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- Protocol VLAN
- Provider Bridging (VLAN Q-in-Q) support (IEEE 802.1ad)
- GVRP
- Voice VLAN

■ Supports **Spanning Tree Protocol**

- STP (IEEE 802.1D Spanning Tree Protocol)
- RSTP (IEEE 802.1w Rapid Spanning Tree Protocol)
- MSTP (IEEE 802.1s Multiple Spanning Tree Protocol)
- STP BPDU filtering, BPDU Guard

■ Supports **Link Aggregation**

–IEEE 802.3ad Link Aggregation Control Protocol (LACP)

–1 LACP group, up to 2 ports per LACP group

–Cisco ether-channel (static trunk)

–1 trunk group, up to 2 ports per trunk group

■ Provides port mirror (many-to-1)

■ Loop detection

- **Quality of Service**

■ Ingress/Egress Rate Limit per port bandwidth control

■ Storm Control support

–Broadcast/ Multicast /DLF (Destination Lookup Fail)/ARP/ICMP

■ Traffic classification

- IEEE 802.1p Qos/CoS
- TCP/UDP/DSCP/IP precedence of IPv4/IPv6 packets

■ Strict priority and Weighted Round Robin (WRR) CoS policies

- **Multicast**

■ Supports IPv4 IGMP snooping v1/ v2 and v3

■ Supports IPv6 MLD snooping v1, v2

- **Security**

■ Access Control List

–IPv4/IPv6 IP-based ACL

–MAC-based ACL

■ Port-MAC-IP Address Binding

–Port-MAC-IP Port Setting

–Port-MAC-IP Entry Setting

■ MAC Address Binding

–Static MAC

–MAC Filtering

■ DHCP snooping to filter distrusted DHCP messages

■ ARP Inspection discards ARP packets with invalid MAC address to IP address binding

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- **Management**

  - IPv4 and IPv6 dual stack management
  - Switch management interface
    - RJ45 Console local management
    - Web switch management
    - Telnet command line interface
    - SNMP v1, v2c and v3
  - BOOTP and DHCP for IP address assignment
  - System maintenance
    - Firmware upgrade via HTTP
    - Configuration upload/download through web interface
    - Hardware-based reset button for system reset to factory default
  - SNTP Network Time Protocol
  - Link Layer Discovery Protocol (LLDP)
  - SNMP trap for interface link up and link down notification
  - Event message logging to remote syslog server
  - BEWARD Smart Discovery utility

SEC.RU | Короткий путь к информации
Скачано с sec.ru

1.5 Product Specifications

Product	STW-822HP
Hardware Specifications	
Copper Ports	8 10/100BASE-TX RJ45 Auto-MDI/MDI-X ports
PoE Injector Port	8 802.3af/802.3at PoE+ injector ports
Gigabit Copper Ports	2 10/100/1000BASE-T RJ45 auto-MDI/MDI-X ports
SFP/mini-GBIC Slots	2 1000BASE-X SFP interfaces, shared with Port-9 to Port-10
Reset Button	< 5 sec: System reboot > 5 sec: Factory default
Thermal Fan	1
Power Requirements	100~240V AC, 50/60Hz, 2.5A (max.)
Power Consumption/Dissipation	Max.121 watts/413BTU
Dimensions (W x D x H)	280 x 180 x 44 mm
Weight	1503g
Enclosure	Metal
LED	**System**: Power (**Green**) SYS (**Green**) **10/100TX RJ45 Interfaces** (Port 1 to Port 8): LNK/ACT (**Green**), PoE-in-Use (**Amber**) 10/100/1000BASE-T RJ45 / SFP Interfaces (Port 9 to Port 10): LNK/ACT 10/100 (**Orange**), 1000 (**Green**)
Switching	
Switch Architecture	Store-and-Forward
Switch Fabric	5.6Gbps/non-blocking
Switch Throughput@64bytes	4.17Mpps @64bytes
MAC Address Table	16K entries
Shared Data Buffer	4Mb
Flow Control	IEEE 802.3x pause frame for full duplex Back pressure for half duplex
Maximum Transmit Unit	16K bytes
Power over Ethernet	
PoE Standard	IEEE 802.3af Power over Ethernet/PSE IEEE 802.3at Power over Ethernet Plus/PSE
PoE Power Supply Type	End-span
Power Pin Assignment	1/2(+), 3/6 (-)
PoE Power Output	Per Port 53V DC, 300mA. Max. 15.4 watts (IEEE 802.3af) Per Port 53V DC, 600mA. Max. 30 watts (IEEE 802.3at)
PoE Power Budget	120 watts
Number of PDs, 7 watts	8
Number of PDs, 15.4 watts	7
Number of PDs, 30 watts	4
Layer 2 Functions	
Port Mirroring	TX/RX/both Many-to-1 monitor
VLAN	Port-based VLAN, up to 10 VLAN groups IEEE 802.1Q tagged VLAN - Up to 256 VLAN groups, out of 4094 VLAN IDs

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	Protocol VLAN Provider Bridging (VLAN Q-in-Q) support (IEEE 802.1ad) GVRP Voice VLAN
Link Aggregation	IEEE 802.3ad LACP supports one 2-port trunk group; static trunk supports one 2-port trunk group
Spanning Tree Protocol	IEEE 802.1D Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) STP BPDU filtering, BPDU Guard
IGMP Snooping	IPv4 IGMP snooping v1/ v2 and v3
MLD Snooping	IPv6 MLD snooping v1, v2
Access Control List	IPv4/IPv6 IP-based ACL MAC-based ACL
QoS	Ingress/Egress Rate Limit per port bandwidth control Storm Control support – Broadcast/ Multicast /DLF (Destination Lookup Failure)/ARP/ICMP Traffic classification - IEEE 802.1p Qos/CoS - TCP/UDP/DSCP/IP precedence of IPv4/IPv6 packets Strict priority and Weighted Round Robin (WRR) CoS policies
Security	Access Control List – IPv4/IPv6 IP-based ACL – MAC-based ACL Port-MAC-IP Address Binding – Port-MAC-IP Port Setting – Port-MAC-IP Entry Setting MAC Address Binding – Static MAC – MAC Filtering DHCP snooping to filter distrusted DHCP messages ARP Inspection discards ARP packets with invalid MAC address to IP address binding
Management Functions	
Basic Management Interfaces	IPv4 and IPv6 dual stack management Switch management interface - Web switch management - Telnet command line interface - SNMP v1, v2c and v3 BOOTP and DHCP for IP address assignment System maintenance - Firmware upgrade via HTTP - Configuration upload/download through web interface - Hardware-based reset button for system reset to factory default SNTP Network Time Protocol Link Layer Discovery Protocol (LLDP) Event message logging to remote Syslog server BEWARD smart discovery utility
Secure Management Interfaces	SNMP v3, SSHv2, TLS v1.2
Standards Conformance	
Regulatory Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x flow control and back pressure IEEE 802.3ad port trunk with LACP

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	IEEE 802.1D Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1s Multiple Spanning Tree Protocol IEEE 802.1p Class of Service IEEE 802.1Q VLAN tagging IEEE 802.1ab LLDP IEEE 802.3af Power over Ethernet IEEE 802.3at Power over Ethernet Plus RFC 2068 HTTP RFC 1112 IGMP version 1 RFC 2236 IGMP version 2 RFC 3376 IGMP version 3 RFC 2710 MLD version 1 RFC 3810 MLD version 2
Environment	
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 10 ~ 90% (non-condensing)
Storage	Temperature: -10 ~ 70 degrees C Relative Humidity: 5 ~ 90% (non-condensing)

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Product	STW-1622HP	STW-2422HP
Hardware Specifications		
Copper Ports	16 10/100BASE-TX RJ45 Auto-MDI/MDI-X ports	24 10/100BASE-TX RJ45 Auto-MDI/MDI-X ports
PoE Injector Port	16 802.3af/802.3at PoE+ injector ports	24 802.3af/802.3at PoE+ injector ports
Gigabit Copper Ports	2 10/100/1000BASE-T RJ45 auto-MDI/MDI-X ports	
SFP/mini-GBIC Slots	2 1000BASE-X SFP interfaces, shared with Gigabit copper ports	
Console	1 x RS-232-to-RJ45 serial port (115200, 8, N, 1)	
Reset Button	> 5 sec: Factory default < 5 sec: System reboot	
Thermal Fan	2	
Power Requirements	100~240V AC, 50/60Hz, 3.6A (max.)	100~240V AC, 50/60Hz, 3.6A (max.)
Power Consumption/Dissipation	Max.270watts/921BTU	Max.281watts/959BTU
Dimensions (W x D x H)	440 x 208 x 44 mm, 1U height	
Weight	2332g	2787g
Enclosure	Metal	Metal
LED	**System**: Power (**Green**) SYS (**Green**) **10/100TX RJ45 Interfaces**: LNK/ACT (**Green**), PoE-in-Use (**Amber**) 10/100/1000BASE-T RJ45 / SFP Interfaces: LNK/ACT10/100 (**Amber**), 1000 (**Green**)	
Switching		
Switch Architecture	Store-and-Forward	
Switch Fabric	7.2Gbps/non-blocking	8.8Gbps/non-blocking
Switch Throughput@64bytes	5.35Mpps @64bytes	6.55Mpps @64bytes
MAC Address Table	16K entries	
Shared Data Buffer	4Mb	
Flow Control	IEEE 802.3x pause frame for full duplex Back pressure for half duplex	
Jumbo Frame	10K bytes	
Power over Ethernet		
PoE Standard	IEEE 802.3af Power over Ethernet/PSE IEEE 802.3at Power over Ethernet Plus/PSE	
PoE Power Output	Per Port 54V DC, 300mA. Max. 15.4 watts (IEEE 802.3af) Per Port 54V DC, 600mA. Max. 30 watts (IEEE 802.3at)	Per Port 53 DC, 300mA. Max. 15.4 watts (IEEE 802.3af) Per Port 53 DC, 600mA. Max. 30 watts (IEEE 802.3at)
PoE Power Supply Type	End-span	Mid-span
Power Pin Assignment	1/2(+), 3/6 (-)	4/5(+), 7/8 (-)
PoE Power Budget	240 watts	240 watts
Number of PDs, 7 watts	16	24
Number of PDs, 15.4 watts	15	15
Number of PDs, 30 watts	8	8

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Layer 2 Functions		
Port Mirroring	TX/RX/both Many-to-1 monitor	
VLAN	Port-based VLAN, up to 18 VLAN groups IEEE 802.1Q tagged VLAN - Up to 256 VLAN groups, out of 4094 VLAN IDs Protocol VLAN Provider Bridging (VLAN Q-in-Q) support (IEEE 802.1ad) GVRP Voice VLAN	Port-based VLAN, up to 26 VLAN groups IEEE 802.1Q tagged VLAN - Up to 256 VLAN groups, out of 4094 VLAN IDs Protocol VLAN Provider Bridging (VLAN Q-in-Q) support (IEEE 802.1ad) GVRP Voice VLAN
Link Aggregation	IEEE 802.3ad LACP supports one 2-port trunk group; static trunk supports one 2-port trunk group	
Spanning Tree Protocol	IEEE 802.1D Spanning Tree Protocol (STP) IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) IEEE 802.1s Multiple Spanning Tree Protocol (MSTP) STP BPDU filtering, BPDU Guard	
IGMP Snooping	IPv4 IGMP snooping v1/ v2 and v3	
MLD Snooping	IPv6 MLD snooping v1, v2	
Access Control List	IPv4/IPv6 IP-based ACL MAC-based ACL	
QoS	Ingress/Egress Rate Limit per port bandwidth control Storm Control support – Broadcast/ Multicast /DLF (Destination Lookup Failure)/ARP/ICMP Traffic classification - IEEE 802.1p Qos/CoS - TCP/UDP/DSCP/IP precedence of IPv4/IPv6 packets Strict priority and Weighted Round Robin (WRR) CoS policies	
Security	Access Control List – IPv4/IPv6 IP-based ACL – MAC-based ACL Port-MAC-IP Address Binding – Port-MAC-IP Port Setting – Port-MAC-IP Entry Setting MAC Address Binding – Static MAC – MAC Filtering DHCP snooping to filter distrusted DHCP messages ARP Inspection discards ARP packets with invalid MAC address to IP address binding	
Management Functions		
Basic Management Interfaces	IPv4 and IPv6 dual stack management Switch management interface - RJ45 console local management - Web switch management - Telnet command line interface - SNMP v1, v2c and v3 BOOTP and DHCP for IP address assignment System maintenance - Firmware upgrade via HTTP - Configuration upload/download through web interface - Hardware-based reset button for system reset to factory default SNTP Network Time Protocol Link Layer Discovery Protocol (LLDP) Event message logging to remote Syslog server	

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	BEWARD Smart Discovery
Secure Management Interfaces	SNMP v3, SSHv2, TLS v1.2
Standards Conformance	
Regulatory Compliance	FCC Part 15 Class A, CE
Standards Compliance	IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3z Gigabit SX/LX IEEE 802.3ab Gigabit 1000T IEEE 802.3x flow control and back pressure IEEE 802.3ad port trunk with LACP IEEE 802.1D Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1s Multiple Spanning Tree Protocol IEEE 802.1p Class of Service IEEE 802.1Q VLAN tagging IEEE 802.1ab LLDP IEEE 802.3af Power over Ethernet IEEE 802.3at Power over Ethernet Plus RFC 2068 HTTP RFC 1112 IGMP version 1 RFC 2236 IGMP version 2 RFC 3376 IGMP version 3 RFC 2710 MLD version 1 RFC 3810 MLD version 2
Environment	
Operating	Temperature: 0 ~ 50 degrees C Relative Humidity: 10 ~ 90% (non-condensing)
Storage	Temperature: -10 ~ 70 degrees C Relative Humidity: 5 ~ 90% (non-condensing)

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2. INSTALLATION

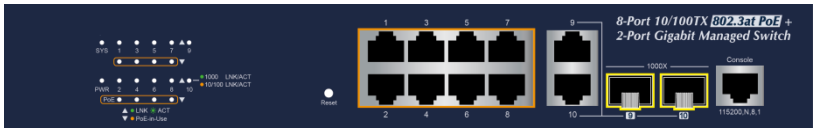
This section describes the hardware features and installation of the Managed PoE+ Switch on the desktop or rack mount. For easier management and control of the Managed PoE+ Switch, familiarize yourself with its display indicators, and ports. Front panel illustrations in this chapter display the unit LED indicators. Before connecting any network device to the Managed PoE+ Switch, please read this chapter completely.

2.1 Hardware Description

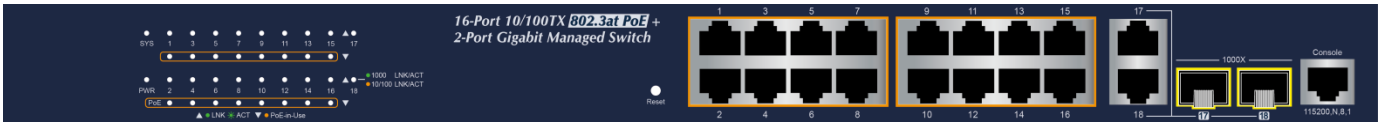
2.1.1 Switch Front Panel

The front panel provides a simple interface monitoring the Managed PoE+ Switch. Figure 2-1 shows the front panels of the Managed PoE+ Switches.

STW-822HP Front Panel



STW-1622HP Front Panel



STW-2422HP Front Panel

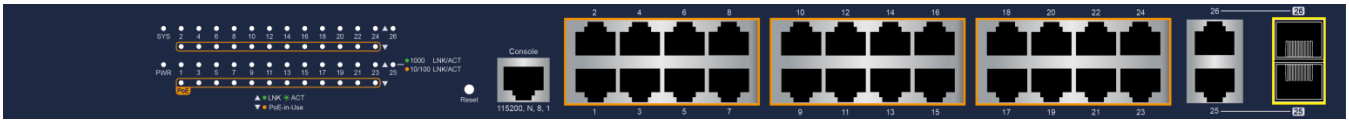


Figure 2-1: Front Panels of Managed PoE+ Switch Series Model

- **Fast Ethernet TP interface**

  10/100BASE-TX Copper, RJ45 Twisted-pair: Up to 100 meters.

- **Gigabit TP interface**

  10/100/1000BASE-T Copper, RJ45 Twisted-pair: Up to 100 meters.

- **SFP slots**

  1000BASE-X mini-GBIC slot, SFP (Small Factor Pluggable) transceiver module: From 550 meters to 2km (Multi-mode fiber), up to above 10/20/30/40/50/60/70/120 kilometers (Single-mode fiber).

- **Reset button**

  At the left of the front panel, the reset button is designed for rebooting the Managed PoE+ Switch without turning off and on the power. The following is the summary table of Reset button functions:

Reset Button Pressed and Released	Function
< 5 sec: System Reboot	Reboot the Managed PoE+ Switch.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

> 5 sec: Factory Default	Reset the Managed PoE+ Switch to Factory Default configuration. The Managed PoE+ Switch will then reboot and load the default settings as below: ◦ Default Username: **admin** ◦ Default Password: **admin** ◦ Default IP address: **192.168.0.100** ◦ Subnet mask: **255.255.255.0** ◦ Default Gateway: **192.168.0.254**

■ RJ45 Console Port

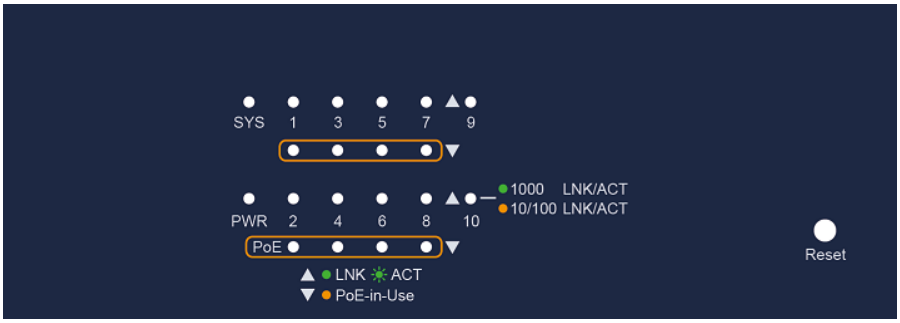
The console port is a DB9, RS-232 male serial port to RJ45 connector. It is an interface for connecting a terminal directly. Through the console port, it provides rich diagnostic information including IP Address setting, factory reset, port management, link status and system setting. Users can use the attached RS-232 to RJ45 console cable in the package and connect to the console port on the device. After the connection, users can run any terminal emulation program (Hyper Terminal, ProComm Plus, Telix, Winterm and so on) to enter the startup screen of the device.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.1.2 LED Indications

The front panel LEDs indicates instant status of power and system status, fan status, port links / PoE in-use and data activity; helps monitor and troubleshoot when needed. Figure 2-2 shows the LED indications of the Managed PoE+ Switches.

STW-822HP LED Indication



- **System**

LED	Color	Function
PWR	**Green**	**Lights** to indicate the Switch has power.
SYS	**Green**	**Lights** to indicate the system is working. **Off** to indicate the system is booting.

- **Per 10/100Mbps Port with PoE Interfaces (Port1 to Port8)**

LED	Color	Function	
LNK/ACT	**Green**	**Lights**	Indicates the link through that port is successfully established at 10/100Mbps.
		Blink	Indicates the Switch is actively sending or receiving data over that port.
PoE In-Use	**Amber**	**Lights**	Indicates the port is providing PoE power.
		Off	Indicates the port is not providing PoE power.

- **Per 10/100/1000Mbps RJ45 Combo Interface (Port9 to Port10)**

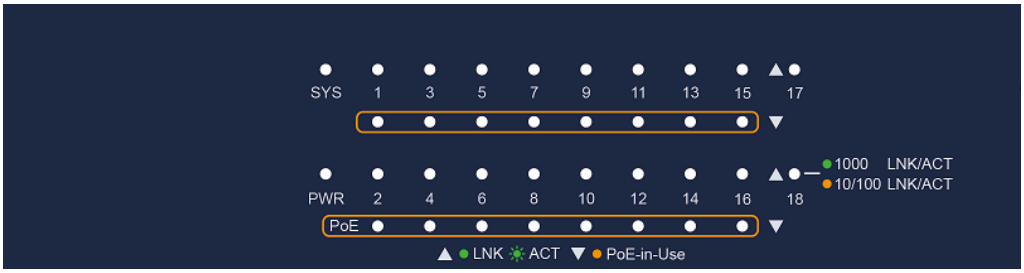
LED	Color	Function	
1000 LNK/ACT	**Green**	**Lights**	Indicates the port is successfully established.
		Blink	Indicates the Switch is actively sending or receiving data over that port.
10/100 LNK/ACT	**Amber**	**Lights**	Indicates the port is successfully established.
		Blink	Indicates the Switch is actively sending or receiving data over that port.

- **Per 1000Mbps SFP Combo Interface (Port9 to Port10)**

LED	Color	Function	
1000 LNK/ACT	**Green**	**Lights**	Indicates the port is successfully established.
		Blink	Indicates the Switch is actively sending or receiving data over that port.
10/100 LNK/ACT	**Amber**	**Lights**	Indicates the port is successfully established.
		Blink	Indicates the Switch is actively sending or receiving data over that port.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

STW-1622HP LED Indication



■ **System**

LED	Color	Function
PWR	**Green**	**Lights** to indicate the Switch has power.
SYS	**Green**	**Lights** to indicate the system is working. **Off** to indicate the system is booting.

■ **Per 10/100Mbps Port with PoE Interfaces (Port1 to Port16)**

LED	Color	Function	
LNK/ACT	**Green**	**Lights**	Indicates the link through that port is successfully established at 10/100Mbps.
		Blink	Indicates the Switch is actively sending or receiving data over that port.
PoE-in-Use	**Amber**	**Lights**	Indicates the port is providing PoE power.
		Off	Indicates the port is not providing PoE power.

■ **Per 10/100/1000Mbps RJ45 Combo Interface (Port17 to Port18)**

LED	Color	Function	
1000 LNK/ACT	**Green**	**Lights**	Indicates the port is successfully established.
		Blink	Indicates the Switch is actively sending or receiving data over that port.
10/100 LNK/ACT	**Amber**	**Lights**	Indicates the port is successfully established.
		Blink	Indicates the Switch is actively sending or receiving data over that port.

■ **Per 1000Mbps SFP Combo Interface (Port17 to Port18)**

LED	Color	Function	
1000 LNK/ACT	**Green**	**Lights**	Indicates the port is successfully established.
		Blink	Indicates the Switch is actively sending or receiving data over that port.
10/100 LNK/ACT	**Amber**	**Lights**	Indicates the port is successfully established.
		Blink	Indicates the Switch is actively sending or receiving data over that port.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

STW-2422HP LED Indication

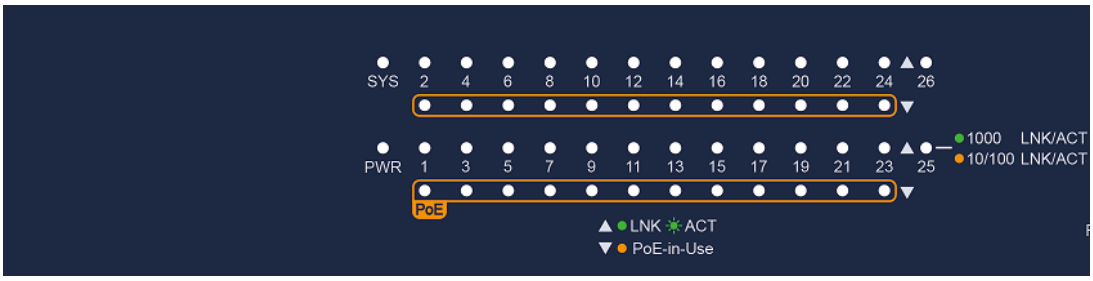


Figure 2-2: Managed PoE+ Switch Series LEDs on Front Panel

■ **System**

LED	Color	Function
PWR	**Green**	**Lights** to indicate the Switch has power.
SYS	**Green**	**Lights** to indicate the system is working. **Off** to indicate the system is booting.

■ **Per 10/100Mbps port with PoE interfaces (Port-1 to Port-24)**

LED	Color	Function	
LNK/ACT	**Green**	**Lights**	Indicates the link through that port is successfully established at 10/100Mbps.
		Blink	Indicates the Switch is actively sending or receiving data over that port.
PoE-in-Use	**Amber**	**Lights**	Indicates the port is providing PoE power.
		Off	Indicates the port is not providing PoE power.

■ **Per 10/100/1000Mbps RJ45 Combo Interface (Port-25 to Port-26)**

LED	Color	Function	
1000 LNK/ACT	**Green**	**Lights**	Indicates the port is successfully established.
		Blink	Indicates the Switch is actively sending or receiving data over that port.
10/100 LNK/ACT	**Amber**	**Lights**	Indicates the port is successfully established.
		Blink	Indicates the Switch is actively sending or receiving data over that port.

■ **Per 1000Mbps SFP Combo Interface (Port-25 to Port-26)**

LED	Color	Function	
1000 LNK/ACT	**Green**	**Lights**	Indicates the port is successfully established.
		Blink	Indicates the Switch is actively sending or receiving data over that port.
10/100 LNK/ACT	**Amber**	**Lights**	Indicates the port is successfully established.
		Blink	Indicates the Switch is actively sending or receiving data over that port.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.1.3 Switch Rear Panel

The rear panel of the Managed PoE+ Switch indicates an AC inlet power socket, which accepts input power from 100 to 240V AC, 50-60Hz. Figure 2-3 shows the rear panel of the Managed PoE+ Switch.

STW-2422HP Rear Panel

STW-1622HP Rear Panel

STW-2422HP Rear Panel

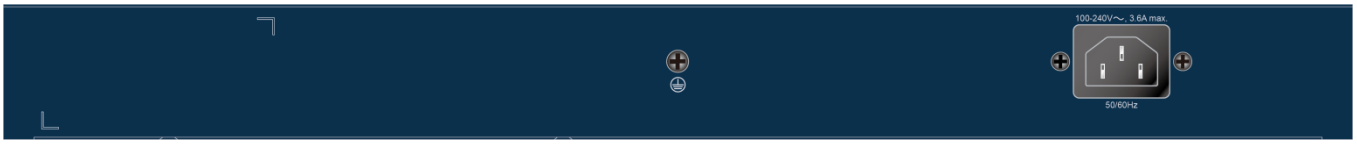


Figure 2-3: Rear Panels of Managed PoE+ Switch Series

■ **AC Power Receptacle**

For compatibility with electric service in most areas of the world, the Managed PoE+ Switch's power supply automatically adjusts to line power in the range of 100-240V AC and 50/60 Hz.

Plug the female end of the power cord firmly into the receptalbe on the rear panel of the Managed PoE+ Switch. Plug the other end of the power cord into an electric service outlet and the power will be ready.

Power Notice: The device is a power-required device, which means it will not work till it is powered. If your networks should be active all the time, please consider using UPS (Uninterrupted Power Supply) for your device. It will prevent you from network data loss or network downtime. In some areas, installing a surge suppression device may also help to protect your Managed PoE+ Switch from being damaged by unregulated surge or current to the Switch.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2.2 Install the Switch

This section describes how to install your Managed PoE+ Switch and make connections to the Managed PoE+ Switch. Please read the following topics and perform the procedures in the order being presented. To install your Managed PoE+ Switch on a desktop or shelf, simply complete the following steps.

Note

As the Managed PoE+ Switch have the same installation procedures, the **STW-1622HP** is picked to be an **example** for describing hardware installation.

2.2.1 Desktop Installation

To install the Managed PoE+ Switch on desktop or shelf, please follow these steps:

Step1: Attach the rubber feet to the recessed areas on the bottom of the Managed PoE+ Switch.

Step2: Place the Managed PoE+ Switch on the desktop or the shelf near an AC power source, as shown in Figure 2-4.

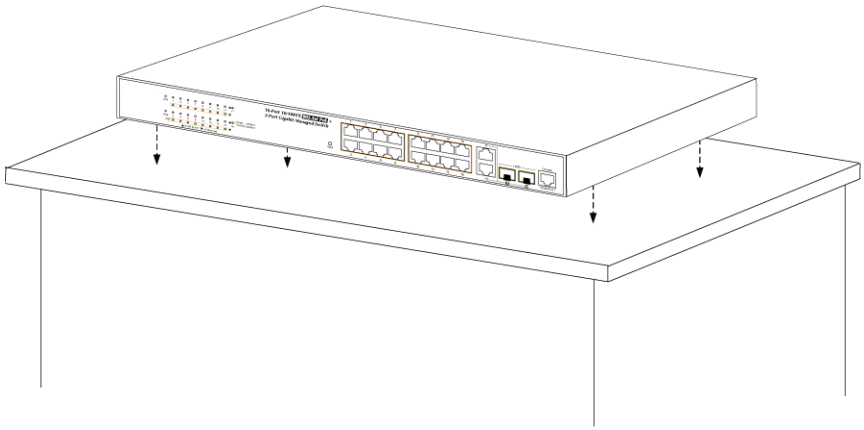


Figure 2-4: Place the Managed PoE+ Switch on the Desktop

Step3: Keep enough ventilation space between the Managed PoE+ Switch and the surrounding objects.

Note

When choosing a location, please keep in mind the environmental restrictions discussed in Chapter 1, Section 4, and specifications.

Step4: Connect the Managed PoE+ Switch to network devices.

Connect one end of a standard network cable to the 10/100/1000 RJ45 ports on the front of the Managed PoE+ Switch. Connect the other end of the cable to the network devices such as printer server, workstation or router.

Note

Connection to the Managed PoE+ Switch requires UTP Category 5 network cabling with RJ45 tips. For more information, please see the Cabling Specification in Appendix A.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Step5: Supply power to the Managed PoE+ Switch.

Connect one end of the power cable to the Managed PoE+ Switch.

Connect the power plug of the power cable to a standard wall outlet.

When the Managed PoE+ Switch receives power, the Power LED should remain solid Green.

2.2.2 Rack Mounting

To install the Managed PoE+ Switch in a 19-inch standard rack, please follow the instructions described below.

Step1: Place the Managed PoE+ Switch on a hard flat surface, with the front panel positioned towards the front side.

Step2: Attach the rack-mount bracket to each side of the Managed PoE+ Switch with supplied screws attached to the package.

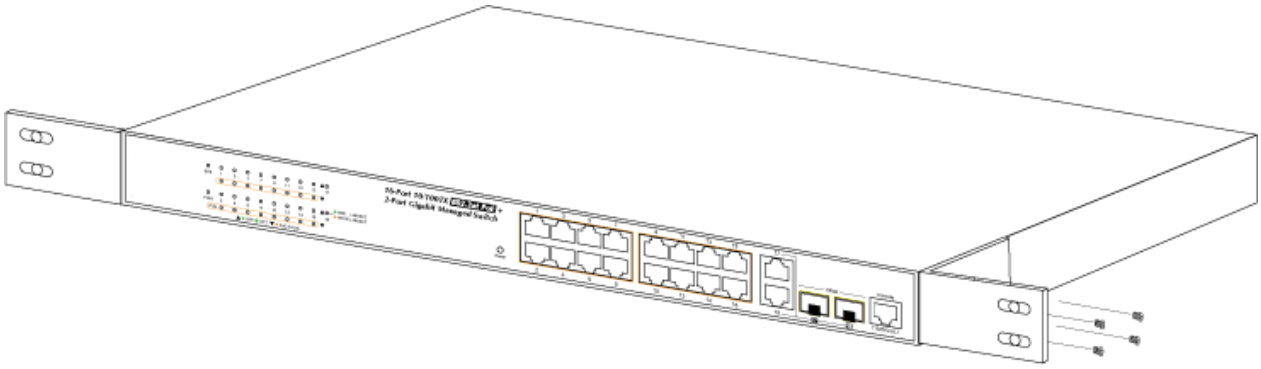


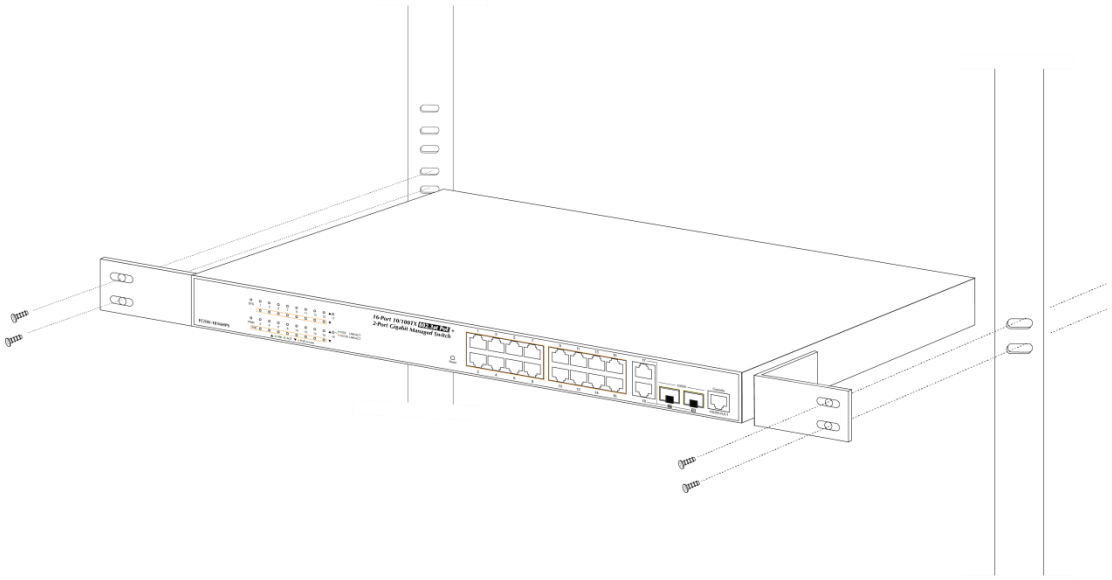
Figure 2-5: Attach Brackets to the Managed PoE+ Switch.

You must use the screws supplied with the mounting brackets. Damage caused to the parts by using incorrect screws would invalidate the warranty.

Step3: Secure the brackets tightly.

Step4: Follow the same steps to attach the second bracket to the opposite side.

Step5: After the brackets are attached to the Managed PoE+ Switch, use suitable screws to securely attach the brackets to the rack, as shown in Figure 2-6.



SEC.RU | Короткий путь к информации
Скачано с sec.ru

Figure 2-6: Mounting Managed PoE+ Switch in a Rack

Step6: Proceeds with the steps 4 and 5 of session 2.2.1 Desktop Installation to connect the network cabling and supply power to the Managed PoE+ Switch.

2.2.3 Installing the SFP Transceiver

The sections describe how to insert an SFP transceiver into an SFP slot.

The SFP transceivers are hot-pluggable and hot-swappable. You can plug-in and out the transceiver to/from any SFP port without having to power down the Managed PoE+ Switch, as the Figure 2-7 shows..

Figure 2-7: Plug-in the SFP Transceiver

SEC.RU | Короткий путь к информации
Скачано с sec.ru

1. Before we connect Managed PoE+ Switch to the other network device, we have to make sure both sides of the SFP transceivers are with the same media type, for example: 1000BASE-SX to 1000BASE-SX, 1000BASE-LX to 1000BASE-LX.
2. Check whether the fiber-optic cable type matches with the SFP transceiver requirement.
   - To connect to 1000BASE-SX SFP transceiver, please use the multi-mode fiber cable with one side being the male duplex LC connector type.
   - To connect to 1000BASE-LX SFP transceiver, please use the single-mode fiber cable with one side being the male duplex LC connector type.

■ Connect the Fiber Cable

1. Insert the duplex LC connector into the SFP transceiver.
2. Connect the other end of the cable to a device with SFP transceiver installed.
3. Check the LNK/ACT LED of the SFP slot on the front of the Managed PoE+ Switch. Ensure that the SFP transceiver is operating correctly.
4. Check the Link mode of the SFP port if the link fails. To function with some fiber-NICs or Media Converters, user has to set the port Link mode to **"1000 Force"**.

■ Remove the Transceiver Module

1. Make sure there is no network activity any more.
2. Remove the Fiber-Optic Cable gently.
3. Lift up the lever of the MGB module and turn it to a horizontal position.
4. Pull out the module gently through the lever.

Figure 2-8: How to Pull Out the SFP Transceiver

Never pull out the module without lifting up the lever of the module and turning it to a horizontal position. Directly pulling out the module could damage the module and the SFP module slot of the Managed PoE+ Switch.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3. SWITCH MANAGEMENT

This chapter explains the methods that you can use to configure management access to the Managed PoE+ Switch. It describes the types of management applications and the communication and management protocols that deliver data between your management device (workstation or personal computer) and the system. It also contains information about port connection options.

This chapter covers the following topics:

- Requirements
- Management Access Overview
- Administration Console Access
- Web Management Access
- SNMP Access
- Standards, Protocols, and Related Reading

3.1 Requirements

- Workstations running Windows 10/XP/2003/Vista/7/8/2008, MAC OS X or later, Linux, UNIX, or other platforms are compatible with TCP/IP protocols.
- Workstations are installed with Ethernet NIC (Network Interface Card)
- **Serial Port Connection** (Terminal)
  - The above Workstations come with COM Port (DB9) or USB-to-RS232 converter.
  - The above Workstations have been installed with **terminal emulator**, such as Hyper Terminal included in Windows XP/2003.
  - Serial cable -- one end is attached to the RS232 serial port, while the other end to the console port of the Managed PoE+ Switch.
- **Ethernet Port Connection**
  - Network cables -- Use standard network (UTP) cables with RJ45 connectors.
  - The above PC is installed with Web browser.

Note

It is recommended to use Internet Explorer 8.0 or above to access the Managed PoE+ Switch. If the Web interface of the Managed PoE+ Switch is not accessible, please turn off the anti-virus software or firewall and then try it again.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.2 Management Access Overview

The Managed PoE+ Switch gives you the flexibility to access and manage it using any or all of the following methods:

- An administration **console**
- **Web browser** interface
- An external **SNMP-based network management application**

The administration console and Web browser interface support are embedded in the Managed PoE+ Switch software and are available for immediate use. Each of these management methods has their own advantages. Table 3-1 compares the three management methods.

Method	Advantages	Disadvantages
Console	• No IP address or subnet needed • Text-based • Telnet functionality and HyperTerminal built into Windows 10 /XP/ 2003 /Vista/ 7/8/2008 operating systems • Secure	• Must be near switch or use dial-up connection • Not convenient for remote users • Modem connection may prove to be unreliable or slow
Web Browser	• Ideal for configuring the switch remotely • Compatible with all popular browsers • Can be accessed from any location • Most visually appealing	• Security can be compromised (hackers need only know the IP address and subnet mask) • May encounter lag times on poor connections
SNMP Agent	• Communicates with switch functions at the MIB level • Based on open standards	• Requires SNMP manager software • Least visually appealing of all three methods • Some settings require calculations • Security can be compromised (hackers need only know the community name)

Table 3-1: Comparison of Management Methods

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.3 Administration Console

The administration console is an internal, character-oriented, and command line user interface for performing system administration such as displaying statistics or changing option settings. Using this method, you can view the administration console from a terminal, personal computer, Apple Macintosh, or workstation connected to the Managed PoE+ Switch 's RJ45 console (serial) port.

There are two ways to use this management method: via direct access or modem port access. The following sections describe these methods. For more information about using the console, refer to **Chapter 5 Command Line Interface Console Management**.

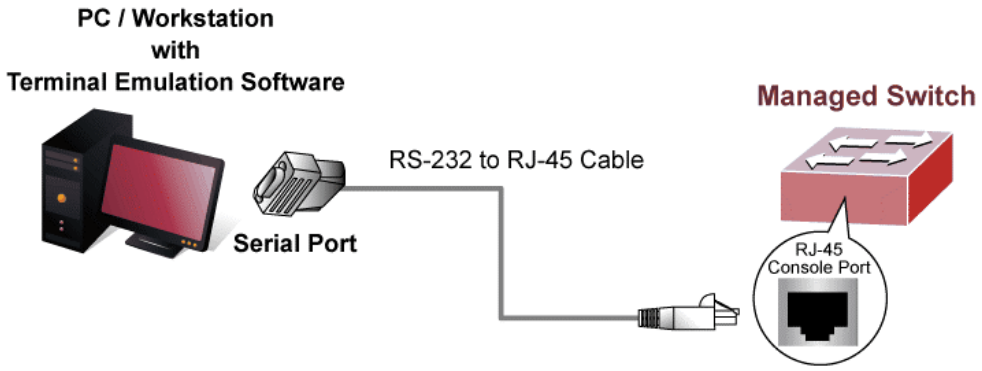


Figure 3-1: Console Management

Direct Access

Direct access to the administration console is achieved by directly connecting a terminal or a PC equipped with a terminal-emulation program (such as **HyperTerminal**) to the Managed PoE+ Switch RJ45 console (serial) port.

A terminal program is required to make the software connection to the Managed PoE+ Switch.

1. Run terminal program on the OS.
2. When the following screen appears, make sure that the COM port should be configured as:

   - **Baud: 115200**
   - **Data bits: 8**
   - **Parity: None**
   - **Stop bits: 1**
   - **Flow control: None**

SEC.RU | Короткий путь к информации
Скачано с sec.ru

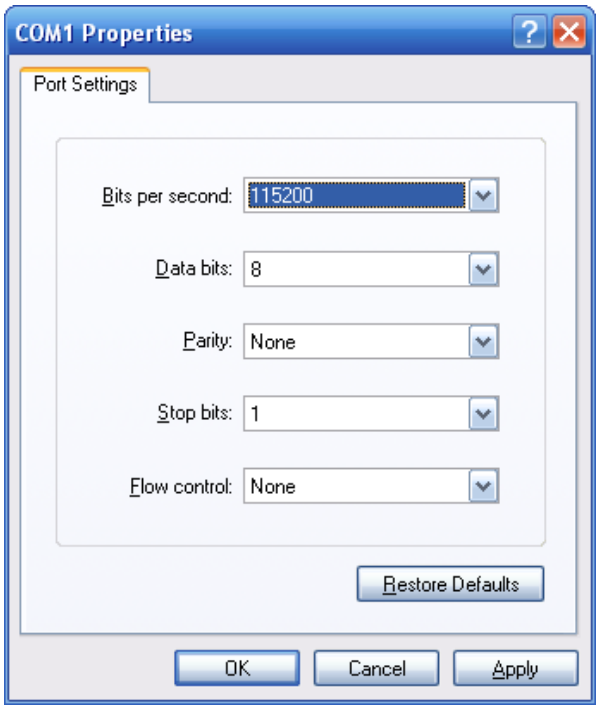


Figure 3-2: COM Port Configuration

This management method is often preferred because you can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A Macintosh or PC attachment can use any terminal-emulation program for connecting to the terminal serial port. A workstation attachment under UNIX can use an emulator such as TIP.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.4 Web Management

The Managed PoE+ Switch offers management features that allow users to manage the Managed PoE+ Switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer or Google Chrome. After set up your IP address for the Managed PoE+ Switch, you can access the Managed PoE+ Switch 's Web interface applications directly in your Web browser by entering the IP address of the Managed PoE+ Switch.

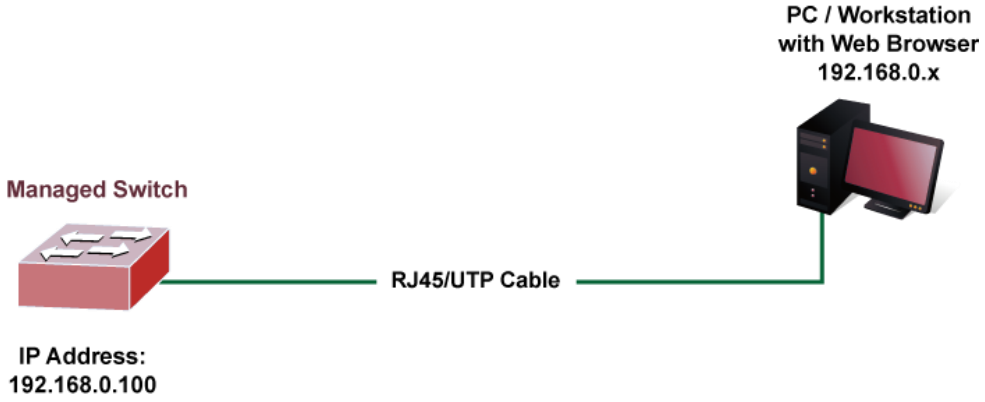


Figure 3-3: Web Management

You can then use your Web browser to list and manage the Managed PoE+ Switch configuration parameters from one central location, just as if you were directly connected to the Managed PoE+ Switch's RJ45 console port. Web Management requires either **Microsoft Internet Explorer 8.0** or later.

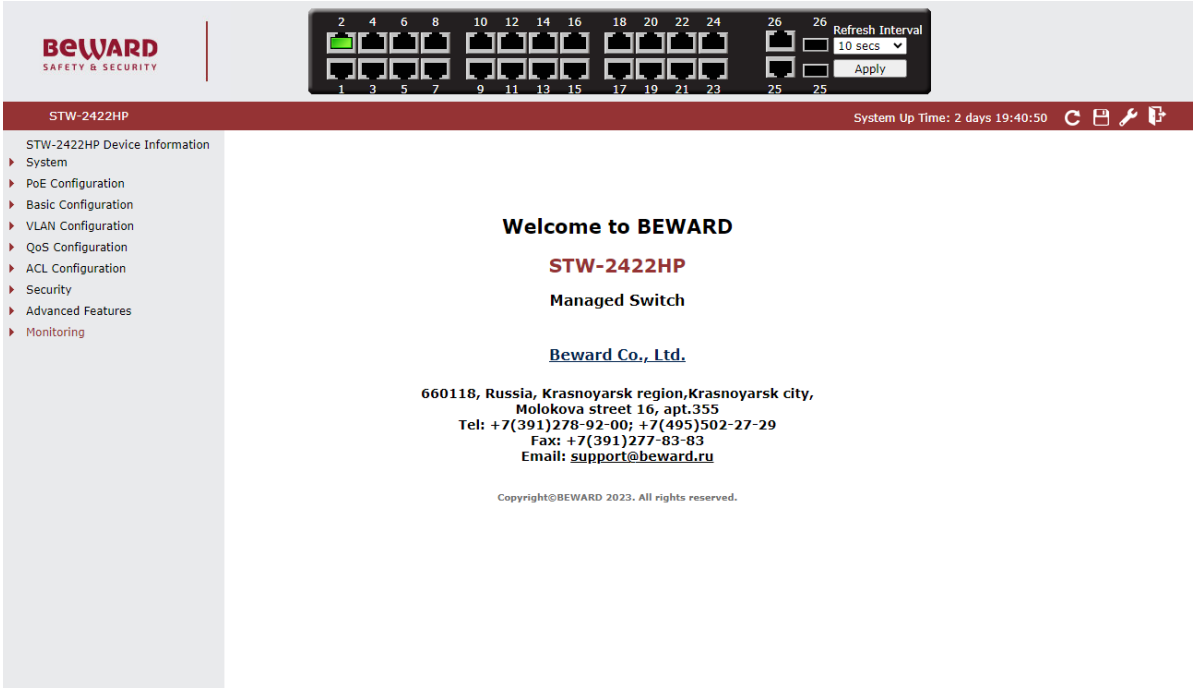


Figure 3-4: Web Main Screen of Managed PoE+ Switch

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.5 SNMP-Based Network Management

You can use an external SNMP-based application to configure and manage the Managed PoE+ Switch, such as SNMP Network Manager, HP Openview Network Node Management (NNM) or What's Up Gold. This management method requires the SNMP agent on the Managed PoE+ Switch and the SNMP Network Management Station to use the **same community string**. This management method, in fact, uses two community strings: the **get community** string and the **set community** string. If the SNMP Net-work management Station only knows the set community string, it can read and write to the MIBs. However, if it only knows the get community string, it can only read MIBs. The default getting and setting community strings for the Managed PoE+ Switch is public.

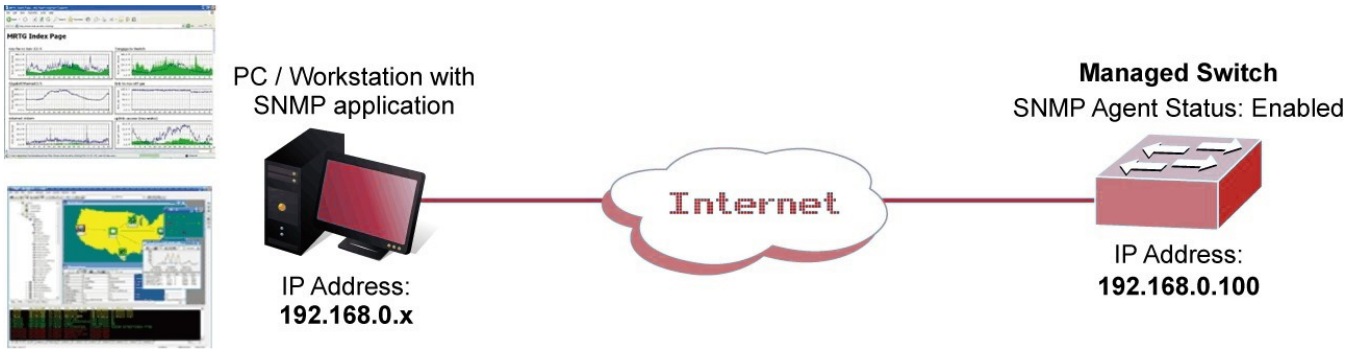


Figure 3-5: SNMP Management

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3.6 BEWARD Smart Discovery Utility

For easily listing the Managed PoE+ Switch in your Ethernet environment, the BEWARD Smart Discovery Utility is an ideal solution. The following installation instructions are to guide you to running the BEWARD Smart Discovery Utility.

1. Deposit the BEWARD Smart Discovery Utility in administrator PC.
2. Run this utility as the following screen appears.

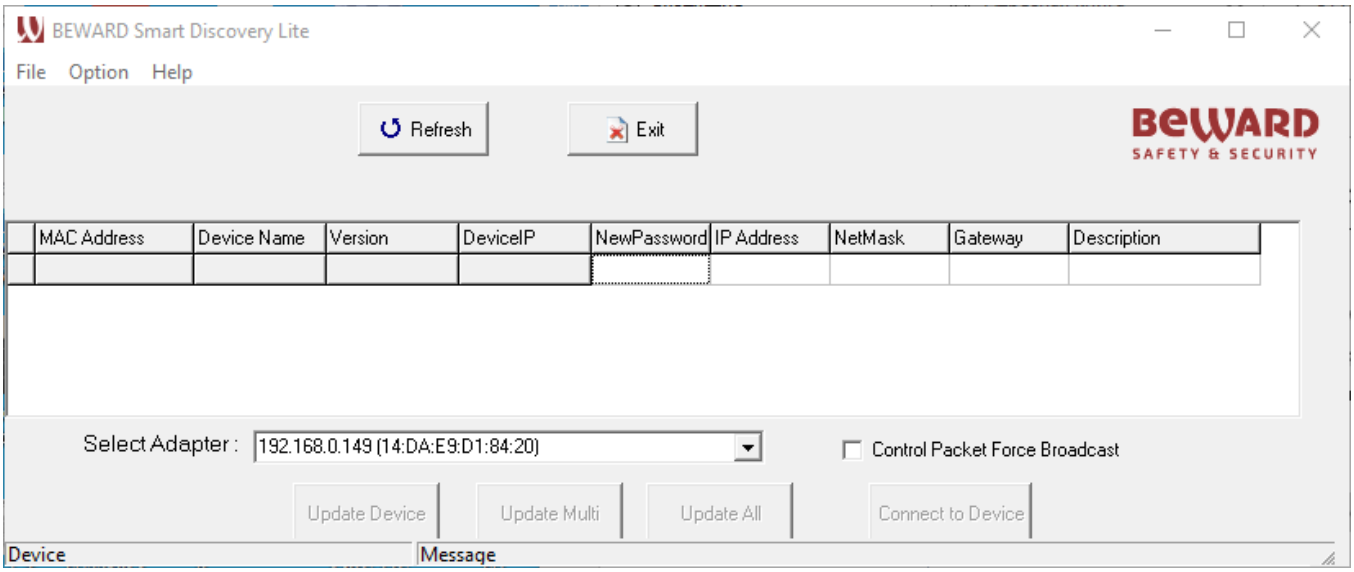


Figure 3-6: BEWARD Smart Discovery Utility Screen

If there are two LAN cards or above in the same administrator PC, choose different LAN card by using the **"Select Adapter"** tool.

3. Press **"Refresh"** button for the currently connected devices in the discovery list as the screen shows below:

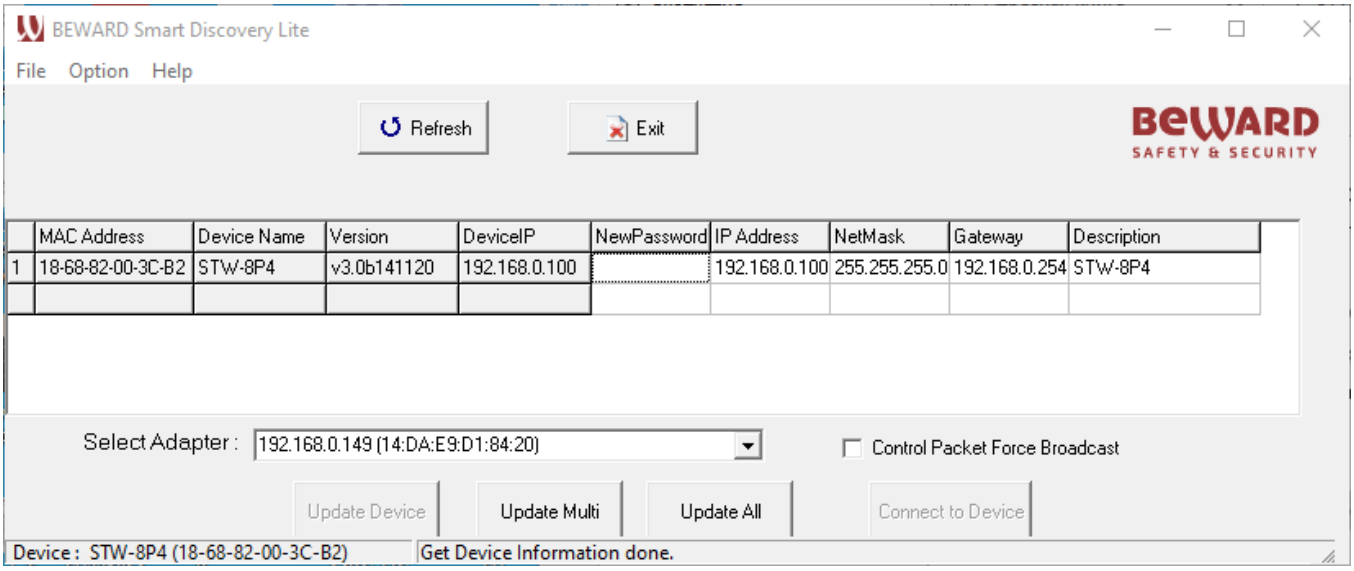


Figure 3-7: BEWARD Smart Discovery Utility Screen

SEC.RU | Короткий путь к информации
Скачано с sec.ru

1. This utility shows all necessary information from the devices, such as MAC Address, Device Name, firmware version, and Device IP Subnet address. It can also assign new password, IP Subnet address and description for the devices.
2. After setup is completed, press **"Update Device"**, **"Update Multi"** or **"Update All"** button to take effect. The meaning of the 3 buttons above are shown as below:
   - **Update Device**: use current setting on one single device.
   - **Update Multi:** use current setting on choose multi-devices.
   - **Update All:** use current setting on whole devices in the list.

   The same functions mentioned above also can be found in **"Option"** tools bar.
3. To click the **"Control Packet Force Broadcast"** function, it can allow assign new setting value to the Web Smart Switch under a different IP subnet address.
4. Press **"Connect to Device"** button and the Web login screen appears in Figure 3-4.
5. Press **"Exit"** button to shut down the BEWARD Smart Discovery Utility.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4. WEB CONFIGURATION

This section introduces the configuration and functions of the Web-based management from Managed PoE+ Switch.

About Web-based Management

The Managed PoE+ Switch offers management features that allow users to manage the Managed PoE+ Switch from anywhere on the network through a standard browser such as Microsoft Internet Explorer or Google Chrome.

The Managed PoE+ Switch can be configured through an Ethernet connection, making sure the manager PC must be set on the same IP subnet address with the Managed PoE+ Switch.

For example, the default IP address of the Managed PoE+ Switch is ***192.168.0.100***, then the manager PC should be set at **192.168.0.x** (where x is a number between 1 and 254, except 100), and the default subnet mask is 255.255.255.0.

If you have changed the default IP address of the Managed PoE+ Switch to 192.168.1.1 with subnet mask 255.255.255.0 via console, then the manager PC should be set at 192.168.1.x (where x is a number between 2 and 254) to do the relative configuration on manager PC.

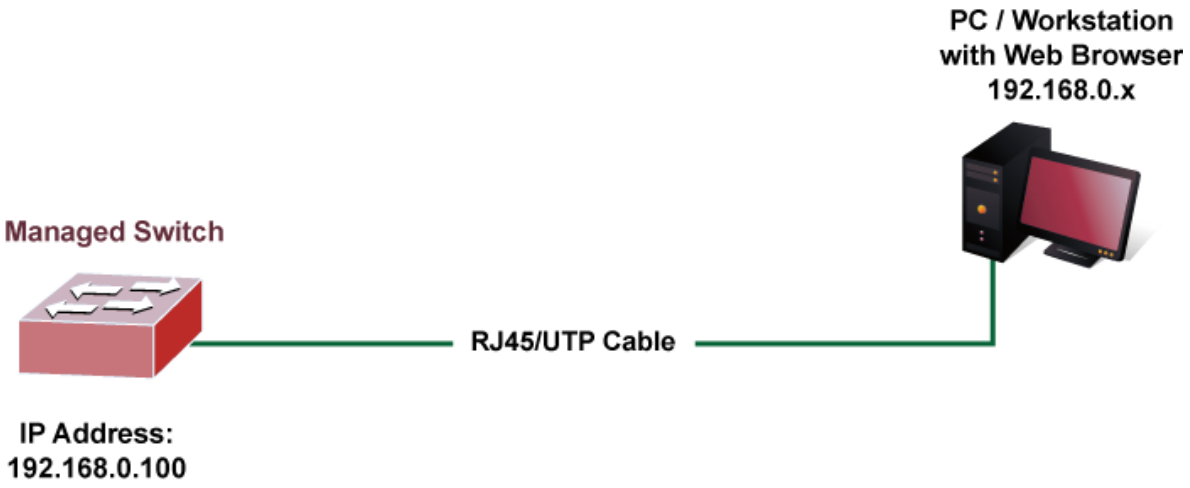


Figure 4-1-1: Web Management

SEC.RU | Короткий путь к информации
Скачано с sec.ru

■ Logging on the Managed PoE+ Switch

1. Use Internet Explorer 8.0 or above Web browser. Enter the factory-default IP address to access the Web interface. The factory-default IP Address is shown as follows:

http://192.168.0.100

2. When the following login screen appears, please enter the default username **"admin"** with password "**admin**" (or the username/password you have changed via console) to login the main screen of Managed PoE+ Switch. The login screen in Figure 4-1-2 appears.

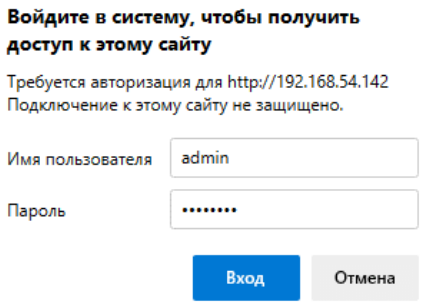


Figure 4-1-2: Login Screen

Default User name: **admin**

Default Password: **admin**

After entering the username and password, the main screen appears as shown in Figure 4-1-3.

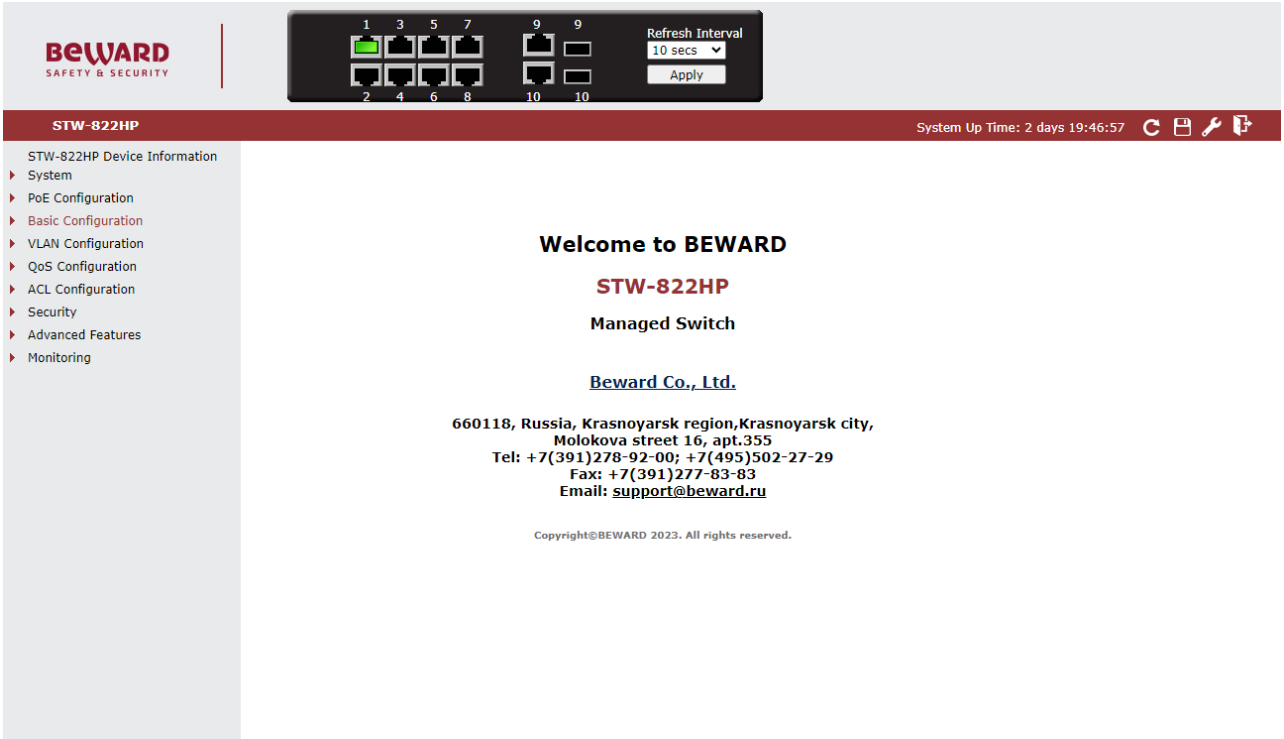
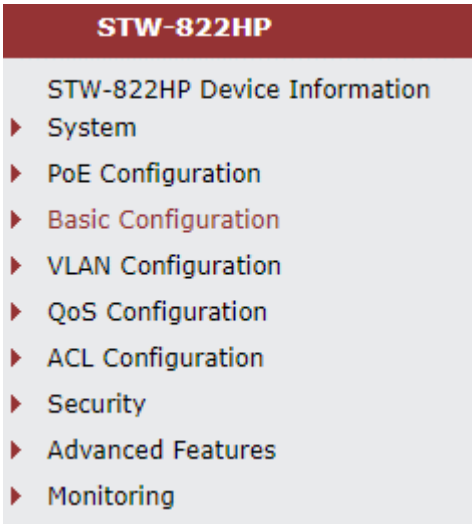


Figure 4-1-3: Web Main Page

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Now, you can use the Web management interface to continue the switch management or manage the Managed PoE+ Switch by Web interface. The Switch Menu on the left of the web Page let you access all the commands and statistics the Managed PoE+ Switch provides.



Note

1. It is recommended to use Internet Explore 8.0 or above to access Managed PoE+ Switch.
2. The changed IP address take effect immediately after clicking the **Save** icon on the top Switch Menu bar. You need to use the new IP address to access the Web interface.
3. For security reason, please change and memorize the new password after this first setup.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.1 Main Web Page

The Managed PoE+ Switch provides a Web-based browser interface for configuring and managing it. This interface allows you to access the Managed PoE+ Switch using the Web browser of your choice. This chapter describes how to use the Managed PoE+ Switch's Web browser interface to configure and manage it.

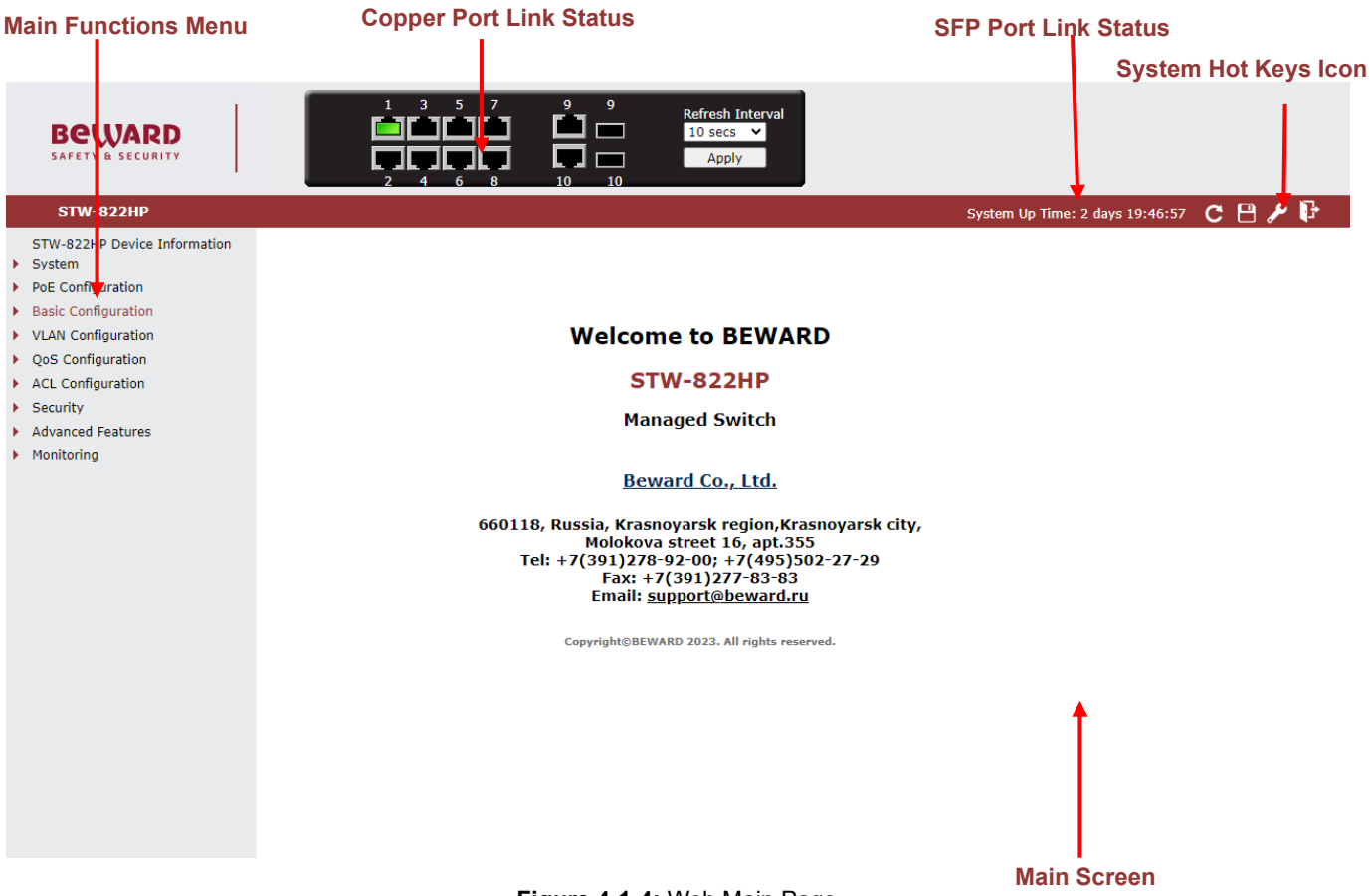


Figure 4-1-4: Web Main Page

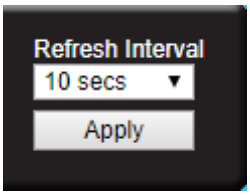
Panel Display

The web agent displays an image of the Managed PoE+ Switch's ports. The Mode can be set to display different information for the ports, including Link up or Link down. The port status are illustrated as follows:

State	Disabled	Down	Link	PoE
RJ45 Ports				
SFP Ports				

Refresh Interval Icon

The refresh interval icon are in the right side of the Managed PoE+ Switch's web panel, it provide following time setting options to refresh the web panel of Managed PoE+ Switch. The available options are **"Never", " 5 secs"**, **"10 secs"**, **"30 secs"**, **"1 min"** and **"Apply"** button to take affect.



SEC.RU | Короткий путь к информации
Скачано с sec.ru

System Hot Key Icons

The system hot keys icons are in the right side of the Managed PoE+ Switch's web page, from left to right side is System Up Time, refresh button, save config button, reboot button and logout button.

Main Menu

Using the onboard web agent, you can define system parameters, manage and control the Managed PoE+ Switch, and all its ports, or monitor network conditions. Via the Web-Management, the administrator can set up the Managed PoE+ Switch by selecting the functions those listed in the Main Function. The screen in Figure 4-1-5 appears.

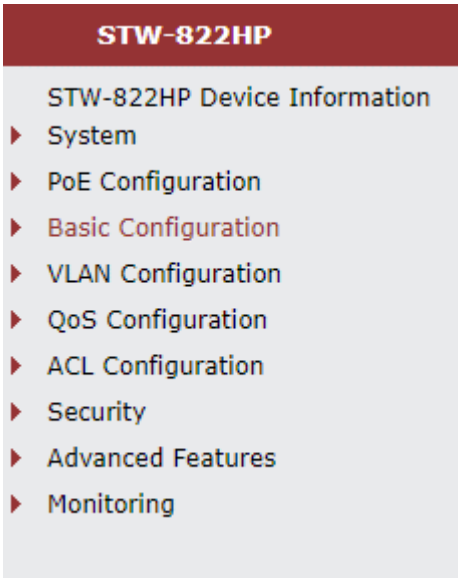
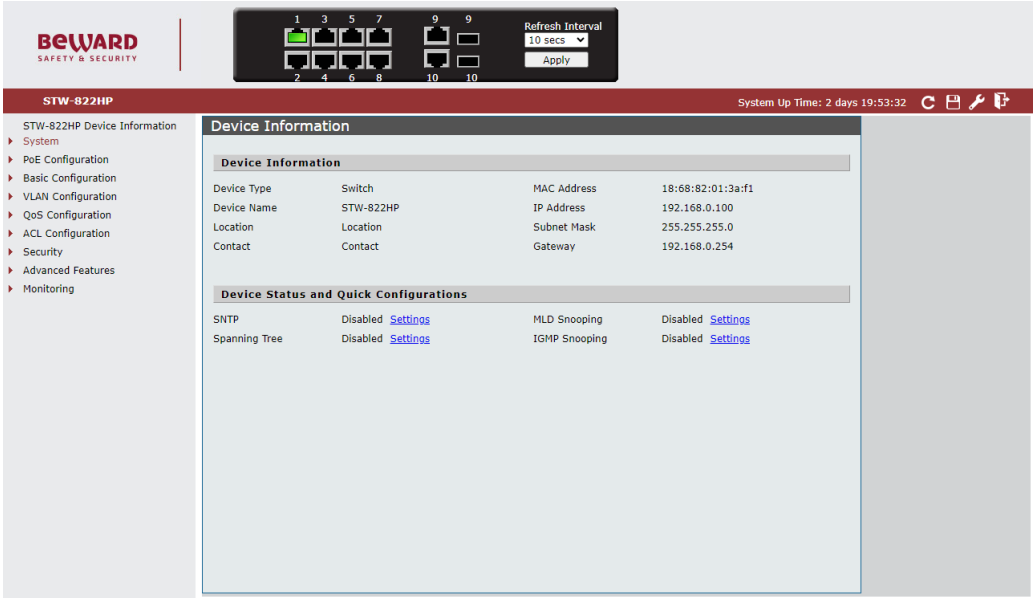


Figure 4-1-5: Managed PoE+ Switch Main Functions Menu

Device Information

Access Device Information web page, you can view device informations of the Managed PoE+ Switch, the screen in Figure 4-1-6 appears and table 4-1-1 show the items of Device Information.



SEC.RU | Короткий путь к информации
Скачано с sec.ru

Figure 4-1-6: Managed PoE+ Switch Device Information Web Page

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Device Information	
Item	**Description**
Device Type	Display the device type information.
Device Name	Display the device name information.
Location	Display the device location information.
Contact	Display the device contact information.
MAC Address	Display the device MAC address information.
IP Address	Display the device IP address information.
Subnet Mask	Display the device subnet mask information.
Gateway	Display the device gateway information.
Device Status and Quick Configurations	
Item	**Description**
SNTP	Display the SNTP status and hyperlink to SNTP setting web page.
Spanning Tree	Display the Spanning Tree status and hyperlink to Spanning Tree setting web page.
MLD Snooping	Display the MLD Snooping status and hyperlink to MLD Snooping setting web page.
IGMP Snooping	Display the IGMP Snooping status and hypelink to IGMP Snoopin setting web page.

Table 4-1-1: Item Desciptions of Device Information

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.2 System

Use the system menu items to display and configure basic administrative details of the Managed PoE+ Switch. Under the system the following topics are provided to configure and view the system information. This section has the following items:

Access system web page, you can view system functions of the Managed PoE+ Switch, the screen in Figure 4-2-1 appears and table 4-2-1 show the items of System.

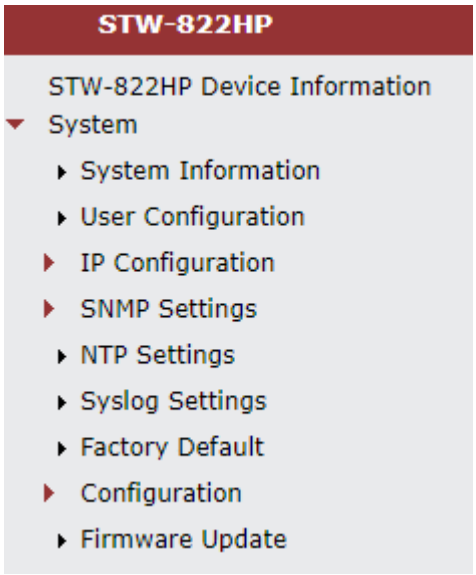


Figure 4-2-1: Managed PoE+ Switch System Web Page

System Configuration	
Item	**Description**
System Information	The Managed PoE+ Switch system information is provided here.
User Configuration	Configure the Managed PoE+ Switch username and password information on this page.
IP Configuration	Configure the Managed PoE+ Switch-managed IP/IPv6 information on this page.
SNMP Settings	Configure the Managed PoE+ Switch-SNMP functions on this web page.
NTP Settings	Configure the Managed PoE+ Switch-NTP function on this web page.
Syslog Settings	Configure the Managed PoE+ Switch-System log function on this web page.
Factory Default	Reset the Managed PoE+ Switch to default mode that excluding the IP address, User name and Password.
Configuration	Configure the Managed PoE+ Switch configuration file backup and restore.
Firmware Update	This Page facilitates an update of the firmware controlling the Managed PoE+ Switch.

Table 4-2-1: Item Desciptions of System Web Page

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.2.1 System Information

The System Infomation Page provides information for the current device information. System Information Page helps a switch administrator to identify the hardware MAC address, firmware version and system uptime and also config the device name, comment, location and contact information. The screen in Figure 4-2-2 appears.

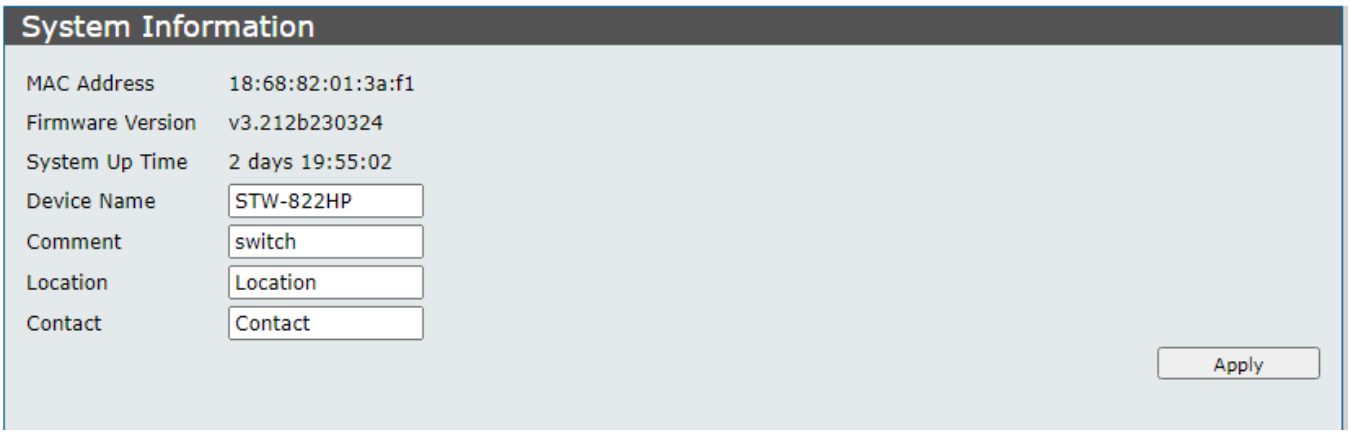


Figure 4-2-2: System Information Page Screenshot

The page includes the following fields:

Object	Description
• **MAC Address**	The Managed PoE+ Switch MAC Address information is provided here.
• **Firmware Version**	The Managed PoE+ Switch firmware version information is provided here.
• **System Up Time**	The Managed PoE+ Switch system active time information is provided here.
• **Device Name**	Configure the Managed PoE+ Switch device name information on this web page, the maximum length is 15 characters.
• **Comment**	Configure the Managed PoE+ Switch comment information on this web page, the maximum length is 15 characters.
• **Location**	Configure the Managed PoE+ Switch location information on this web page, the maximum length is 15 characters.
• **Contact**	Configure the Managed PoE+ Switch contact information on this web page, the maximum length is 15 characters.

Button

Apply : press this button to take affect.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.2.2 User Configuration

The User configuration includes the User Name,Password and Confirm Password. The configured column is used to view or change the User Name and Password. The screen in Figure 4-2-3 appears.

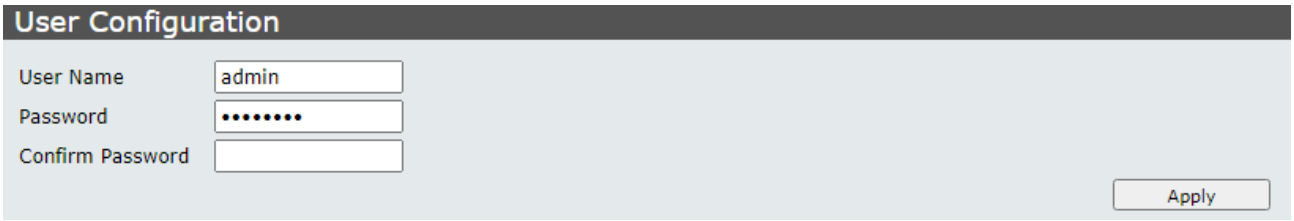
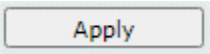


Figure 4-2-3: User Configuration Page Screenshot

The Current column is used to show the user configuration.

Object	Description
• **User Name**	Configure the Managed PoE+ Switch user name information on this web page, the maximum length is 15 characters.
• **Password**	Configure the Managed PoE+ Switch password information on this web page, the maximum length is 15 characters.
• **Confirm Password**	Confirm the Managed PoE+ Switch password information on this web page, the maximum length is 15 characters.

Button



: press this button to take affect.

If you forget the new password after changing the default password, please press the ***"Reset"*** button on the front panel of the Managed PoE+ Switch for over 5 seconds and then release it. The current setting including VLAN will be lost and the Managed PoE+ Switch will restore to the default mode.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.2.3 IP Configuration

The IP configuration includes the IPv4 subnet address setting and IPv6 subnet address setting, the configured column is used to view or change the IP configuration.

4.2.3.1 IPv4

The IPv4 configuration includes the IPv4 Address, Subnet Mask, Default Gateway and DNS Server, also the DHCPv4 Client Enable function. The configured column is used to view or change the IPv4 Address, Subnet Mask, Default Gateway and DNS Server. Fill up the IPv4 Address, Subnet Mask and Default Gateway or enable the DHCPv4 Client function for the Managed PoE+ Switch. The screen in Figure 4-2-4 appears.

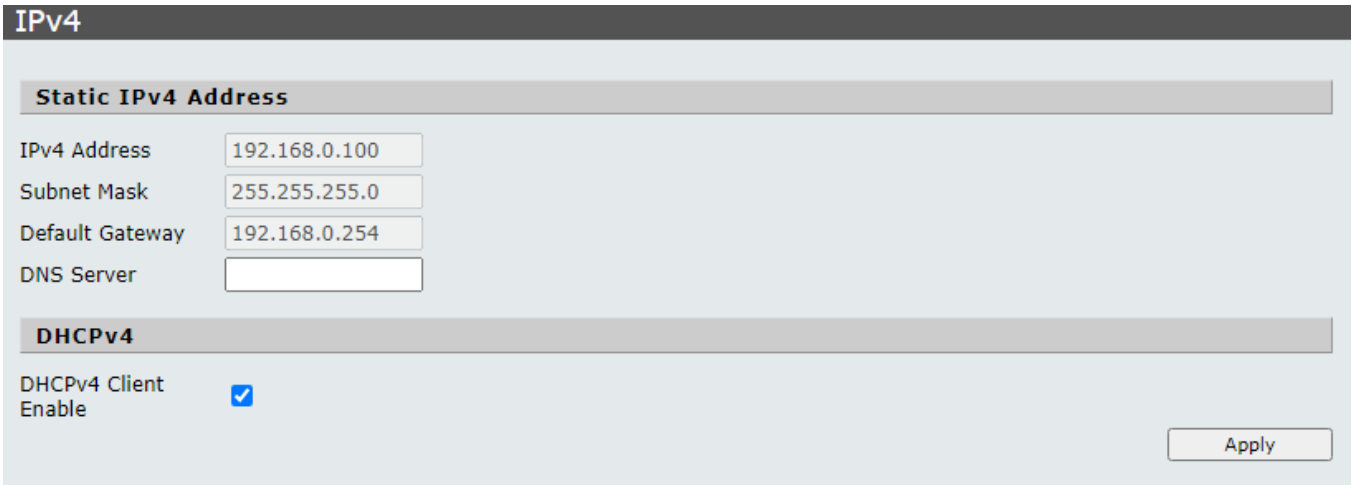


Figure 4-2-4: IPv4 Page Screenshot

4.2.3.2 IPv6

The IPv4 Configuration includes the IPv6 Address, Subnet Prefix Length, Default Gateway and DNS Server, also the DHCPv6 Client Enable function. The configured column is used to view or change the IPv6 Address, Subnet Prefix Length, Default Gateway and DNS Server. Fill up the IPv6 Address, Subnet Prefix Length and Default Gateway or enable the DHCPv6Client function for the Managed PoE+ Switch. The screen in Figure 4-2-5 appears.

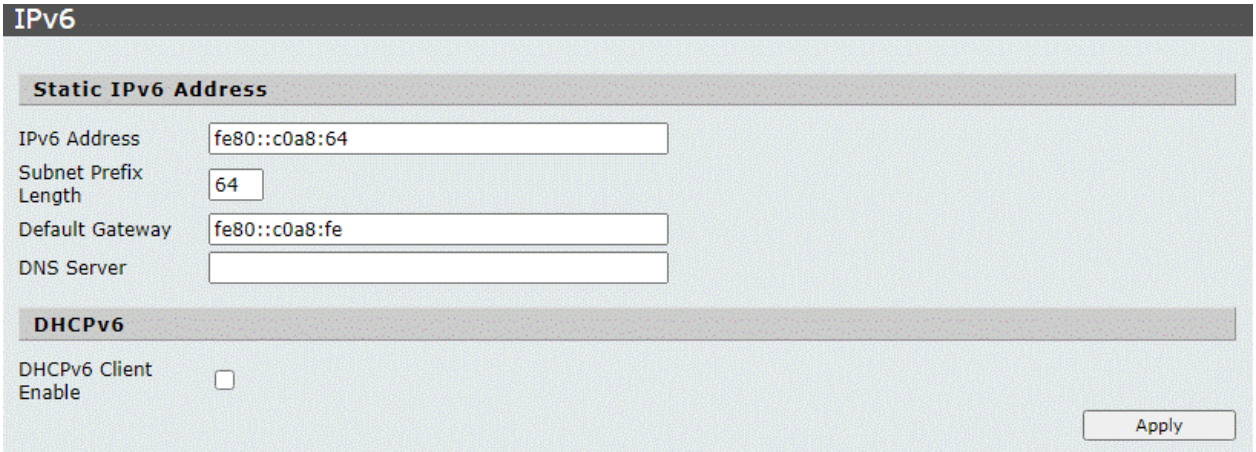


Figure 4-2-5: IPv6 Page Screenshot

Button

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Apply : press this button to take affect.

4.2.4 SNMP Settings

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

An SNMP-managed network consists of three key components: Network management stations (NMSs), SNMP agents, Management information base (MIB) and network-management protocol：

- **Network management stations (NMSs)**：Sometimes called consoles, these devices execute management applications that monitor and control network elements. Physically, NMSs are usually engineering workstation-caliber computers with fast CPUs, megapixel color displays, substantial memory, and abundant disk space. At least one NMS must be present in each managed environment.
- **Agents**：Agents are software modules that reside in network elements. They collect and store management information such as the number of error packets received by a network element.
- **Management information base (MIB)**：A MIB is a collection of managed objects residing in a virtual information store. Collections of related managed objects are defined in specific MIB modules.
- **network-management protocol**：A management protocol is used to convey management information between agents and NMSs. SNMP is the Internet community's de facto standard management protocol.

SNMP Operations

SNMP itself is a simple request/response protocol. NMSs can send multiple requests without receiving a response.

- **Get --** Allows the NMS to retrieve an object instance from the agent.
- **Set --** Allows the NMS to set values for object instances within an agent.
- **Trap --** Used by the agent to asynchronously inform the NMS of some event. The SNMPv2 trap message is designed to replace the SNMPv1 trap message.

SNMP community

An SNMP community is the group that devices and management stations running SNMP belong to. It helps define where information is sent. The community name is used to identify the group. A SNMP device or agent may belong to more than one SNMP community. It will not respond to requests from management stations that do not belong to one of its communities. SNMP default communities are:

- **Write** = private
- **Read** = public

Use the SNMP Menu to display or configure the Managed PoE+ Switch's SNMP function. This section has the following items:

■ **SNMP View Table**	Configure SNMP view table settings on this web page.
■ **SNMP Group Table**	Configure SNMP group settings on this web page.
■ **SNMP User Table**	Configure SNMP user table settings on this web page.
■ **SNMP Community Table**	Configure SNMP community table on this web page.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

- **SNMP Host Table** Configure SNMP host table on this web page.
- **SNMP Configuration** Configure SNMP configuration on this web page.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.2.4.1 SNMP View Table

The SNMP View Table provide to set view rules for allow or deny access to certain MIB objects, the configured column is used to input the view name, subtree OID and change the view type. The screen in Figure 4-2-6 appears.

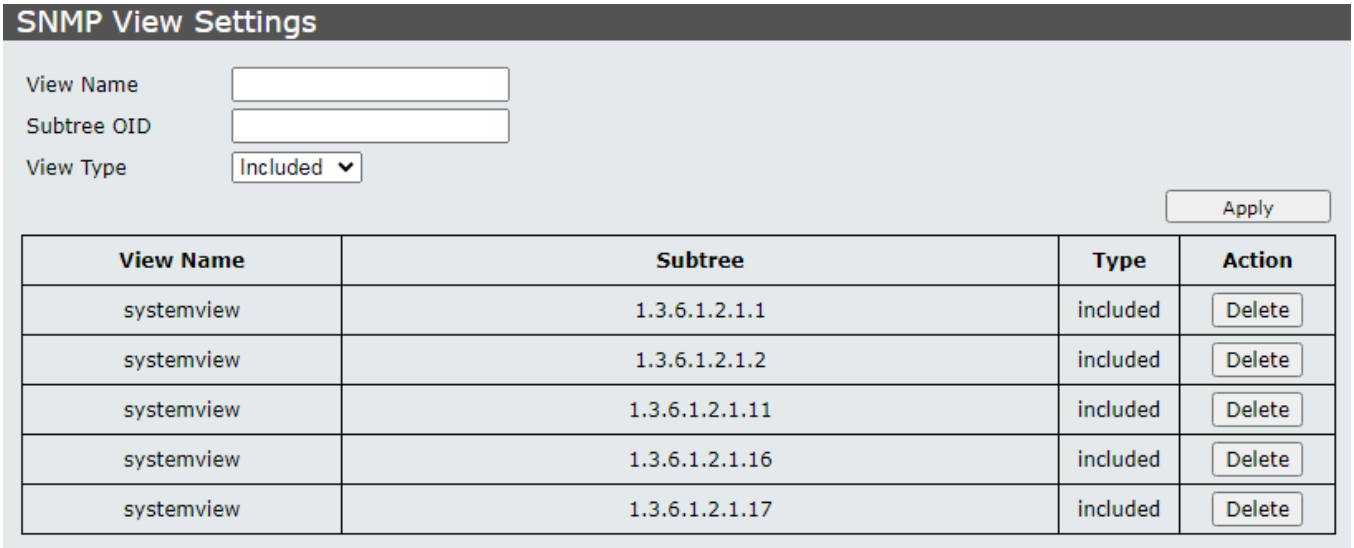


Figure 4-2-6: SNMP View Table Configuration Page Screenshot

The Current column is used to show the SNMP View Table configuration.

Object	Description
• **View Name**	Configure the Managed PoE+ Switch view name information on this web page, the maximum length is 20 characters.
• **Subtree OID**	Configure the Managed PoE+ Switch Subtree OID information on this web page.
• **View Type**	Configure the Managed PoE+ Switch view type mode on this web page, the available options are **Included** and **Excluded**.

Buttons

Apply : press this button to take affect.

Delete : press this button to delete.

Note

Each view need to configure a view rule, otherwise it will affect the SNMP function.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.2.4.2 SNMP Group Table

The SNMP View Table provide to set SNMP Group settings, the configured column is used to input the group name, change the Read, Write, Notify view type and Security Model /Level. The screen in Figure 4-2-7 appears.

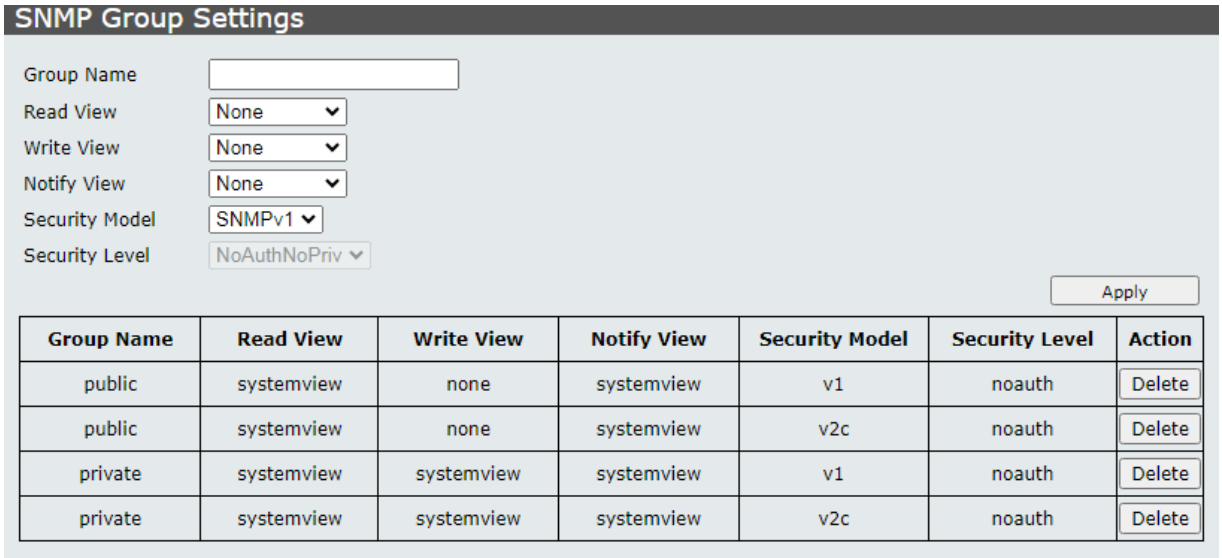


Figure 4-2-7: SNMP Group Table Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Group Name**	Configure the Managed PoE+ Switch group name information on this page, the maximum length is 20 characters.
• **Read View**	Choose the Read View and available options are: ■ **None**: Set none for Read View status. ■ **systemview**: Set systemview for Read View status.
• **Write View**	Choose the Write View and available options are: ■ **None**: Set none for Read View status. ■ **systemview**: Set systemview for Write View status.
• **Notify View**	Choose the Notify View and available options are: ■ **None**: Set none for Read View status. ■ **systemview**: Set systemview for Notify View status.
• **Security Model**	Indicates the SNMP supported version. Possible versions are: ■ **SNMP v1**: Set SNMP supported version 1. ■ **SNMP v2**: Set SNMP supported version 2c. ■ **SNMP v3**: Set SNMP supported version 3.
• **Security Level**	Available when choose the SNMPv3 in Security Model. Possible versions are: ■ **NoAuthNoPriv**: None authentication and none privacy. ■ **AuthNoPriv**: Authentication and none privacy. ■ **AuthPriv**: Authentication and privacy.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Buttons

Apply : press this button to take affect.

Delete : press this button to delete.

Note

The SNMP group needs to create the view before group create.

4.2.4.3 SNMP User Table

The SNMP User Table provide to set SNMP user settings, the configured column is used to input the user name, select the group name and input the password for Auth-Protocol MD5 /Priv-Protocol DES. The screen in Figure 4-2-8 appears.

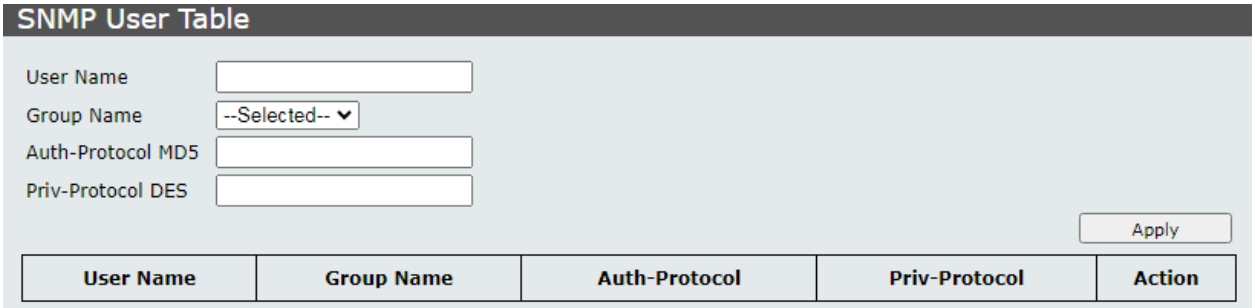


Figure 4-2-8: SNMP User Table Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **User Name**	Configure the Managed PoE+ Switch user name information on this page, the maximum length is 20 characters.
• **Group Name**	Select the exist SNMP group.
• **Auth-Protocol MD5**	Set the authorization password with using the MD5 authentication level, the available length is 8 to16 characters.
• **Priv-Protocol DES**	Set the authorization password with using the standard DES private encryption protocol, the available length is 8 to16 characters.

Buttons

Apply : press this button to take affect.

Delete : press this button to delete.

Note

Create SNMP views and groups are required to use, the security level of the user needs to be the same as the security level of the group.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.2.4.4 SNMP Community Table

The SNMP User Table provides to set SNMP community settings; the configured column is used to input the community name, and select the group name for access group as the screen in Figure 4-2-9 appears.

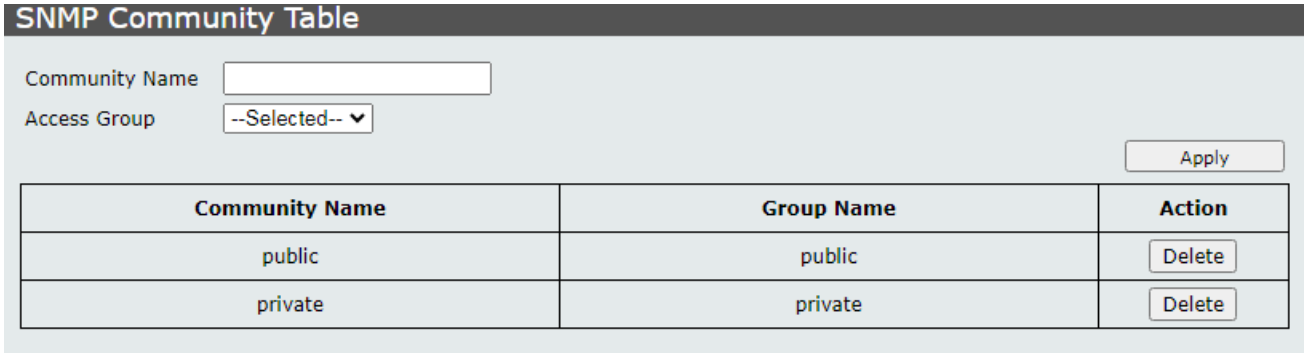


Figure 4-2-9: SNMP Community Table Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Community Name**	Configure the Managed PoE+ Switch community name information on this page, the maximum length is 20 characters.
• **Access Group**	Select the exist access group.

Buttons

Apply : press this button to take affect.

Delete : press this button to delete.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.2.4.5 SNMP Host Table

The SNMP Host Table provides to set SNMP host settings. The configured column is used to input the host IP address, and select the security model, security level and community string for SNMPv3 user as the screen in Figure 4-2-10 appears.

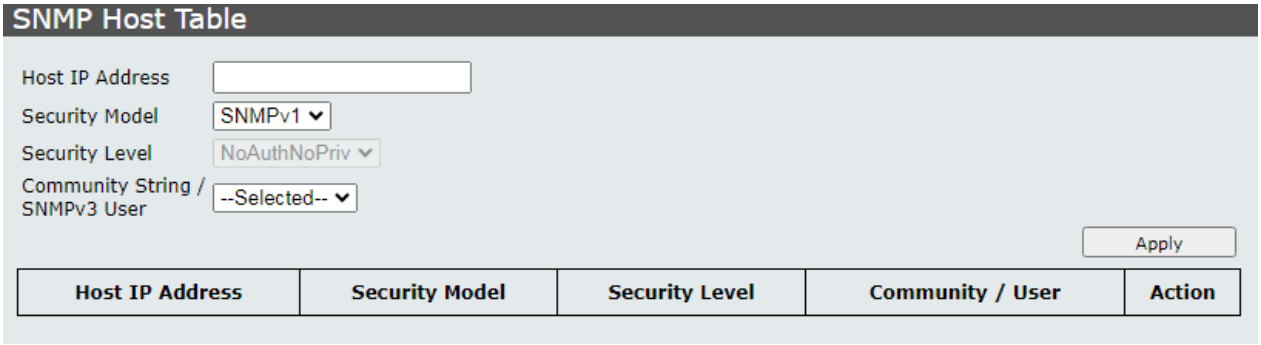


Figure 4-2-10: SNMP Host Table Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Host IP Address**	Configure the Managed PoE+ Switch IPv4 Host Ip address on this page.
• **Security Model**	Indicates the SNMP supported version. Possible versions are: ■ **SNMP v1**: Set SNMP supported version 1. ■ **SNMP v2**: Set SNMP supported version 2c. ■ **SNMP v3**: Set SNMP supported version 3.
• **Security Level**	Available when choose the SNMPv3 in Security Model. Possible versions are: ■ **NoAuthNoPriv**: None authentication and none privacy. ■ **AuthNoPriv**: Authentication and none privacy. ■ **AuthPriv**: Authentication and privacy.
• **Community String/SNMPv3 User**	Select the exist community string for SNMPv3 user.

Button

Apply: press this button to take affect.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.2.4.6 SNMP Configuration

The SNMP Host Table provides to set SNMP settings; the configured column is used to input the selected operation modes of SNMP State, SNMP Trap and SNMP Link Change Traps as the screen in Figure 4-2-11 appears.

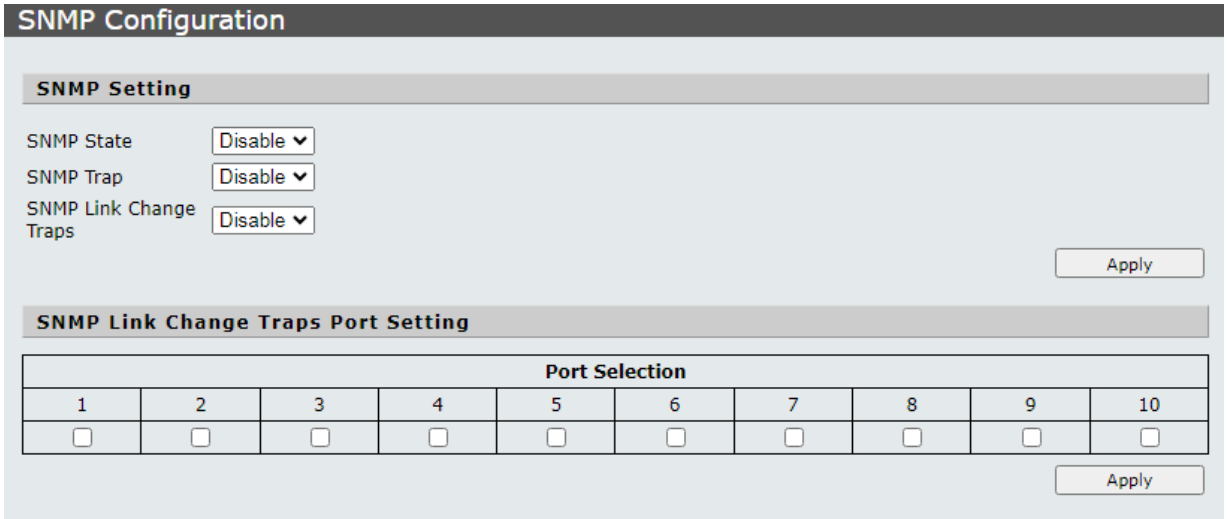
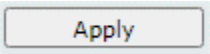


Figure 4-2-11: SNMP Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **SNMP State**	Enable or Disable the Managed PoE+ Switch SNMP function on this page.
• **SNMP Trap**	Enable or Disable the Managed PoE+ Switch SNMP trap function on this page.
• **SNMP Link Change Traps**	Enable or Disable the Managed PoE+ Switch SNMP Link Change trap function on this page.

Button



: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.2.5 NTP Settings

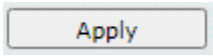
On this page. **NTP**, an acronym for **Network Time Protocol**, is for synchronizing the clocks of computer systems. NTP uses UDP (data grams) as transport layer. You can specify NTP Servers and set GMT time zone. The NTP configuration screen in Figure 4-2-12 appears.

Figure 4-2-12: NTP Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **System Time**	Display current system time of Managed PoE+ Switch.
• **State**	Indicates the NTP mode operation. Possible modes are: ■ **Enable**: Enable NTP mode operation. When enable NTP mode operation, the agent forward and to transfer NTP messages between the clients and the server when they are not on the same subnet domain. ■ **Disable**: Disable NTP mode operation.
• **Time Zone**	Allow selecting the time zone according to current location of Managed PoE+ Switch.
• **Primary Server IP**	Configure the NTP server IPv4 IP address on this page.
• **Secondary Server IP**	Configure the NTP server IPv4 IP address on this page.

Button



: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.2.6 Syslog Settings

The Syslog settings provide to set system log settings, the configured column is used to select the related settings of Syslog settings as the screen in Figure 4-2-13 appears.

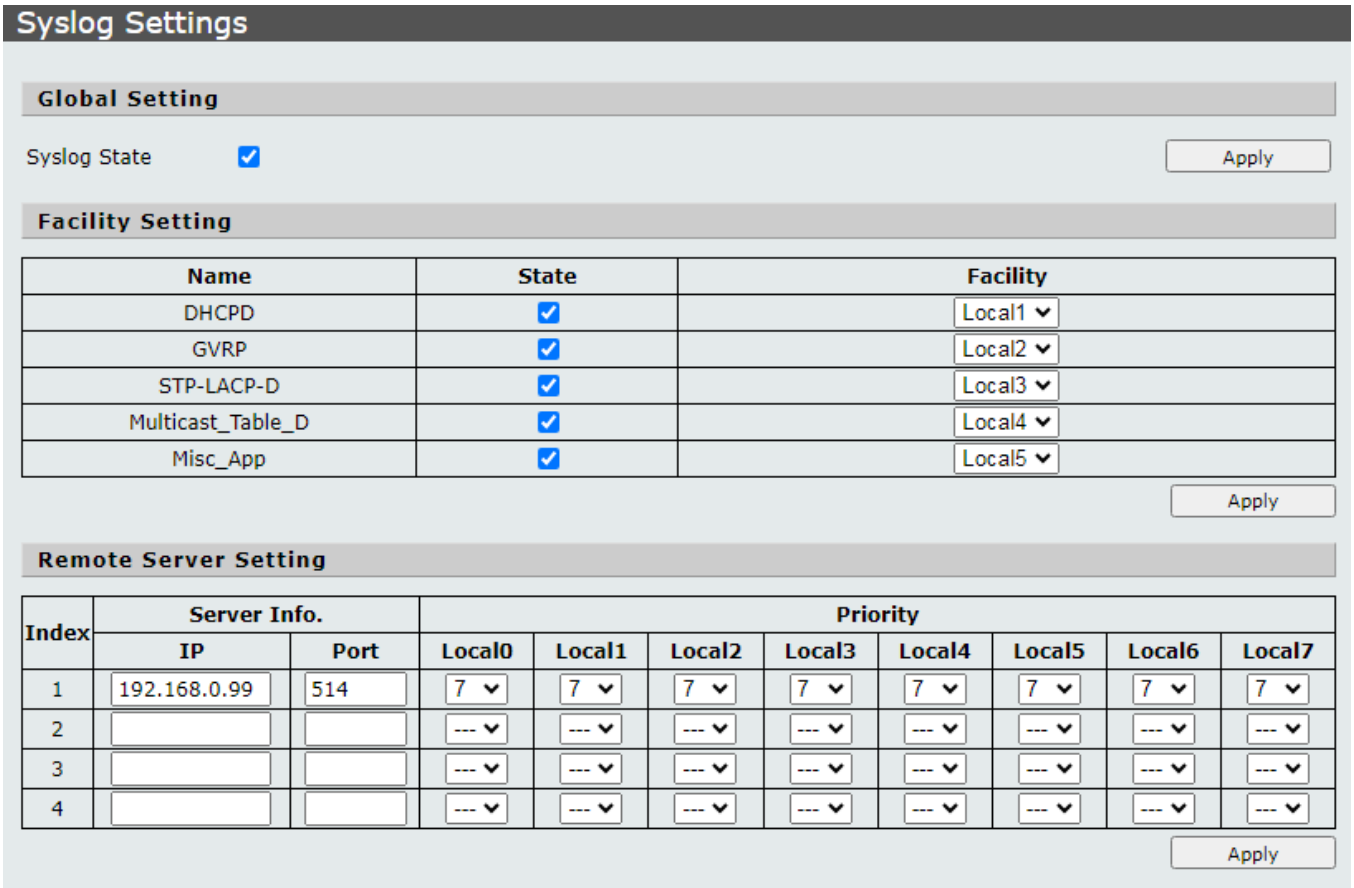
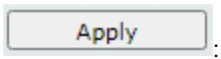


Figure 4-2-13: Syslog Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Syslog State**	Enable or disable the Syslog function.
• **Name**	Display the available protocol for facility setting on this page.
• **State**	Click to enable the available protocol for facility setting on this page.
• **Facility**	Selelct the local device number and the range is 0 to 7.
• **IP**	Input the IP address of remote server
• **Port**	The port number of remote server.
• **Priority**	Log priority range 0 to 7.

Button



: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.2.7 Factory Default

You can reset the configuration of the Managed PoE+ Switch on this page. Only the IP configuration is retained. The new configuration is available immediately, which means that no restart is necessary. The Factory Default screen in Figure 4-2-14 appears.

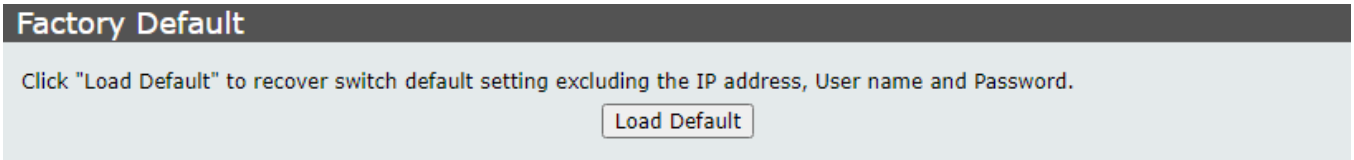


Figure 4-2-14: Factory Default Configuration Page Screenshot

Button

Load Default : Click to reset the configuration to Factory Defaults.

Note

To reset the Managed PoE+ Switch to the Factory default setting, you can also press the hardware-based reset button at the front panel about 5 seconds.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.2.8 Configuration

The configuration includes backup and reload the current configuration of the Managed PoE+ Switch to/from the local management station.

4.2.8.1 Backup

The backup configuration provides downloading the Managed PoE+ Switch configuration file (Current.tar.gz) to local management station as the screen in Figure 4-2-15 appears.

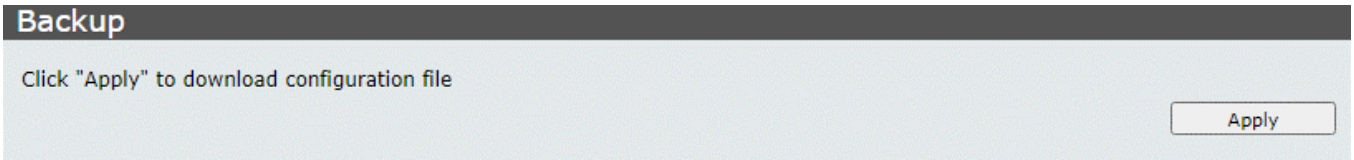


Figure 4-2-15: Backup Configuration Page Screenshot

4.2.8.2 Restoration

The restore configuration provides upload the Managed PoE+ Switch configuration file (Current.tar.gz) to other Managed PoE+ Switch from local management station as the screen in Figure 4-2-16 appears.

Figure 4-2-16: Restoring Configuration Page Screenshot

Note

The Managed PoE+ Switch configures restoration as **the IP address setting is excluded**.

Button

Apply : press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.2.9 Firmware Update

This page facilitates an update on the firmware controlling the switch as the Web Firmware Upgrade screen in Figure 4-2-17 appears.

Figure 4-2-17: Web Firmware Update Page Screenshot

To open **Firmware Upgrade** screen, perform the following:

1. Click **System** -> **Firmware Upgrade**.
2. Click the "Choose File" button of the Main Page and select the firmware file in the pop-up selection menu.
3. Select the firmware then click "Apply", the **Software Upload Progress** would show the file with upload status.
4. The firmware is loaded to the system successfully. Firmware will update after reboot.

Note

DO NOT Power OFF the Managed PoE+ Switch until the update progress is complete.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.3 PoE Configuration

On the Access PoE configuration web page, you can view PoE function information of the Managed PoE+ Switch as the screen in Figure 4-3-1 appears.

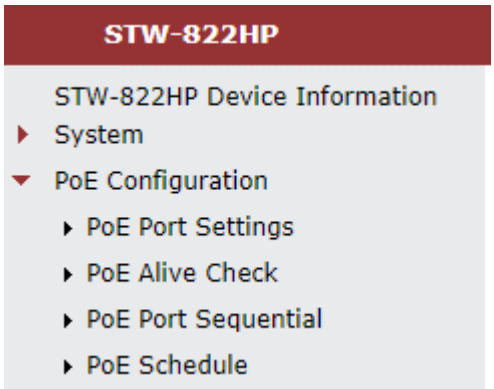


Figure 4-3-1: Managed PoE+ Switch PoE Configuration Web Page

PoE Configuration	
Item	**Description**
PoE Port Settings	Display and configure PoE Port settings.
PoE Alive Check	Display and configure PoE Alive Check settings.
PoE Port Sequential	Display and configure PoE Port Sequential settings.
PoE Schedule	Display and configure PoE Schedule settings.

Table 4-3-1: Descriptions of PoE Configuration

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.3.1 PoE Port Settings

This page provides configuration for all PoE ports as the PoE Port settings screen in Figure 4-3-3 appears.

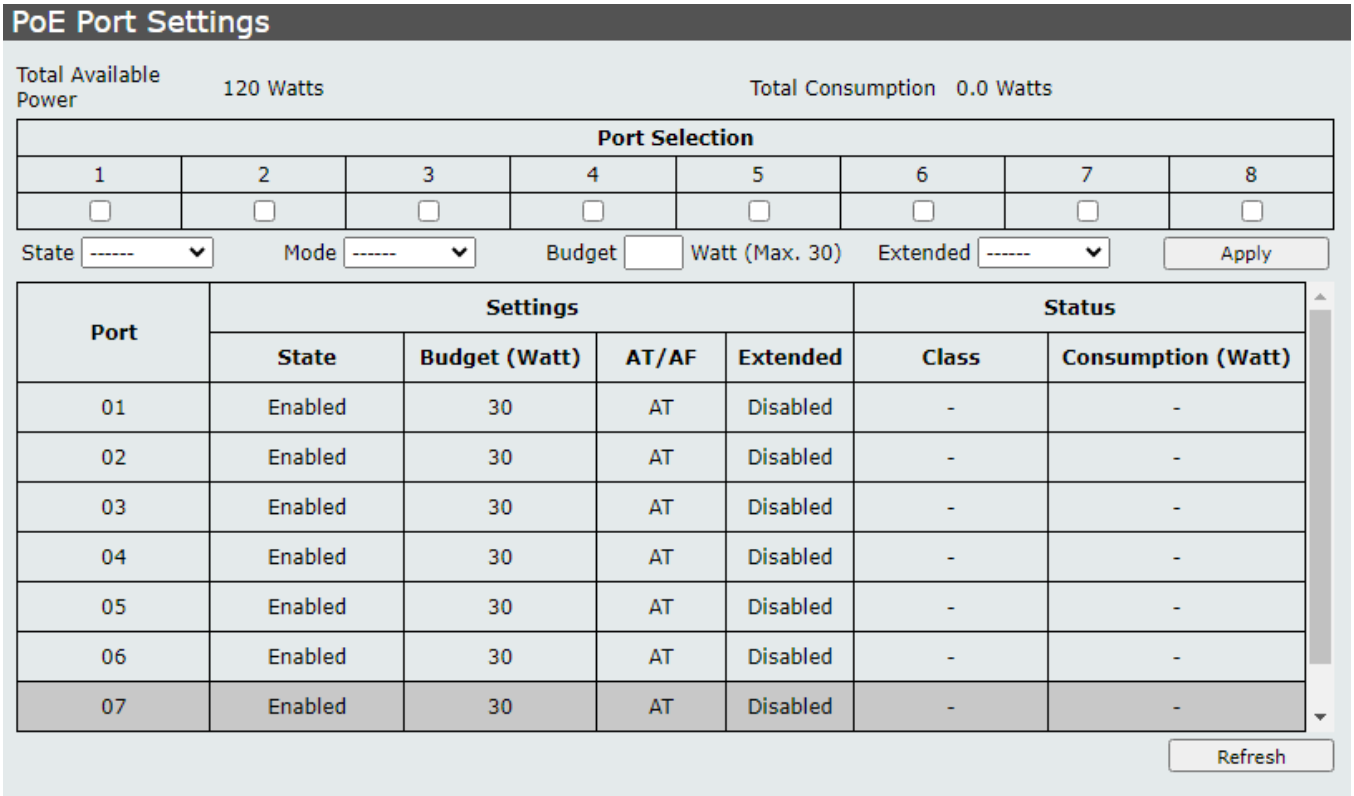


Figure 4-3-3: PoE Port Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Total Available Power**	Display Managed PoE+ Switch PoE Budget.
• **Total Consumption**	Display Managed PoE+ Switch current PoE power used in watts..
• **Port Selection**	Select specific PoE port for further configuration.
• **State**	Enable or disable specific PoE port power feeding function.
• **Mode**	Choose AT or AF PoE operation mode.
• **Budget (Watt)**	Input the PoE power output value and the available options are 1 to 30 watts.
• **Extended**	Enable or disable PoE extend mode
Port	Display per PoE port list.
Settings	
• **State**	Display per PoE port operation status.
• **Budget (Watt)**	Display per PoE port budget setting.
• **AT/AF**	Display per PoE port AT/AF setting.
• **Extended**	Display per PoE port extend mode status
Status	
• **Class**	Display per PoE port current PoE class value detection.
• **Consumption (Watt)**	Display per PoE port current PoE power usage information in watts.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Buttons

Apply : press this button to confirm the changes.

Refresh : press this button to refresh information.

4.3.2 PoE Alive Check

The Managed PoE+ Switch can be configured to monitor connected PD's status in real-time via ping action. Once the PD stops working and without response, Managed PoE+ Switch is going to restart PoE port port power, and bring the PD back to work. It will greatly enhance the reliability and reduces administrator management burden.

This page provides you how to configure PD Alive Check function as the screen in Figure 4-3-4 appears.

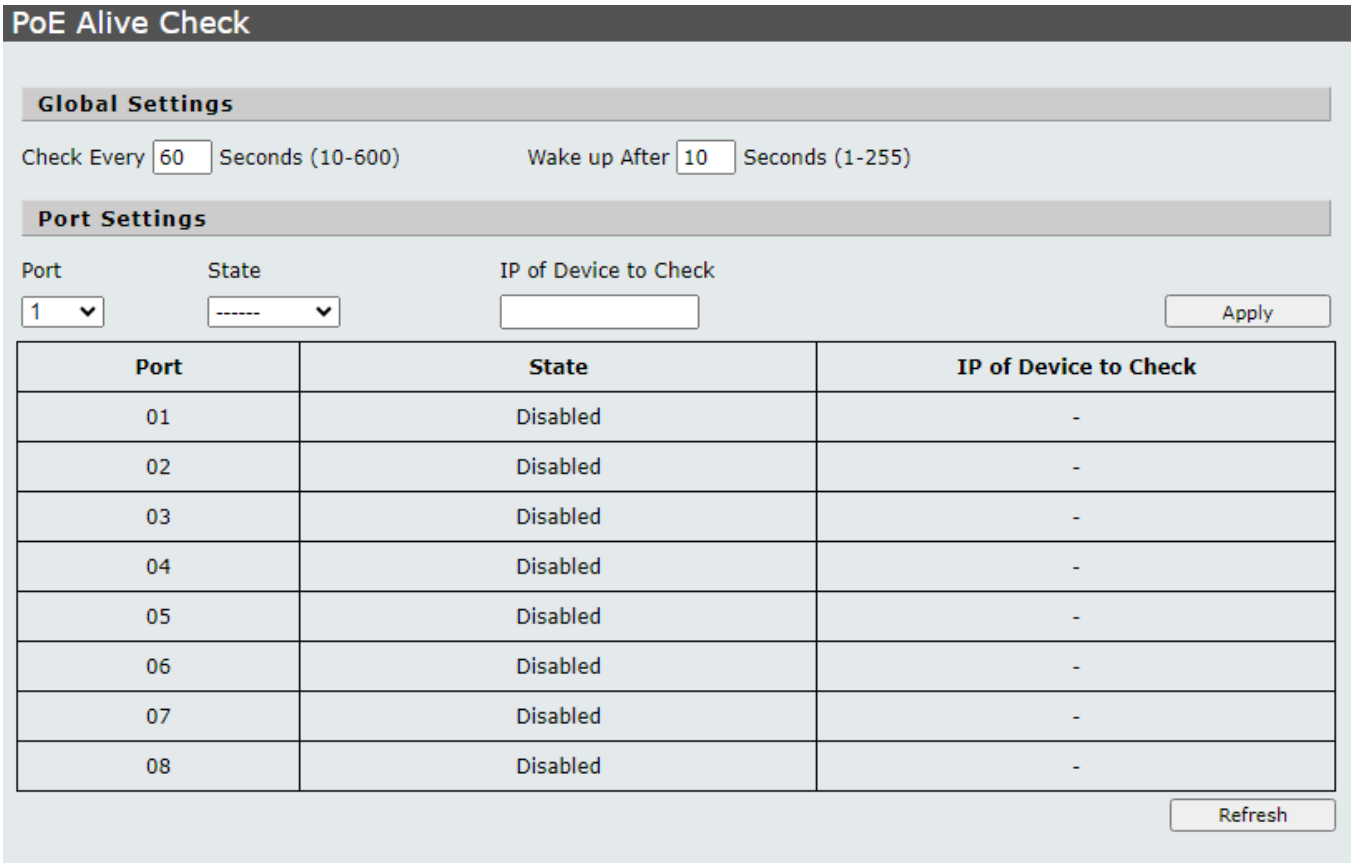


Figure 4-3-4: PoE Alive Check Configuration Page Screenshot

The page includes the following fields:

Object	Description
Global Settings	
• **Check Every xxx Seconds**	This column allows user to set how long system should be issue a ping request to PD for detecting PD is alive or dead. Check time range is from 10 seconds to 600 seconds.
• **Wake up After xxx Seconds**	This column allows user to set the PoE device rebooting time, due to there are so many kind of PoE device on the market and theyhave different rebooting time. This function is not a defining standard, so the PoE device on the market doesn't report reboots done information to Managed PoE+ Switch, so user has

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	to make sure how long the PD will be finished to boot, and then set the time value to this column. System is going to check the PD again according to the reboot time. If ou can not make sure precisely booting time, we suggest you to set it longer.
Port Settings	
• **Port**	Select specific PoE port for further configuration and list all ports on this page.
• **State**	Enable or disable specific PoE port PoE Alive Check function and display current status of eachPoE port.
• **IP of Device to Check**	This column allows user to set PoE device IP address here for system making ping to the PoE device. Please be noticed that the PD's IP address must be set to the same network segment with Managed PoE+ Switch. Also display current setting of eachPoE port.

Buttons

Apply : press this button to confirm the changes.

Refresh : press this button to refresh information.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.3.3 PoE Port Sequential

This page allows the user to configure the PoE Ports started up interval time as the PoE Port Sequential configuration screen in Figure 4-3-5 appears.

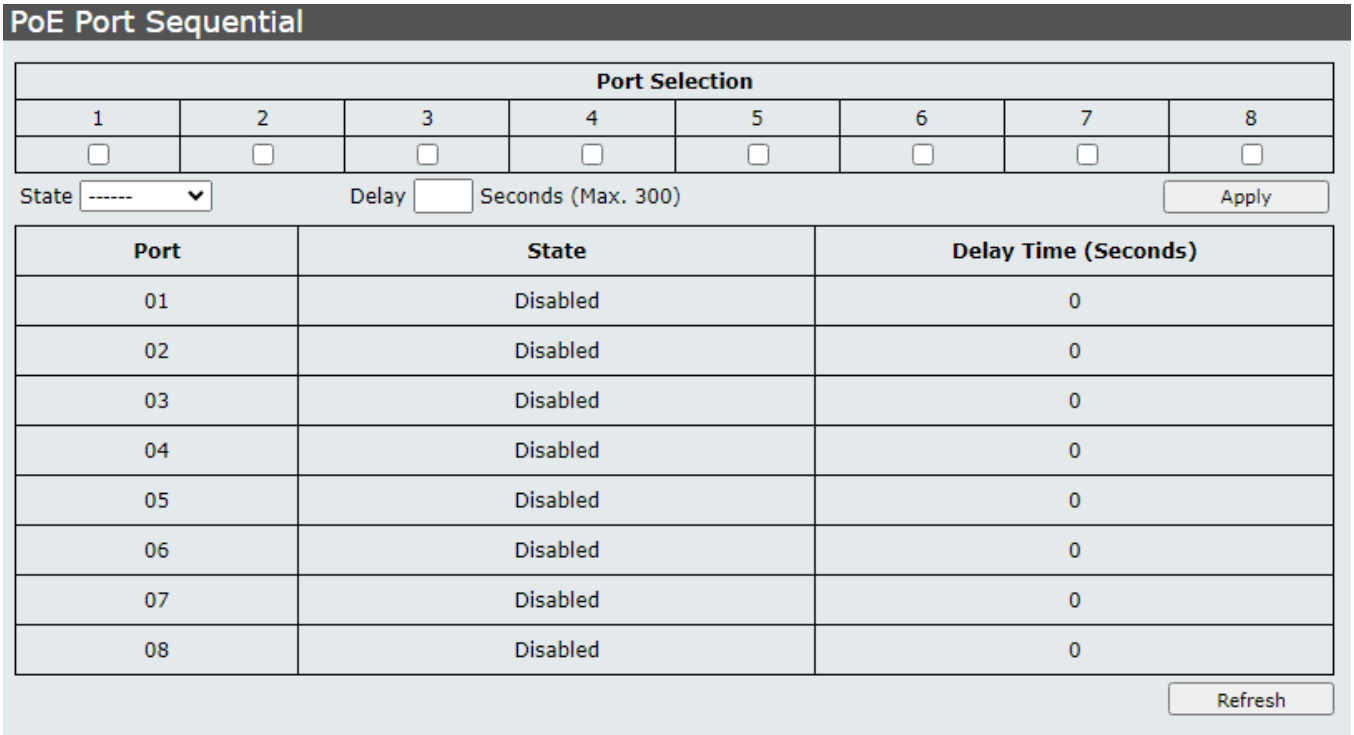


Figure 4-3-5: PoE Port Sequential Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Selection**	Select specific PoE port for further configuration.
• **State**	Enable or disable specific PoE Port sequential function.
• **Delay xxx Seconds** • **(Max. 300)**	This column allows user to configure the PoE Port Start Up interval time. Delay time range is from 1 seconds to 300 seconds.
• **Port**	Display per PoE port list.
• **State**	Display per PoE port operation status.
• **Delay Time (Seconds)**	Display per PoE port delay time (seconds) setting.

Buttons

Apply : press this button to confirm the changes.

Refresh : press this button to refresh information.

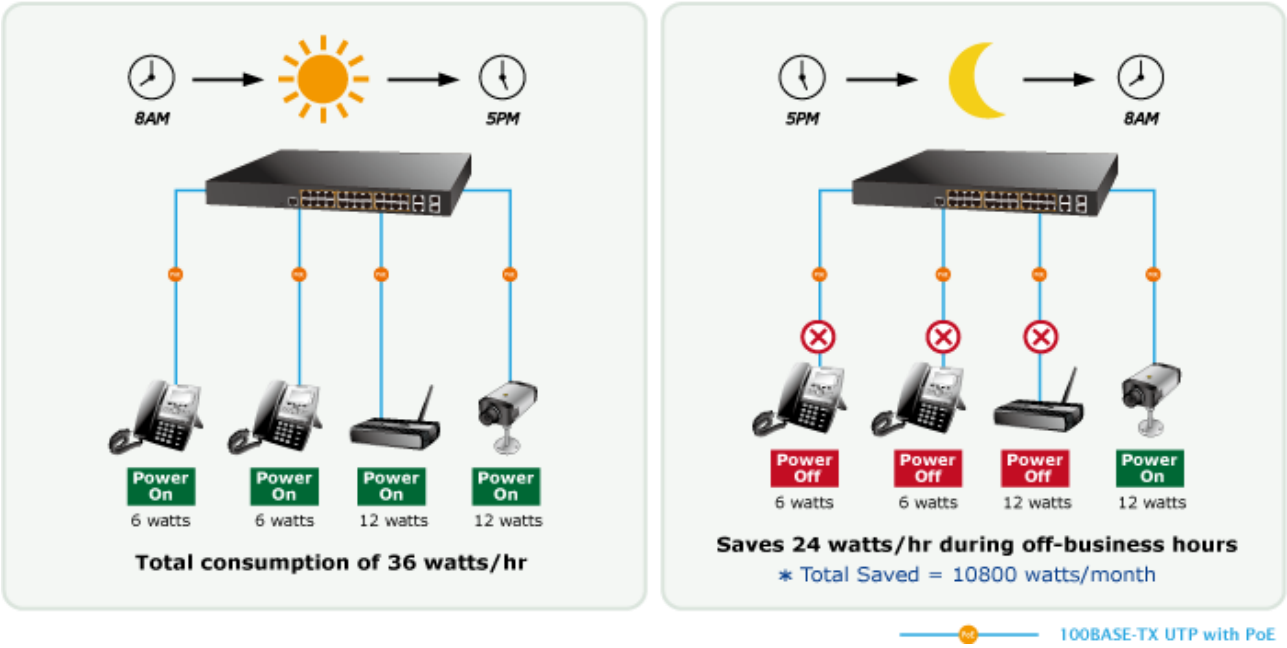
SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.3.4 PoE Schedule

This page allows the user to define PoE schedule and schedule power recycle.

PoE Schedule

Besides being used as an IP Surveillance, the Managed PoE+ Switch is certainly applicable to constructing any PoE network including VoIP and Wireless LAN. Under the trend of energy saving worldwide and contributing to the environmental protection on the Earth, the Managed PoE switch can effectively control the power supply besides its capability of giving high watts power.



The "**PoE schedule**" function helps you to enable or disable PoE power feeding for each PoE port during specified time intervals and it is a powerful function to help SMBs or Enterprises save power and budget. The screen in Figure 4-3-6 appears.

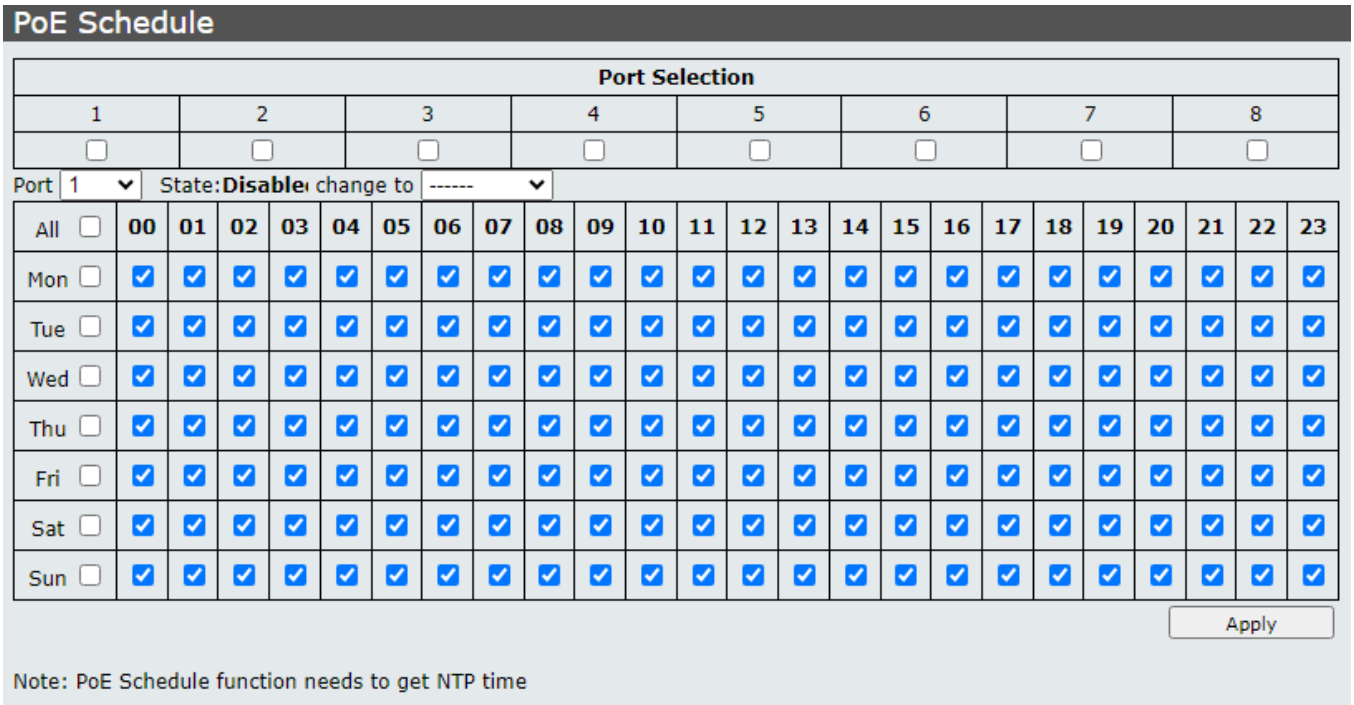


Figure 4-3-6: PoE Schedule Configuration Page Screenshot

SEC.RU | Короткий путь к информации
Скачано с sec.ru

The page includes the following fields:

Object	Description
• **Port Selection**	Select specific PoE port for further configuration.
• **Port**	List all PoE Port for configure PoE schedule function.
• **State: xxxxx change to**	This column allows user to configure the PoE Port Start Up interval time. Delay time range is from 1 seconds to 300 seconds.
• **All**	Select all optios on this page.
• **Mon-Sun**	Provide Mon/Tue/Wed/Thu/Fri/Sat/Sun options on this page.
• **00-23**	Provide 24 hours options on this page.

Button

Apply: press this button to confirm the changes.

Note

The Managed PoE+ Switch PoE schedule function needs to get NTP time.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.4 Basic Configuration

On the Access Basic configuration web page, you can view Port management function informations of the Managed PoE+ Switch as the screen in Figure 4-4-1 appears.

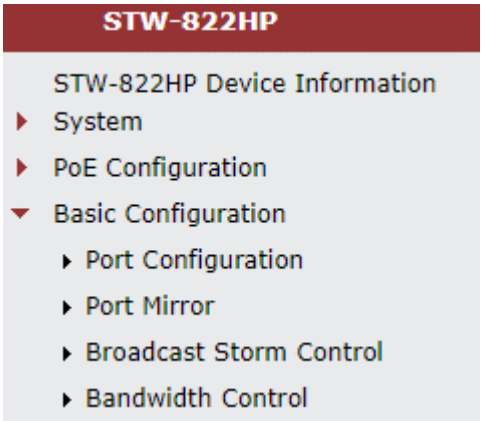


Figure 4-4-1: Managed PoE+ Switch Basic Configuration Web Page

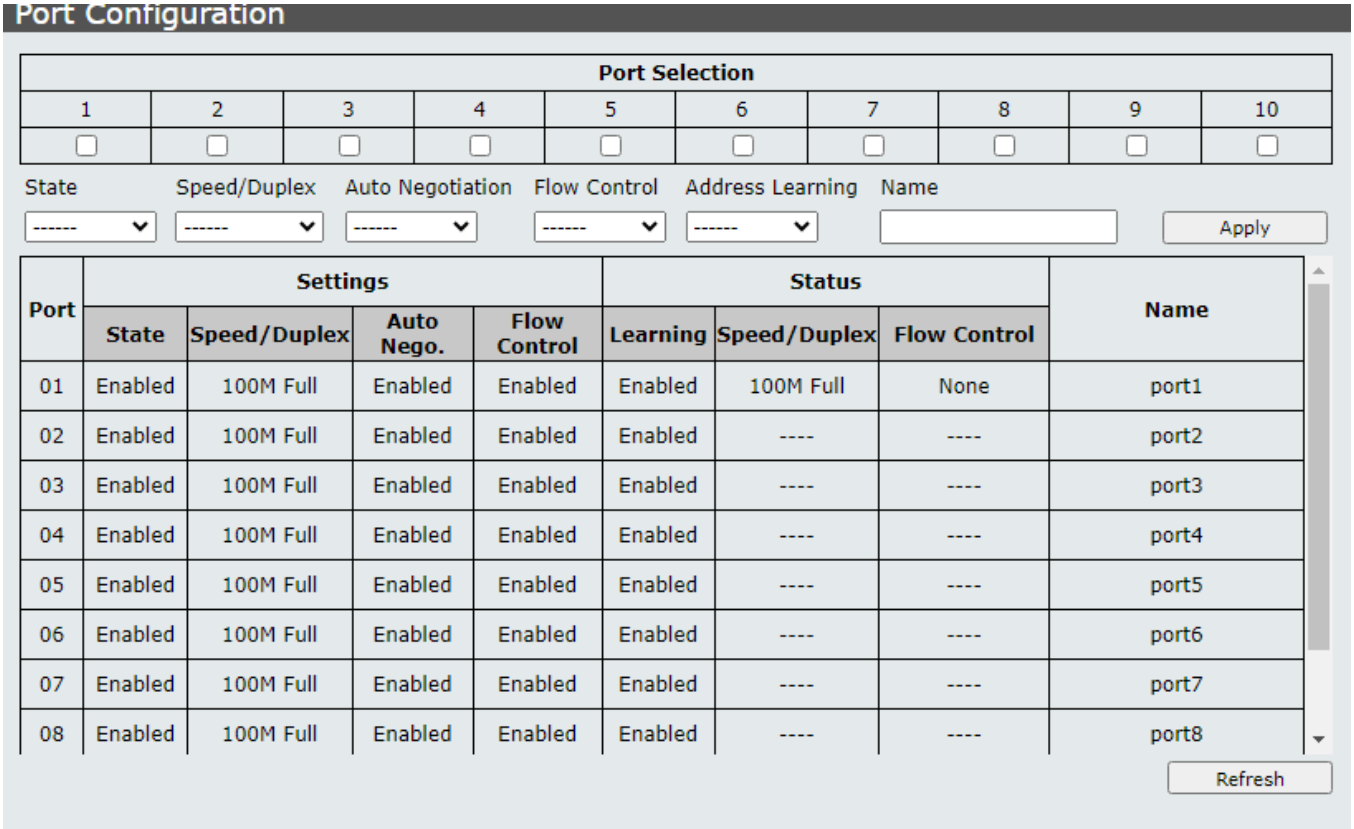
Basic Configuration	
Item	**Description**
Port Configuration	Display and configure per Port configuration settings.
Port Mirror	Display and configure Port Mirror function.
Broadcast Storm Control	Display and configure Broadcast Storm Control function.
Bandwidth Control	Display and configure Bandwidth Control function.

Table 4-4-1: Descriptions of Basic Configuration

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.4.1 Port Configuration

This page displays current port configurations and each port can also be configured here as the Port configuration screen in Figure 4-4-2 appears.



Port	Settings				Status			Name
	State	Speed/Duplex	Auto Nego.	Flow Control	Learning	Speed/Duplex	Flow Control	
01	Enabled	100M Full	Enabled	Enabled	Enabled	100M Full	None	port1
02	Enabled	100M Full	Enabled	Enabled	Enabled	----	----	port2
03	Enabled	100M Full	Enabled	Enabled	Enabled	----	----	port3
04	Enabled	100M Full	Enabled	Enabled	Enabled	----	----	port4
05	Enabled	100M Full	Enabled	Enabled	Enabled	----	----	port5
06	Enabled	100M Full	Enabled	Enabled	Enabled	----	----	port6
07	Enabled	100M Full	Enabled	Enabled	Enabled	----	----	port7
08	Enabled	100M Full	Enabled	Enabled	Enabled	----	----	port8

Figure 4-4-2 : Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Selection**	Select specific port for further configuration.
• **State**	Enable or disable specific Port function.
• **Speed/Duplex**	Change specific Port speed duplex and the available optios are shown below: Top Speed/10M Half/10M Full/100M Half/100M Full/1000M Full.
• **Auto Negotiation**	Enable or disable auto negotiation function on specific Port.
• **Flow Control**	Enable or disable flow control function on specific Port.
• **Address Learning**	Enable or disable address learning function on specific Port.
• **Name**	Configure the Managed PoE+ Switch per port description information on this page; the maximum length is 20 characters.
• **Port**	Display per port list.
Setting	
• **State**	Display per port current operation setting mode.
• **Speed/Duplex**	Display per port current speed/duplex setting mode.
• **Auto Nego.**	Display per port current auto negotiation setting mode.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

• **Flow Control**	Display per port current flow control setting mode.
Status	
• **Learning**	Display per port current learning setting mode.
• **Speed/Duplex**	Display per port current speed/duplex mode.
• **Flow Control**	Display per port current flow control mode.
• **Name**	Display per port current description information.

Buttons

Apply **: press this button to confirm the changes.**

Refresh **: press this button to refresh information.**

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.4.2 Port Mirroring

On this page, port mirroring provides monitoring network traffic that forwards a copy of each incoming or outgoing packet from one port of a Managed PoE+ Switch to another port where the packet can be studied. It enables the manager to keep close track of switch performance and alter it if necessary.

- To debug 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 Managed PoE+ Switch can unobtrusively mirror traffic from any port to a monitor port. You can then attach a protocol analyzer or RMON probe to this port to perform traffic analysis and verify connection integrity.

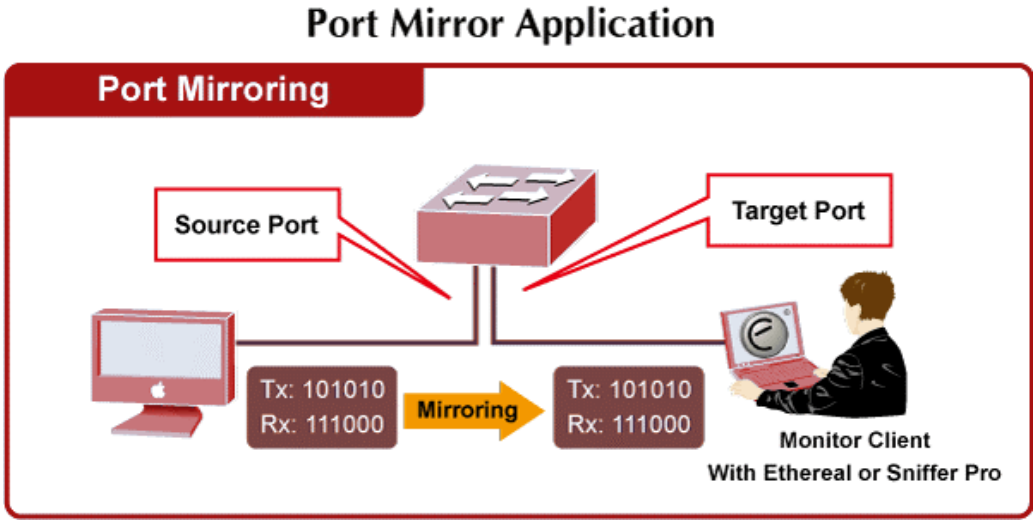


Figure 4-4-3: Port Mirroring Application

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 Mirroring Configuration

The Port Mirroring screen in Figure 4-4-4 is shown below.

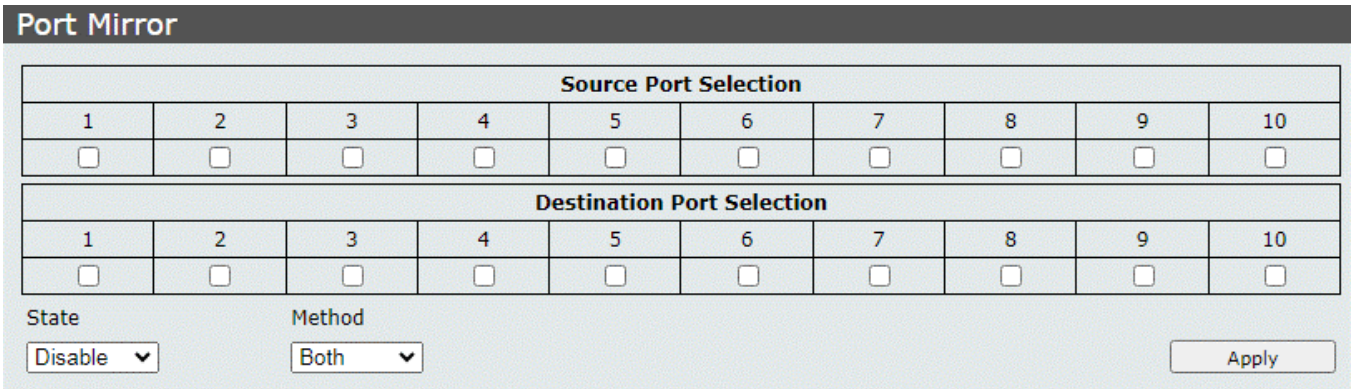


Figure 4-4-4: Port Mirroring Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Source Port Selection**	Select specific port for monitoring incoming and outgoing flow from the port.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

• **Destination Port Selection**	Select the specific port for copy flow data from source ports and then forward to message analyzer to analyze message, and finally analysis of message forward to destination port.
• **State**	Enable or disable the port mirroring function.
• **Method**	Select method for monitoring of incoming, outgoing or both methods, and the available options are shown below: Egress/Ingress/Both.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.4.3 Broadcast Storm Control

Storm control for the switch is configured on this page. There are a broadcast storm rate control, multicast storm rate control, and unicast storm rate control. These only affect flooded frames, i.e. frames with a (VLAN ID, DMAC) pair not present on the MAC Address table.

The configuration indicates the permitted packet rate for unicast, multicast or broadcast traffic across the switch as the Broadcast Storm Control configuration screen in Figure 4-4-5 appears.

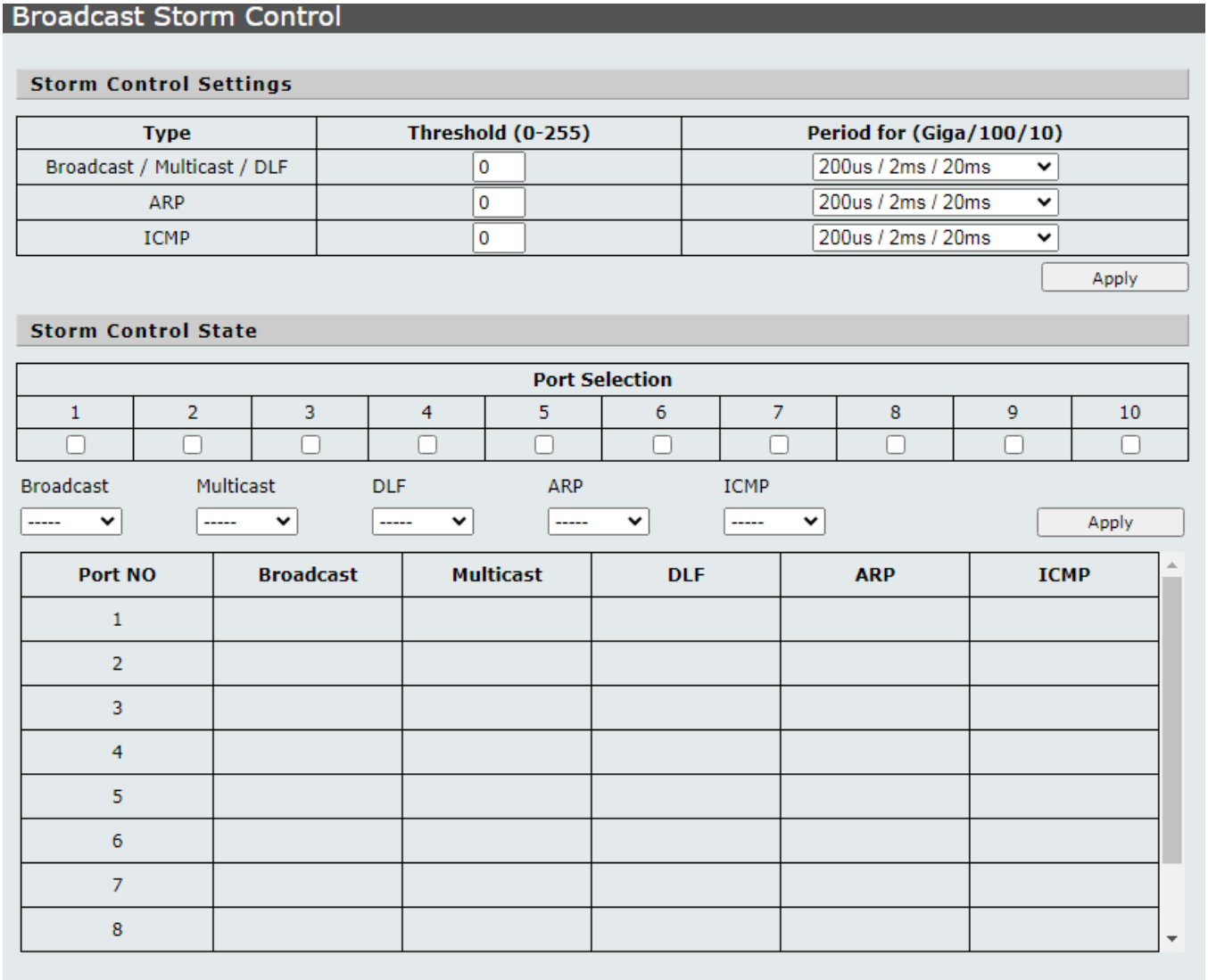


Figure 4-4-5: Broadcast Storm Control Configuration Page Screenshot

The page includes the following fields:

Object	Description
Storm Control Settings	
• **Type**	Types of storm control: Broadcast: Broadcast packet. Multicast: Multicast packet, 40th bit in the destination MAC is 1 DLF: The destination address in the MAC table does not exist ARP: ARP packet. ICMP: ICMP packet.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

• **Threshold (0-255)**	During the receive period, the port receives an upper limit for the specified packet type
• **Period for (Giga/100/10)**	Set reception period and the available options are shown below: 200us/2ms/20ms 1ms/10ms/100ms 10ms/10ms/10ms 100ms/100ms/100ms
Storm Control State	
• **Port Selection**	Select specific port for further configuration.
• **Broadcast**	Enable or disable the broadcast storm control function.
• **Multicast**	Enable or disable the multicast storm control function.
• **DLF**	Enable or disable the unknown destination MAC packets control function.
• **ARP**	Enable or disable the ARP packets control function.
• **ICMP**	Enable or disable the ICMP packets control function.
• **Port No.**	Display per port list.
• **Broadcast**	Display per port broadcast storm control setting.
• **Multicast**	Display per port multicast storm control setting.
• **DLF**	Display per port unknown destination MAC packets control setting.
• **ARP**	Display per port ARP packets control setting.
• **ICMP**	Display per port ICMP packets control setting.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.4.4 Bandwidth Control

This page allows you to configure the incoming and outgoing bandwidth control settings for all switch ports as the bandwidth control screen in Figure 4-4-6 appears.

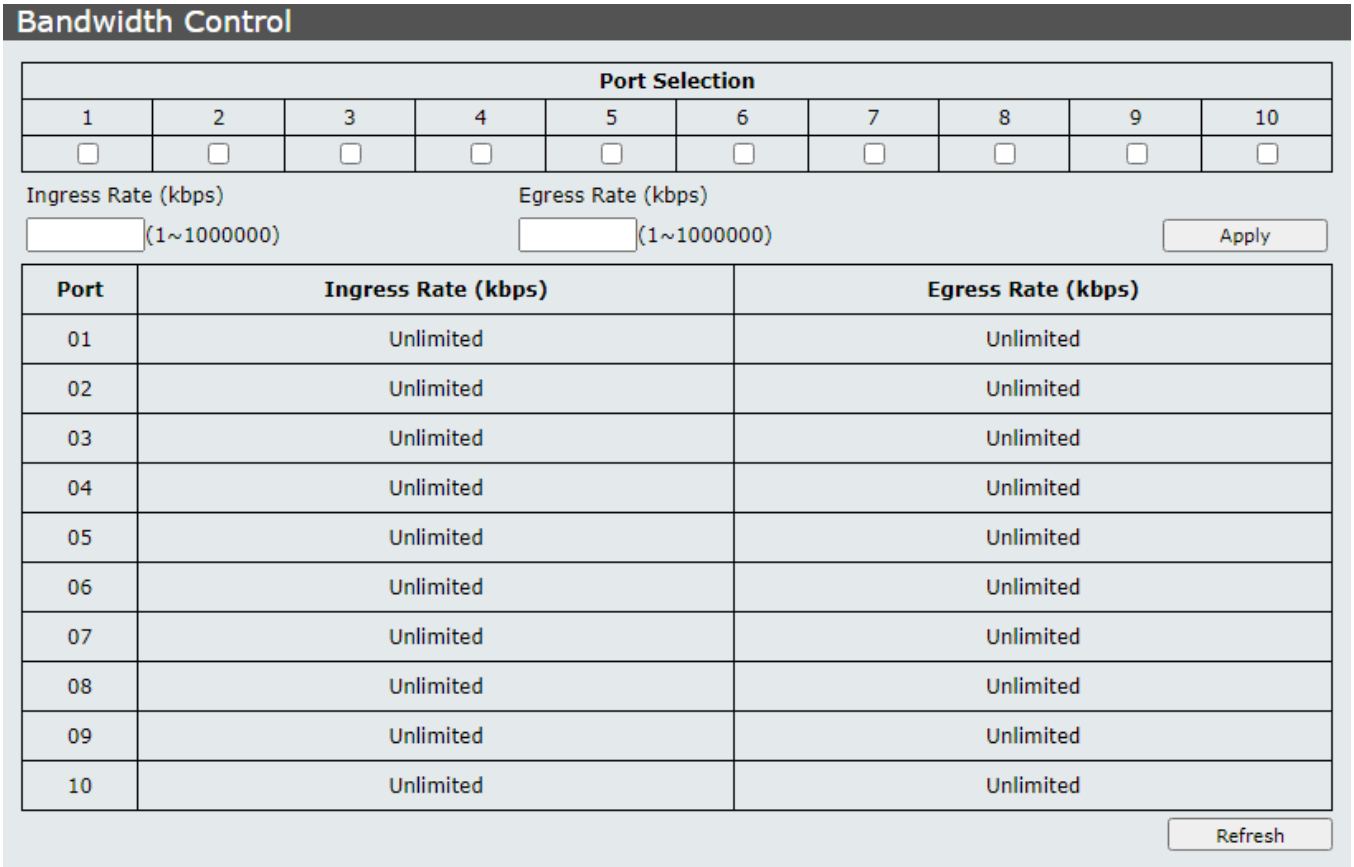


Figure 4-4-6: Bandwidth Control Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Selection**	Select specific port for incoming and outgoing bandwidth control settings.
• **Ingress Rate (kbps)** • **(1-1000000)**	Controls the rate (unit: kbps) for the ingress rate. This value is restricted to 1-1000000. The default value is **Unlimited**.
• **Egress Rate (kbps)** • **(1-1000000)**	Controls the rate (unit: kbps) for the egress rate. This value is restricted to 1-1000000. The default value is **Unlimited**.
• **Port**	Display per port list.
• **Ingress Rate (kbps)**	Display per port ingress rate setting value.
• **Egress Rate (kbps)**	Display per port egress rate setting value.

Buttons

Apply: press this button to confirm the changes.

Refresh: press this button to refresh information.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.5 VLAN Configuration

4.5.1 VLAN Overview

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLAN also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

Note

1. No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLAN without a network device performing a routing function between the VLANs.
2. The Managed PoE+ Switch supports IEEE 802.1Q VLAN. The port untagging function can be used to remove the 802.1 tag from packet headers to maintain compatibility with devices that are tag-unaware.

Note

The Managed PoE+ Switch 's default is to assign all ports to a single 802.1Q VLAN named DEFAULT_VLAN. As new VLAN is created, the member ports assigned to the new VLAN will be removed from the DEFAULT_ VLAN port member list. The DEFAULT_VLAN has a VID = 1.

On the Access VLAN configuration web page, you can view VLAN management function information of the Managed PoE+ Switch as the screen in Figure 4-5-1 appears.

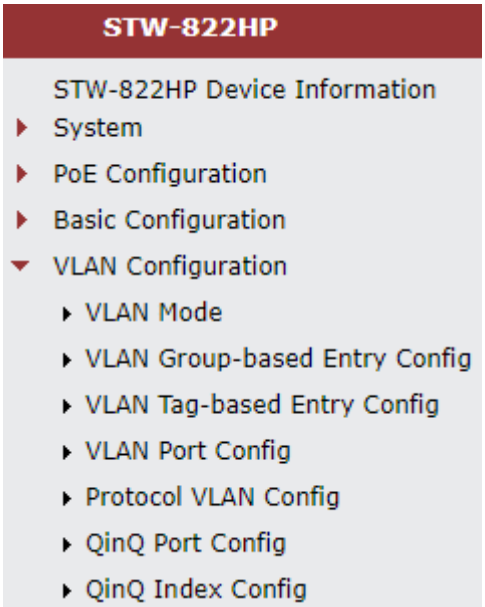


Figure 4-5-1: Managed PoE+ Switch VLAN Configuration Web Page

SEC.RU | Короткий путь к информации
Скачано с sec.ru

VLAN Configuration	
Item	**Description**
VLAN Mode	Configure VLAN Mode configuration settings on this web page.
VLAN Group-based Entry Config	Display and configure VLAN Group-based Entry Config function on this web page.
VLAN Tag-based Entry Config	Display and configure VLAN Tag-based Entry Config function on this web page.
VLAN Port Config	Display and configure VLAN Port Config function on this web page.
Ptotocol VLAN Config	Display and configure Protocol VLAN Config function on this web page.
QinQ Port Config	Display and configure QinQ Port Config function on this web page.
QinQ Index Config	Display and configure QinQ Index Config function on this web page.

Table 4-5-1: Descriptions of VLAN Configuration

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.5.2 IEEE 802.1Q VLAN

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. This Managed PoE+ Switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing you to move devices to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow you to make network changes without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

This Managed PoE+ Switch supports the following VLAN features:

- Up to 26 VLANs based on the IEEE 802.1Q standard
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between VLAN-aware and VLAN-unaware devices
- Priority tagging

IEEE 802.1Q Standard

IEEE 802.1Q (tagged) VLAN are implemented on the Switch. 802.1Q VLAN require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLAN allows a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

VLAN can also provide a level of security to your network. IEEE 802.1Q VLAN will only deliver packets between stations that are members of the VLAN. Any port can be configured as either **tagging** or **untagging**.:

- The untagging feature of IEEE 802.1Q VLAN allows VLAN to work with legacy switches that don't recognize VLAN tags in packet headers.
- The tagging feature allows VLAN to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

Some relevant terms:

- **Tagging** - The act of putting 802.1Q VLAN information into the header of a packet.
- **Untagging** - The act of stripping 802.1Q VLAN information out of the packet header.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

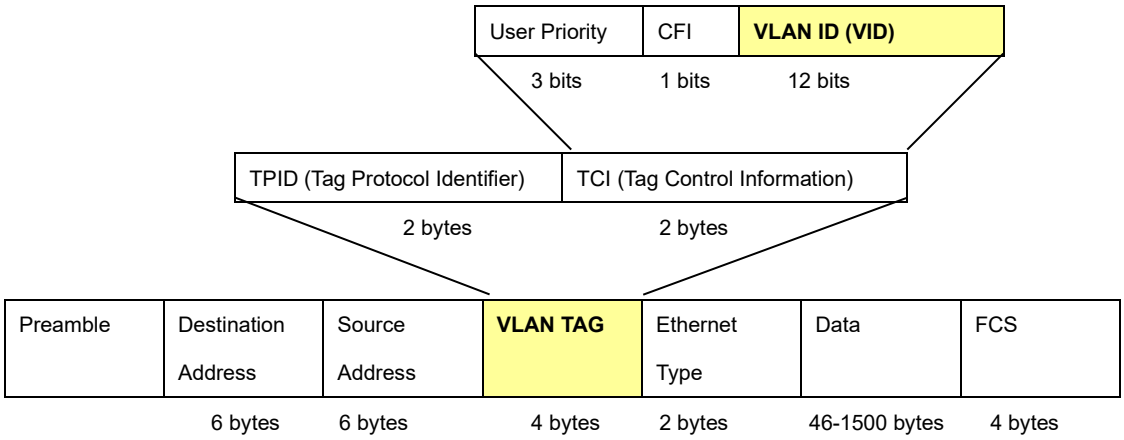
SEC.RU | Короткий путь к информации
Скачано с sec.ru

802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of **0x8100** in the Ether Type field. When a packet's Ether Type field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of **VLAN ID (VID)**. The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLAN can be identified.

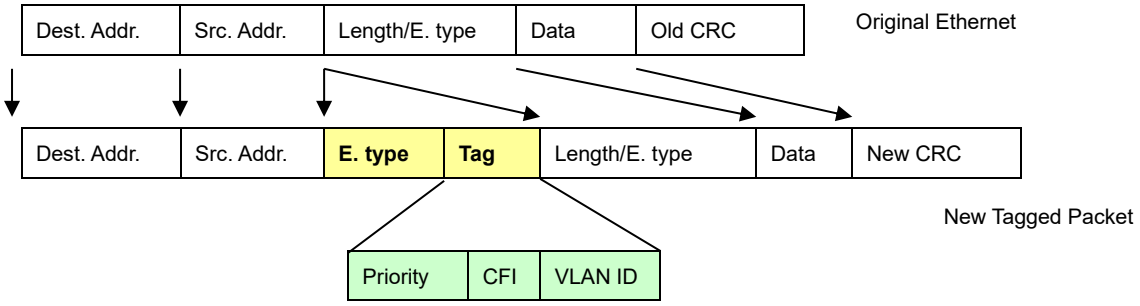
The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

802.1Q Tag



The Ether Type and VLAN ID are inserted after the MAC source address, but before the original Ether Type/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

Adding an IEEE802.1Q Tag



SEC.RU | Короткий путь к информации
Скачано с sec.ru

Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLAN to span network devices (and indeed, the entire network – if all network devices are 802.1Q compliant).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the switch. If no VLAN are defined on the switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLAN are concerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVID within the switch to VID on the network. The switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VID are different the switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VID as the switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted – should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Default VLANs

The Switch initially configures one VLAN, VID = 1, called **"Default."** The factory default setting assigns all ports on the Switch to the **"Default"**. As new VLAN are configured in Port-based mode, their respective member ports are removed from the "default."

Assigning Ports to VLANs

Before enabling VLANs for the switch, you must first assign each port to the VLAN group(s) in which it will participate. By default all ports are assigned to VLAN 1 as untagged ports. Add a port as a tagged port if you want it to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-aware network devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if you want a port on this switch to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then you should add this port to the VLAN as an untagged port.

Note	VLAN-tagged frames can pass through VLAN-aware or VLAN-unaware network interconnection devices, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

VLAN Classification

When the switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Port Overlapping

Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if you implement VLANs which do not overlap, but still need to communicate, you can connect them by enabled routing on this switch.

Untagged VLANs

Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.5.3 VLAN Mode

The VLAN Mode Page provide VLAN Mode configuration supported by the Managed PoE+ Switch as the VLAN Mode screen in Figure 4-5-2 appears.

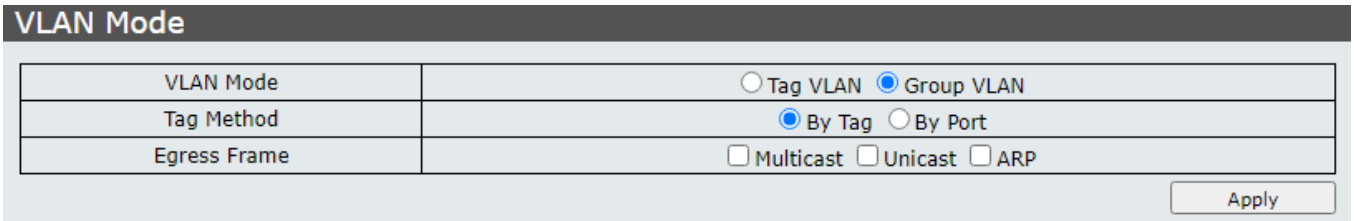
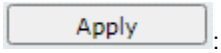


Figure 4-5-2: VLAN Mode Configuration Page Screenshot

The Page includes the following fields:

Object	Description
• **VLAN Mode**	Display the current VLAN mode used by this Managed PoE+ Switch. ■ **Tag VLAN** determines the VID of each entry and those ports are VLAN members of which VLAN based on the settings of the Tag-based Entry. ■ **Group VLAN** determines which port in each group is its VLAN member based on the settings of the Group-based Entry.
• **Tag Method**	This option only available in Tag VLAN mode. ■ **By Tag-** whether packet sent out add/remove tag is judged on the basis of the value set by the port in the Tag-based entry. ■ **By Port-**whether the port sent out the packet add/remove tag is judged by the tagging value set by the port in the VLAN port config web page
• **Egress Frame**	It could connect the selected packet type via engress rule to transport between different VLAN groups. The available options are shown below: ■ **Multicast** ■ **Unicast** ■ **ARP**

Button



: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.5.4 VLAN Group-based Entry Config

■ **Adding Static Members to VLANs (VLAN Index)**

Use the VLAN Group Member Port to configure port members for the selected VLAN index. The VLAN Group-based Entry Config configuration can be monitored and modified here. Up to 26 VLANs are supported. This page allows for adding and deleting VLANs as well as adding and deleting port members of each VLAN as the VLAN Group-based Entry Config screen in Figure 4-5-3 appears.

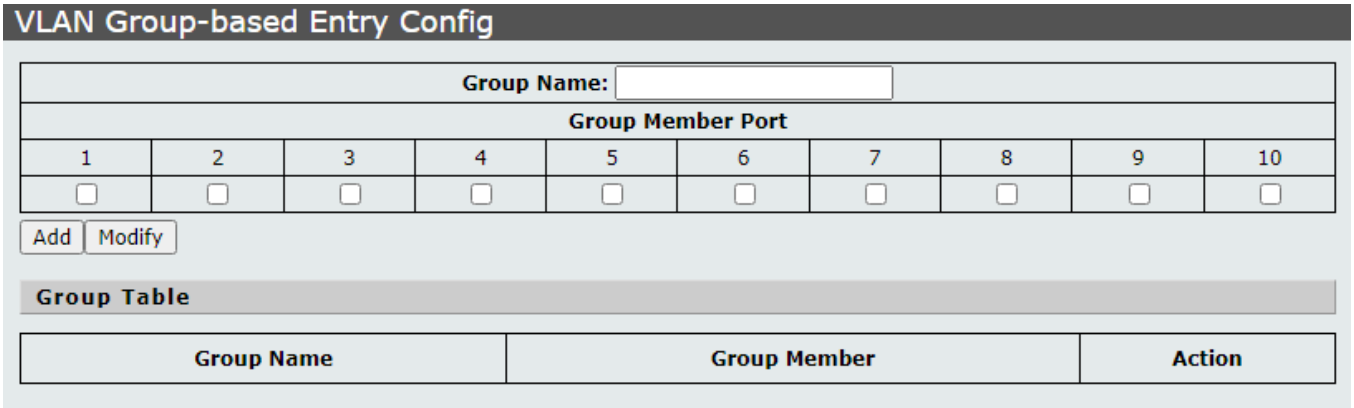


Figure 4-5-3: VLAN Group-based Entry Config Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Group Name**	Configure the Managed PoE+ Switch per VLAN group name information on this web page; the maximum length is 20 characters.
• **Group Member Port**	Assign specific port to per VLAN group. Add: press this button to create a new specific VLAN group. Modify: press this button to modify a specific VLAN group.
Group Table	
• **Group Name**	Display the current group name of VLAN group.
• **Group Member Port**	Display the current group member port number of VLAN group.
• **Action**	Edit: press this button to edit specific VLAN group. Delete: press this button to delete specific VLAN group.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Buttons

Add: press this button to create a new specific VLAN group.

Modify: press this button to modify a specific VLAN group.

Edit: press this button to edit specific VLAN group.

Delete: press this button to delete specific VLAN group.

4.5.5 VLAN Tag-based Entry Config

Use the VLAN Tag-based entry config to configure port members function for the selected VLAN index. The VLAN Tag-based Entry config configuration can be monitored and modified here. Up to 26 VLANs are supported. This page allows for adding and deleting VLANs as well as configure port members function of each VLAN as the VLAN Tag-based Entry Config screen in Figure 4-5-4 appears.

VLAN Tag-based Entry Config

Add

Name	State	VID	Don't care	Add Tag	Remove Tag	Forbidden	Priority	GVRP Forward	Action	
Default	Static	1	1-10	0	0	0	0	Deny	Edit	Delete
Protocol_VLAN1	Static	4081	1-10	0	0	0	0	Deny	Edit	Delete
Protocol_VLAN2	Static	4082	1-10	0	0	0	0	Deny	Edit	Delete
Protocol_VLAN3	Static	4083	1-10	0	0	0	0	Deny	Edit	Delete
Protocol_VLAN4	Static	4084	1-10	0	0	0	0	Deny	Edit	Delete
Voice-VLAN	Static	4080	0	0	0	0	0	Deny	Edit	Delete

Figure 4-5-4: VLAN Tag-based Entry Config Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Name**	Display the name of specific VLAN group.
• **Static**	Display the state of specific VLAN group.
• **VID**	Display the VLAN ID of specific VLAN group.
• **Don't care**	Display the per port Don't care information of specific VLAN group.
• **Add Tag**	Display the per port Add Tag state of specific VLAN group.
• **Remove Tag**	Display the per port Remove Tag state of specific VLAN group.
• **Forbidden**	Display the per port Forbidden state of specific VLAN group.
• **Priority**	Display the Priority state of specific VLAN group.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

• **GVRP Forward**	Display the GVRP Forward state of specific VLAN group.
• **Action**	Edit: press this button to edit specific VLAN group. Delete: press this button to delete specific VLAN group.

Buttons

Add: press this button to create a new specific VLAN group.

Edit: press this button to edit specific VLAN group.

Delete: press this button to delete specific VLAN group.

Press the Edit button to edit per member port state and the screen in Figure 4-5-5 appears.

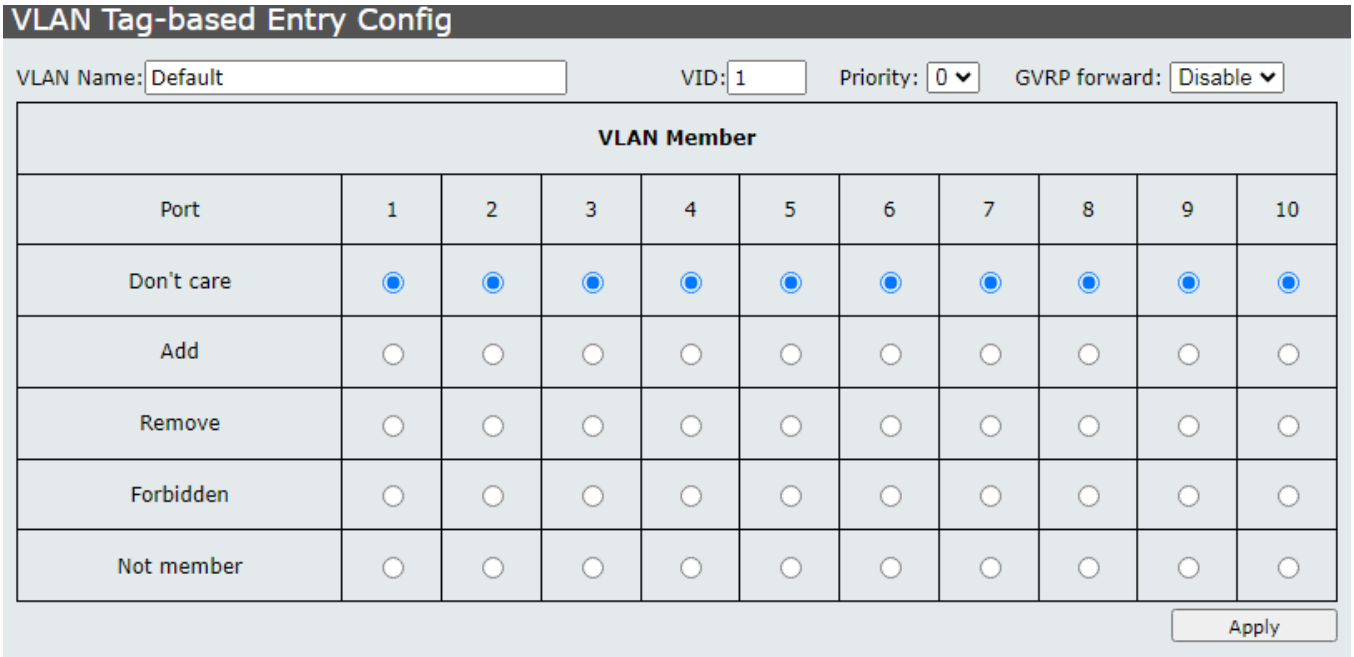


Figure 4-5-5: Edit VLAN Tag-based Entry Config Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **VLAN Name**	Display and configure the name of specific VLAN group; the maximum length is 20 characters.
• **VID**	Display and configure the VLAN ID of specific VLAN group.
• **Priority**	Display and configure the Priority value of specific VLAN group.
• **GVRP Forward**	Display and configure the GVRP Forward mode
• **Port**	Display per port list of Managed PoE+ Switch.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

• **Don't care**	As a VLAN member of specific VLAN group without any action.
• **Add**	As a VLAN member, add the Tag action to the packet sent out by this port.
• **Remove**	As a VLAN member, remove the Tag action to the packet sent out by this port.
• **Forbidden**	Configure that this port cannot register this Tag VLAN dynamically through GVRP.
• **Not Member**	Not a member of the VLAN.

Button

Apply: press this button to confirm the changes.

Note

GVRP (GARP VLAN Registration Protocol) maintains VLAN dynamic registration information for GVRP devices based on the working mechanism of GARP to maintain VLAN dynamic registration information that supports GVRP devices.

And propagate this information to other devices in order to achieve agreement on VLAN information for all devices supporting GVRP in the same LAN.

The VLAN registration information propagated by GVRP includes both local manual static registration information and dynamic registration information from other switches.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.5.6 VLAN Port Config

This page is used for configuring the Managed PoE+ Switch port VLAN. The VLAN per port configuration page contains fields for managing ports that are part of a VLAN. The port default VLAN ID (PVID) is configured on the VLAN port configuration page. All untagged packets arriving to the device are tagged by the ports PVID.

Understanding Nomenclature of the Switch

IEEE 802.1Q Tagged and Untagged

Every port on an 802.1Q compliant switch can be configured as tagged or untagged.

- **Tagged:** Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into those ports. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet-forwarding decisions.
- **Untagged:** Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Frame Income / Frame Leave	Income Frame is **tagged**	Income Frame is **untagged**
Leave port is tagged	Frame remains tagged	Tag is inserted
Leave port is untagged	Tag is removed	Frame remains untagged

Table 4-5-2: Ingress / Egress Port with VLAN VID Tag / Untag table

SEC.RU | Короткий путь к информации
Скачано с sec.ru

The VLAN Port configuration screen in Figure 4-5-6 is shown below.

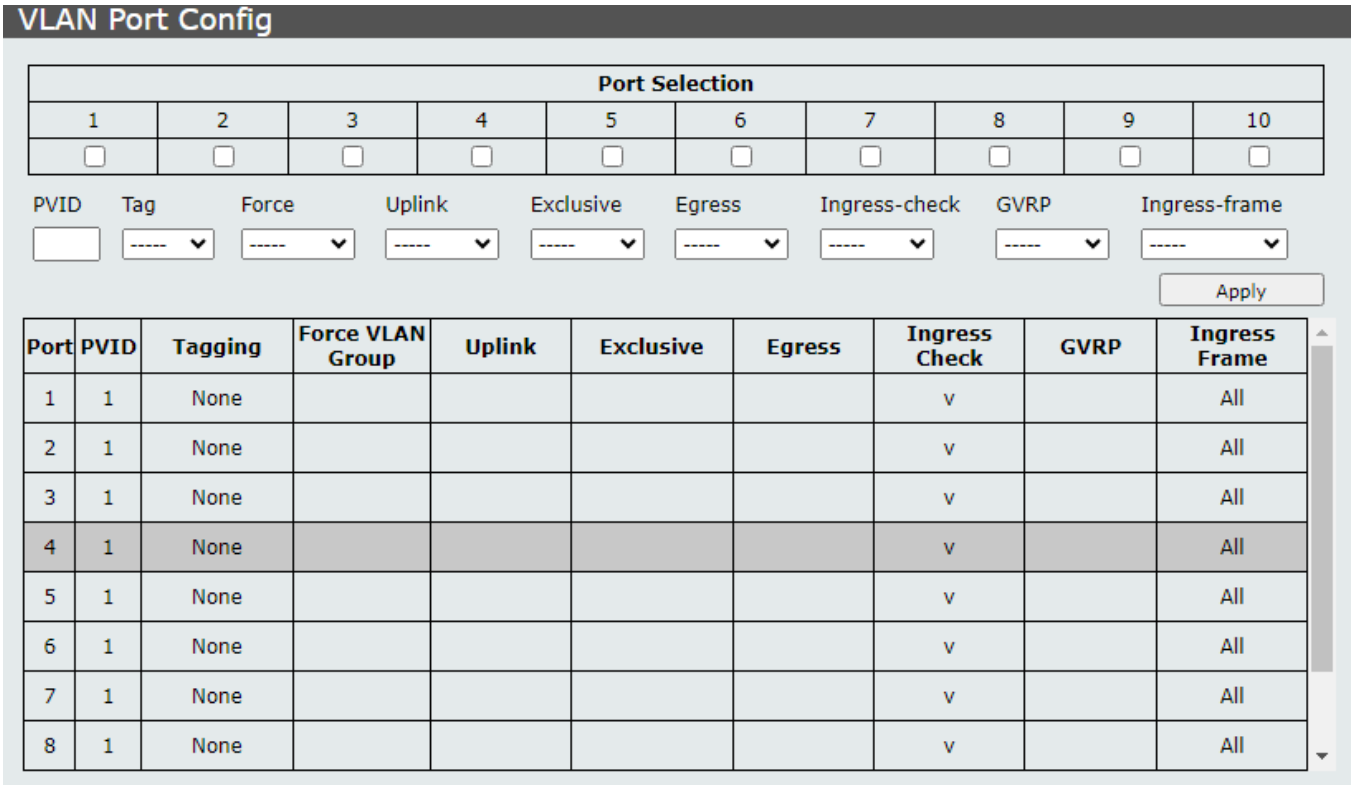


Figure 4-5-6 : VLAN Port Config Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Selection**	Select specific port for VLAN settings.
• **PVID**	Allow assigned PVID for selected port. The range for the PVID is 1-4094. The PVID will be inserted into all untagged frames entering the ingress port. The PVID must as same as the VLAN ID that the port belong to VLAN group, or the untagged traffic will be dropped.
• **Tag**	Set whether VLAN Tag is added or removed from the packet sent out by selected port. The available options are **"Add"**, **"RMV"** and **"None"**.
• **Force**	Whether or not to set priority according to the group VLAN setting for the action.
• **Uplink**	Set up the Uplink port, which automatically sends the packet out of the Uplink Port when the destination Port is not the same as the VLAN.
• **Exclusive**	Enable or disable the exclusive function on specific port, the exclusive port unable to transfer packets.
• **Egress**	Enable or disable the exgress function on specific port, when the destination port of the packet is not in the same VLAN, it can still be transmitted to the destination port via the egress rule.
• **Ingress-Check**	Enable or disable the ingress check function, check whether port is member of this VLAN through VID.
• **GVRP**	Enable or disable the port GVRP function.
• **Ingress-Frame**	Setting allows the specified frame to do the forwarding action. The available options are **"Tag-Frame"** and **"All"**.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

• **Port**	Display per port list.
• **PVID**	Display per port PVID information.
• **Tagging**	Display per port Tagging information.
• **Force VLAN Group**	Display per port Force VLAN Group information.
• **Uplink**	Display per port Uplink information.
• **Exclusive**	Display per port Exclusive information.
• **Egress**	Display per port Egress information.
• **Ingress Check**	Display per port Ingress Check information.
• **GVRP**	Display per port GVRP information.
• **Ingress-Frame**	Display per port Ingress Frame information.

Note

The port must be a member of the same VLAN as the Port VLAN ID.

Button

Apply : press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.5.7 Protocol VLAN Config

This page is used for configuring the Managed PoE+ Switch Protocol VLAN Config as the Protocol VLAN Config screen in Figure 4-5-7 appears.

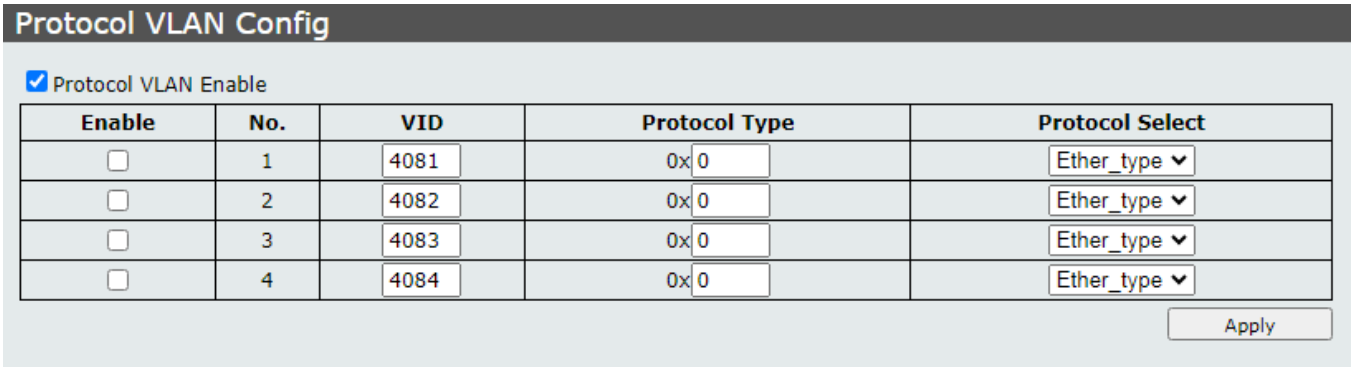


Figure 4-5-7 : Protocol VLAN Config Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Protocol VLAN Enable**	Click to activate the Protocol VLAN settings.
• **Enable**	Select the number of groups to enable.
• **No.**	Display the groups number.
• **VID**	Set the VID value and when the packet conforms to the set protocol on this web page, the VLAN member is queried with VID.
• **Protocol Type**	Set protocol type.
• **Protocol Select**	Select the Protocol and the available options are shown below: **Ether Type:** The set value of the protocol type must be greater than 0x0600 when setting Ether Type. Its format is DA+SA+Protocol type. **LLC:** Its format is DA+SA+Protocol Type. **RFC1042:** Its format is DA+SA+length+AAAA03+000000+Protocol Type.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.5.8 Q-in-Q Port Config

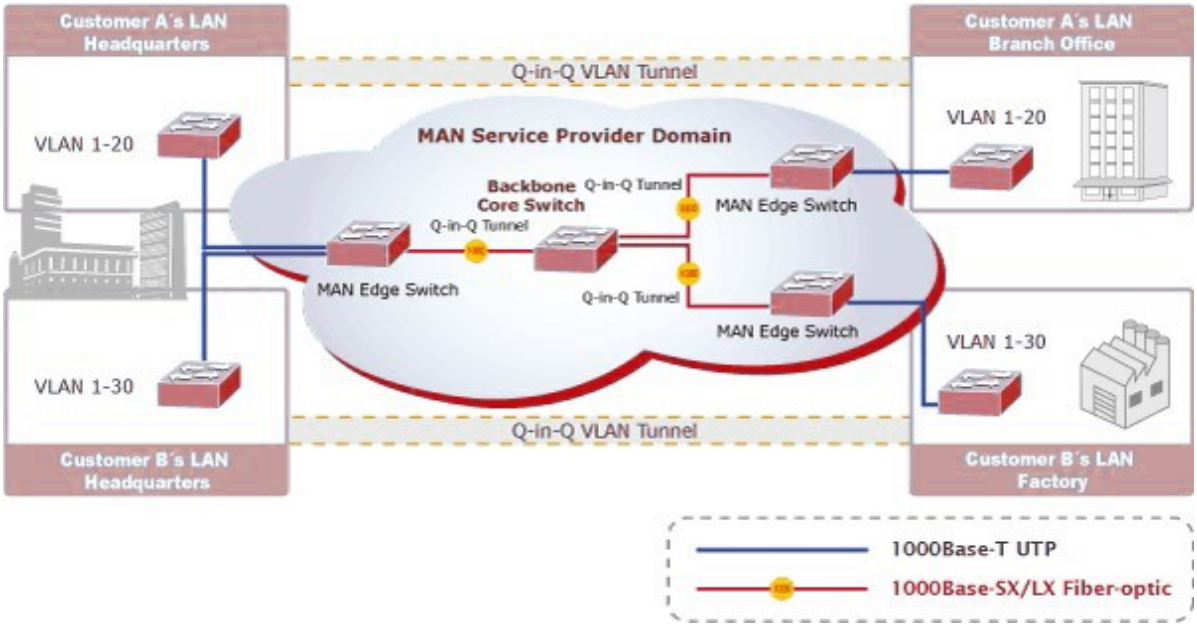
This page is used for configuring the Managed PoE+ Switch Q-in-Q port VLAN function; the Q-in-Q port VLAN function configuration page contains fields for managing ports that are part of Q-in-Q VLAN.

Understanding Nomenclature of the Switch

IEEE 802.1Q Tunneling (Q-in-Q)

IEEE 802.1Q Tunneling (Q-in-Q) is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting **Service Provider VLAN (SPVLAN)** tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.



The Managed PoE+ Switch supports multiple VLAN tags and can therefore be used in MAN applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the **MAN (Metro Access Network)** space. One of the purposes of the provider bridge is to recognize and use VLAN tags so that the VLANs in the MAN space can be used independent of the customers' VLANs. This is accomplished by adding a VLAN tag with a MAN-related VID for frames entering the MAN. When leaving the MAN, the tag is stripped and the original VLAN tag with the customer-related VID is again available.

This provides a tunneling mechanism to connect remote costumer VLANs through a common MAN space without interfering with the VLAN tags. All tags use EtherType **0x8100** or **0x88A8**, where 0x8100 is used for customer tags and 0x88A8 are used for service provider tags.

In cases where a given service VLAN only has two member ports on the switch, the learning can be disabled for the particular VLAN and can therefore rely on flooding as the forwarding mechanism between the two ports. This way, the MAC table

SEC.RU | Короткий путь к информации
Скачано с sec.ru

requirements is reduced.

Q-in-Q Port Configuration

The Q-in-Q Port configuration screen in Figure 4-5-8 is shown below.

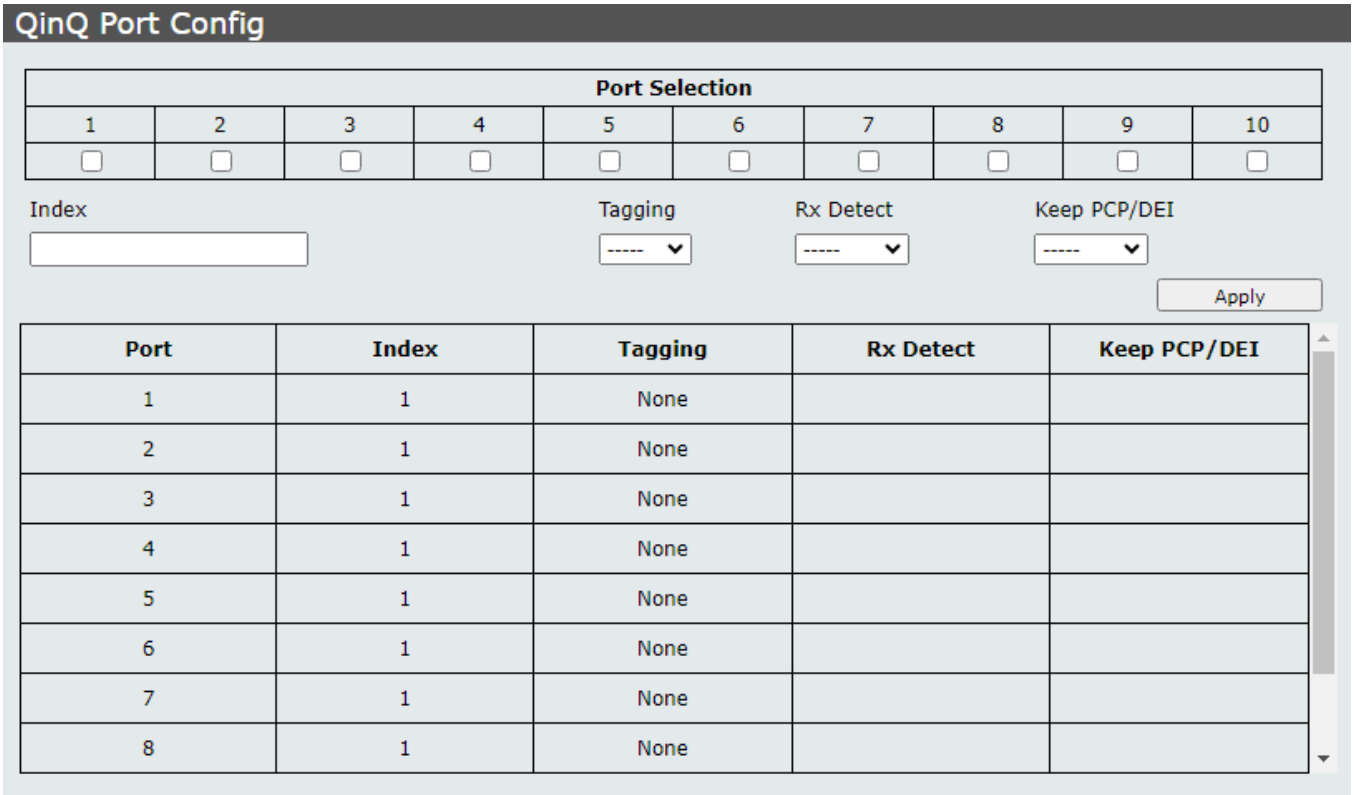


Figure 4-5-8 : Q-in-Q Port Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Selection/Port**	Select specific port for Q-in-Q Port configuration./ List per port numbers.
• **Index**	Choose to use the set of indexes in which the service Tag value is placed in the Q-in-Q Index config web page setting. Also display current Index information.
• **Tagging**	Set whether VLAN Tag is added or removed from the packet sent out by selected port. The available options are **"Add"**, **"RMV"** and **"None"**. **Add:** Do the new service Tag action on the incoming and outgoing packet from this port, if the incoming packet itself has service tag, modify or directly replace the service Tag action depending on whether the RX detect is opened or not. **RMV:** RX detect enable state to remove service Tag. Also display current Tagging information.
• **RX Detect**	Enable or disable the packet that enters the port to do the service Tag check. Also display current RX Detect information.
• **Keep PCP/DEI**	Set whether to retain the original PCP and DEI values when modifying the service Tag entered into the packet. Also display current Keep PCP/DEI information.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.5.9 Q-in-Q Index Config

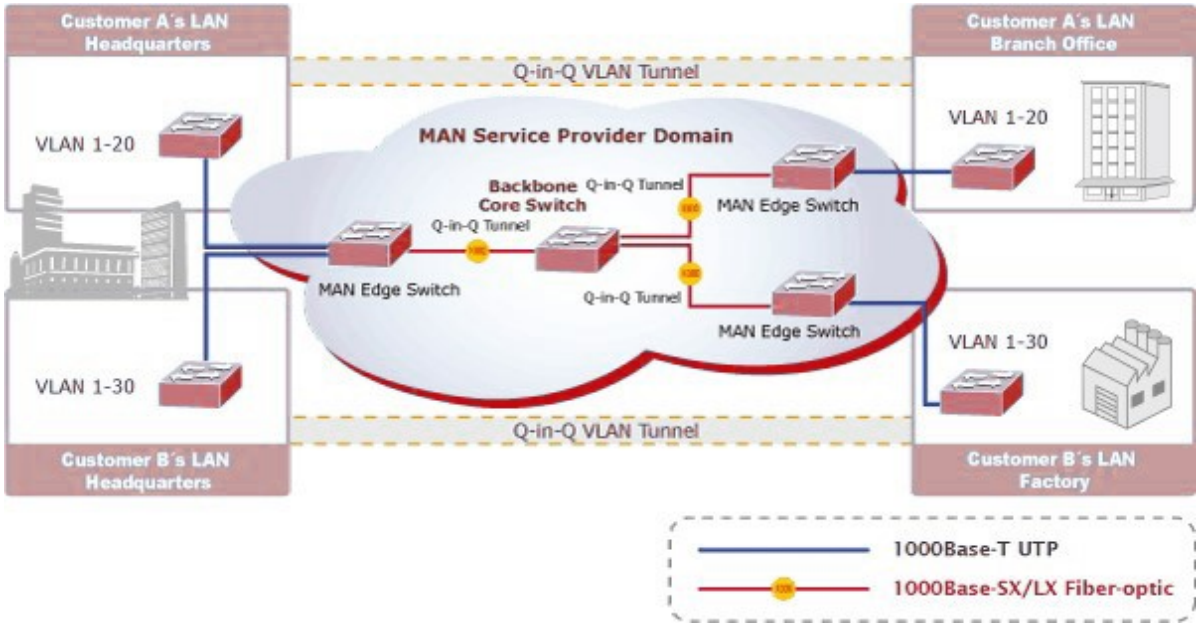
This page is used for configuring the Managed PoE+ Switch Q-in-Q port VLAN function; the Q-in-Q port VLAN function configuration page contains fields for managing ports that are part of Q-in-Q VLAN.

Understanding Nomenclature of the Switch

■ IEEE 802.1Q Tunneling (Q-in-Q)

IEEE 802.1Q Tunneling (Q-in-Q) is designed for service providers carrying traffic for multiple customers across their networks. Q-in-Q tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting **Service Provider VLAN (SPVLAN)** tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.



The Managed PoE+ Switch supports multiple VLAN tags and can therefore be used in MAN applications as a provider bridge, aggregating traffic from numerous independent customer LANs into the **MAN (Metro Access Network)** space. One of the purposes of the provider bridge is to recognize and use VLAN tags so that the VLANs in the MAN space can be used independent of the customers' VLANs. This is accomplished by adding a VLAN tag with a MAN-related VID for frames entering the MAN. When leaving the MAN, the tag is stripped and the original VLAN tag with the customer-related VID is again available. This provides a tunneling mechanism to connect remote costumer VLANs through a common MAN space without interfering with the VLAN tags. All tags use EtherType **0x8100** or **0x88A8**, where 0x8100 is used for customer tags and 0x88A8 are used for service provider tags.

In cases where a given service VLAN only has two member ports on the switch, the learning can be disabled for the particular VLAN and can therefore rely on flooding as the forwarding mechanism between the two ports. This way, the MAC table requirements is reduced.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Q-in-Q Index Configuration

The Q-in-Q Index configuration screen in Figure 4-5-9 appears.

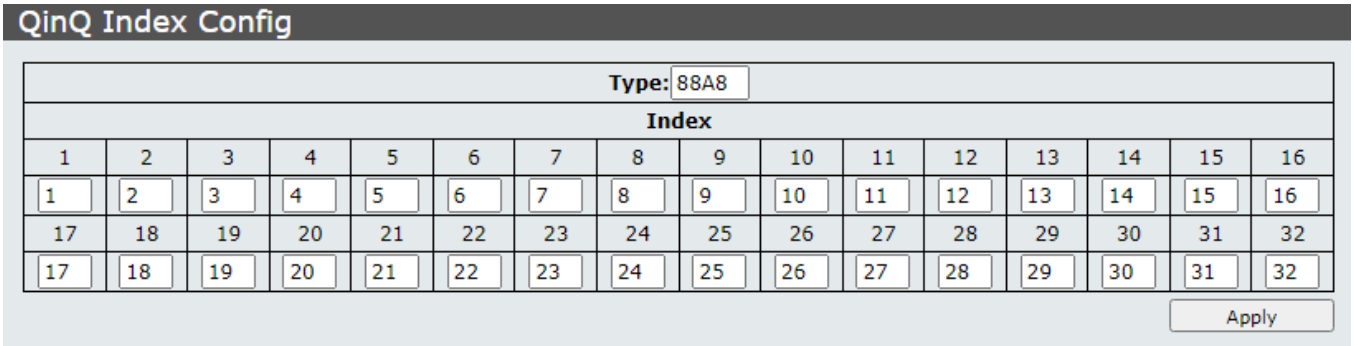


Figure 4-5-9 : Q-in-Q Index Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Type**	Set the type value of service Tag.
• **Index**	Set the service Tag value for each index.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.6 QoS Configuration

4.6.1 Understanding QoS

Quality of Service (QoS) is an advanced traffic prioritization feature that allows you to establish control over network traffic. QoS enables you to assign various grades of network service to different types of traffic, such as multi-media, video, protocol-specific, time critical, and file-backup traffic.

QoS reduces bandwidth limitations, delay, loss, and jitter. It also provides increased reliability for delivery of your data and allows you to prioritize certain applications across your network. You can define exactly how you want the switch to treat selected applications and types of traffic. You can use QoS on your system to:

- Control a wide variety of network traffic by:
- Classifying traffic based on packet attributes.
- Assigning priorities to traffic (for example, to set higher priorities to time-critical or business-critical applications).
- Applying security policy through traffic filtering.
- Provide predictable throughput for multimedia applications such as video conferencing or voice over IP by minimizing delay and jitter.
- Improve performance for specific types of traffic and preserve performance as the amount of traffic grows.
- Reduce the need to constantly add bandwidth to the network.
- Manage network congestion.

QoS Terminology

- **Classifier**—classifies the traffic on the network. Traffic classifications are determined by protocol, application, source, destination, and so on. You can create and modify classifications. The Switch then groups classified traffic in order to schedule them with the appropriate service level.
- **DiffServ Code Point (DSCP)** — is the traffic prioritization bits within an IP header that are encoded by certain applications and/or devices to indicate the level of service required by the packet across a network.
- **Service Level**—defines the priority that will be given to a set of classified traffic. You can create and modify service levels.
- **Policy**—comprises a set of "rules" that are applied to a network so that a network meets the needs of the business. That is, traffic can be prioritized across a network according to its importance to that particular business type.
- **QoS Profile**—consists of multiple sets of rules (classifier plus service level combinations). The QoS profile is assigned to a port(s).
- **Rules**—comprises a service level and a classifier to define how the Switch will treat certain types of traffic. Rules are associated with a QoS Profile (see above).

To implement QoS on your network, you need to carry out the following actions:

1. Define a service level to determine the priority that will be applied to traffic.
2. Apply a classifier to determine how the incoming traffic will be classified and thus treated by the Switch.
3. Create a QoS profile which associates a service level and a classifier.
4. Apply a QoS profile to a port(s).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

On the Access QoS configuration web page, you can view QoS management function informations of the Managed PoE+ Switch as the screen in Figure 4-6-1 appears.

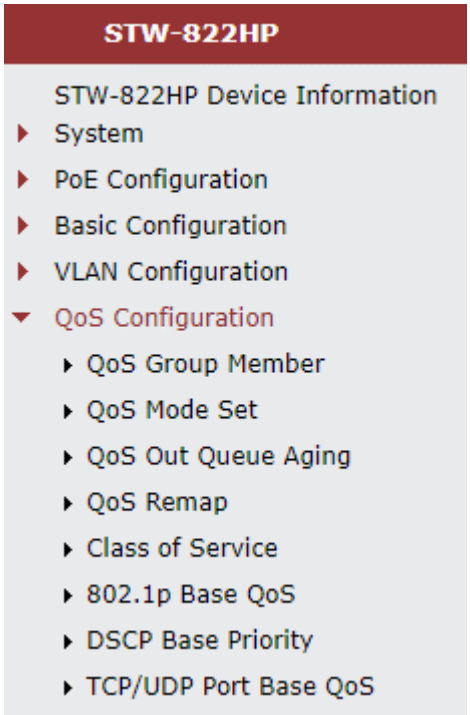


Figure 4-6-1: Managed PoE+ Switch QoS Configuration Web Page

QoS Configuration	
Item	**Description**
QoS Group Member	Configure QoS Group Member configuration settings on this web page.
QoS Mode Set	Configure QoS Mode Set configuration settings on this web page.
QoS Out Queue Aging	Display and configure QoS Out Queue Aging settings on this web page.
QoS Remap	Display and configure QoS Remap settings on this web page.
Class of Service	Display and configure QoS Class of Service settings on this web page.
802.1p-based QoS	Display and configure 802.1p-based QoS settings on this web page.
DSCP-based Priority	Display and configure DSCP-based Priority settings on this web page.
TCP/UDP Port-based QoS	Display and configure TCP/UDP Port-based QoS settings on this web page.

Table 4-6-1: Descriptions of QoS Configuration

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.6.2 QoS Group Member

This page allows you to configure the QoS group member for all switch ports as the QoS group member screen in Figure 4-6-2 appears.

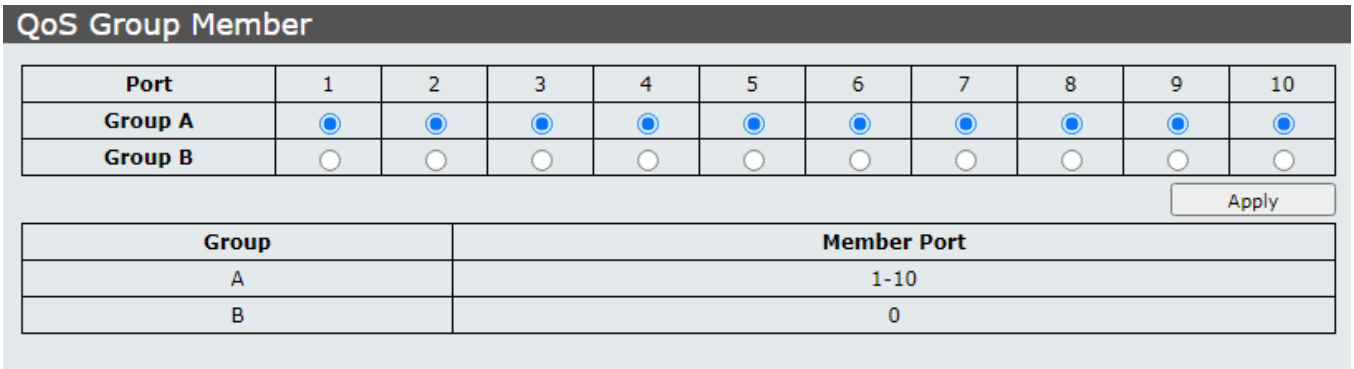


Figure 4-6-2: QoS Group Member Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Display per port list.
• **Group A**	Allow assigning specific port to Group A.
• **Group B**	Allow assigning specific port to Group B.
• **Group**	Display Group A and Group B.
• **Member Port**	Display Member Port setting on Group A and Group B.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.6.3 QoS Mode Set

This page allows you to configure the QoS mode settings for Managed PoE+ Switch as the QoS mode settings screen in Figure 4-6-3 appears.

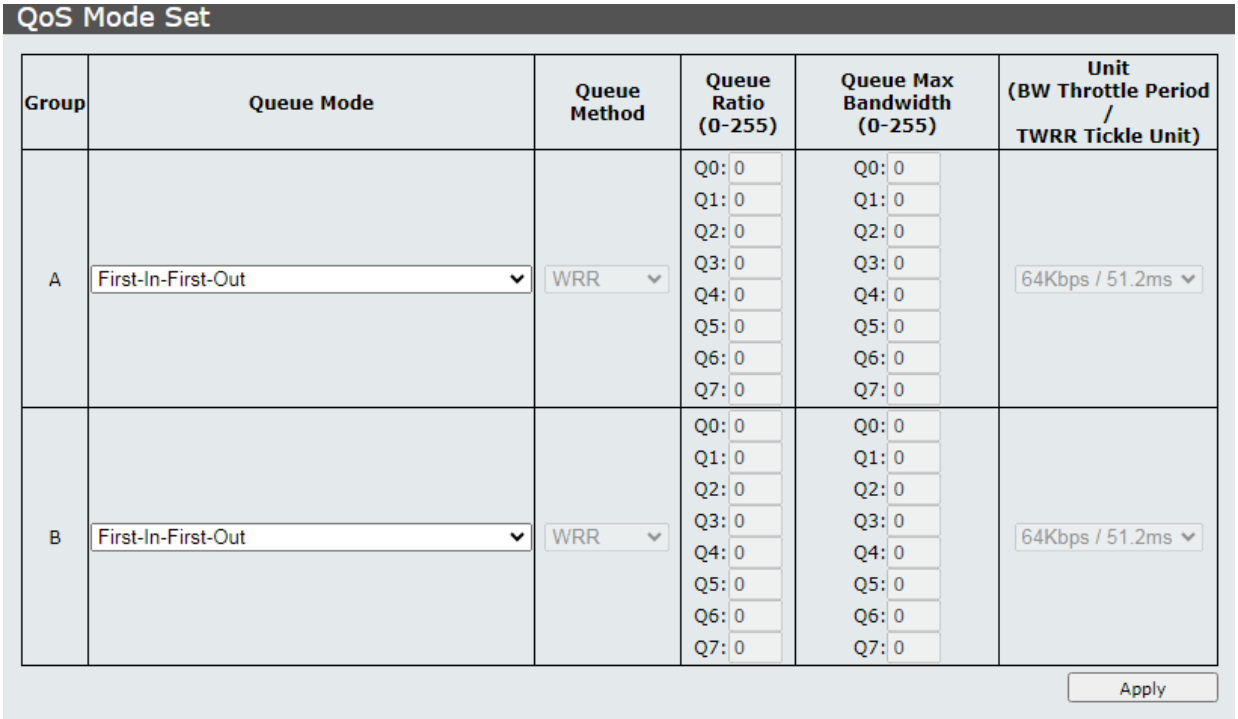


Figure 4-6-3 : QoS Mode Set Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Group**	Display Group A and Group B.
• **Queue Mode**	Select the Queue Mode for QoS and the available options are shown below: **First-In-First-Out** **WRR/WFQ/Bwassure/Bwlimit/TWRR** **SPx1 WRR/WFQ/Bwassure/Bwlimit/TWRRx7** **SPx2 WRR/WFQ/Bwassure/Bwlimit/TWRRx6** **SPx4 WRR/WFQ/Bwassure/Bwlimit/TWRRx4** **SPx8**
• **Queue Method**	Select the Queue Method for QoS and the available options are shown below: **WRR** **WFQ** **Bwassure** **Bwlimit** **TWRR**
• **Queue Ratio (0-255)**	Set Queue Ratio for each mode and the available range is **0-255**.
• **Queue Maximum Bandwidth (0-255)**	Set Queue maximum bandwidth and the available range is **0-255**.
• **Unit (BW Throttle Period/TWRR Tickle Unit)**	Set Queue Ratio Unit for each mode and the available options are shown below: **64Kbps/51.2ms** **1Mbps/3.1ms** **2Mbps/1.55ms** **4Mbps/0.82ms**

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.6.4 QoS Out Queue Aging

This page allows you to configure the QoS Out Queue Aging settings for all switch ports as the QoS Out Queue Aging screen in Figure 4-6-4 appears.

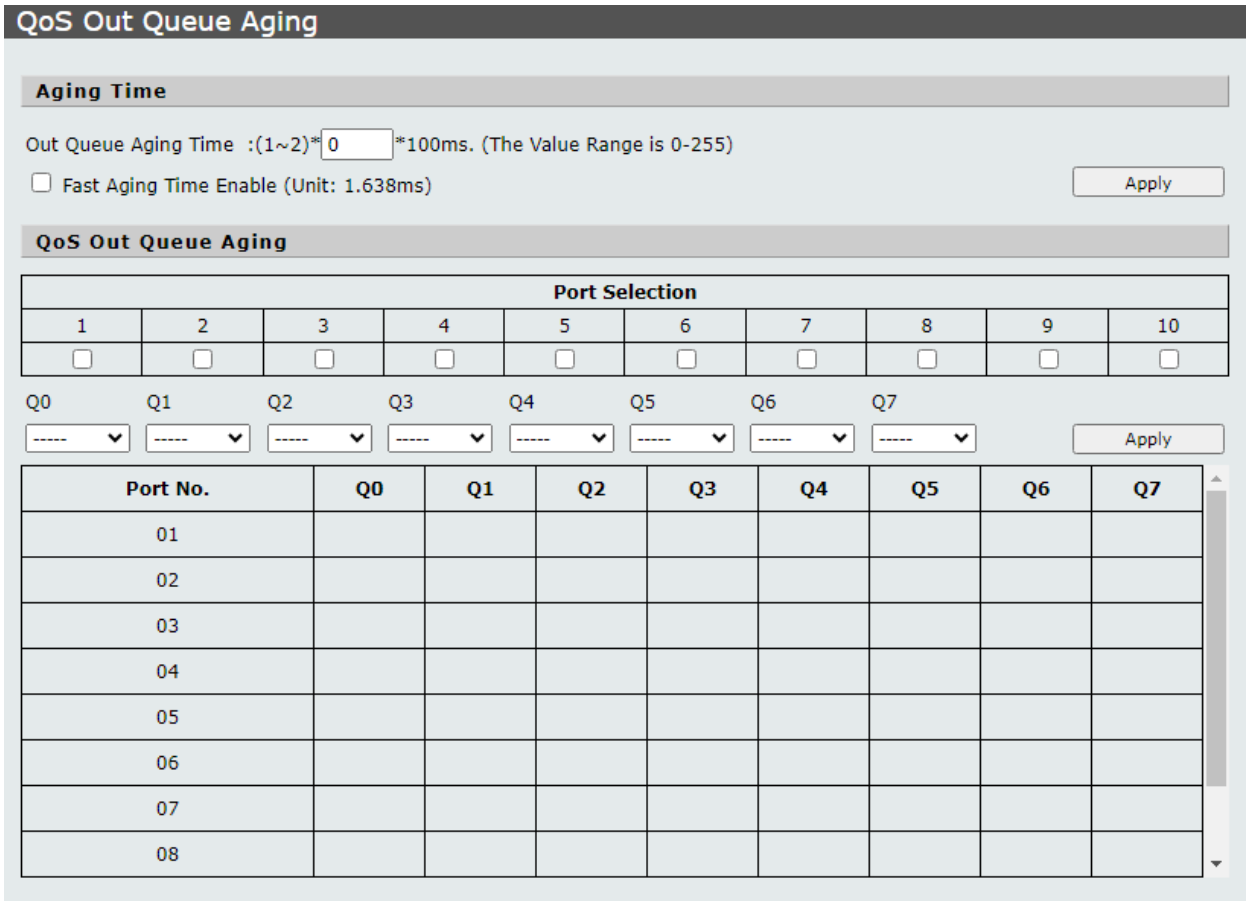


Figure 4-6-4: QoS Out Queue Aging Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Out Queue Aging Time**	Set Out Queue Aging time and the available range is **0-255**.
• **Fast Aging Time Enable**	Set the conversion unit of aging time from **100ms** to **1.638ms**.
• **Port Selection**	Select specific port for QoS Out Queue Aging settings.
• **Q0 ~ Q7**	Enable or disable the QoS Out Queue Aging settings.
• **Port No.**	Display per port list.
• **Q0-Q7**	Display per port QoS Out Queue Aging settings.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.6.5 QoS Remap

This page allows you to configure the QoS Remap settings for all switch ports as the QoS Remap screen in Figure 4-6-5 appears.

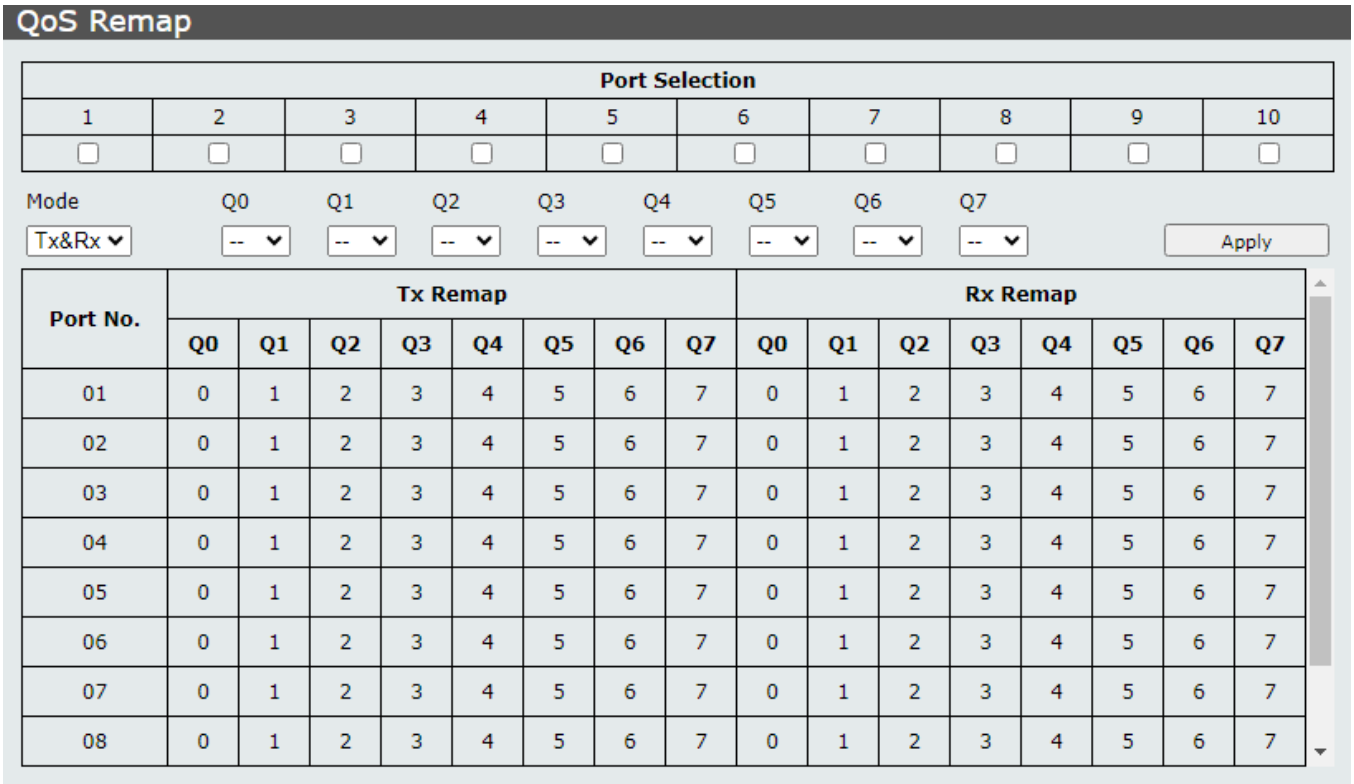


Figure 4-6-5: QoS Remap Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Selection**	Select specific port for QoS Remap settings.
• **Mode**	Set operation mode for specific port and the available options are shown as below: **Tx&Rx** **Tx** **Rx**
• **Q0 ~Q7**	Set each queue to the queue number of QoS Remap.
• **Port No.**	Display per port list.
• **TX Remap Q0-Q7**	Display per port queue number of Q0 to Q7 from TX Remap.
• **RX Remap Q0-Q7**	Display per port queue number of Q0 to Q7 from RX Remap.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.6.6 Class of Service

This page allows you to configure the QoS Class of Service settings for all switch ports as the QoS Class of Servic screen in Figure 4-6-6 appears.

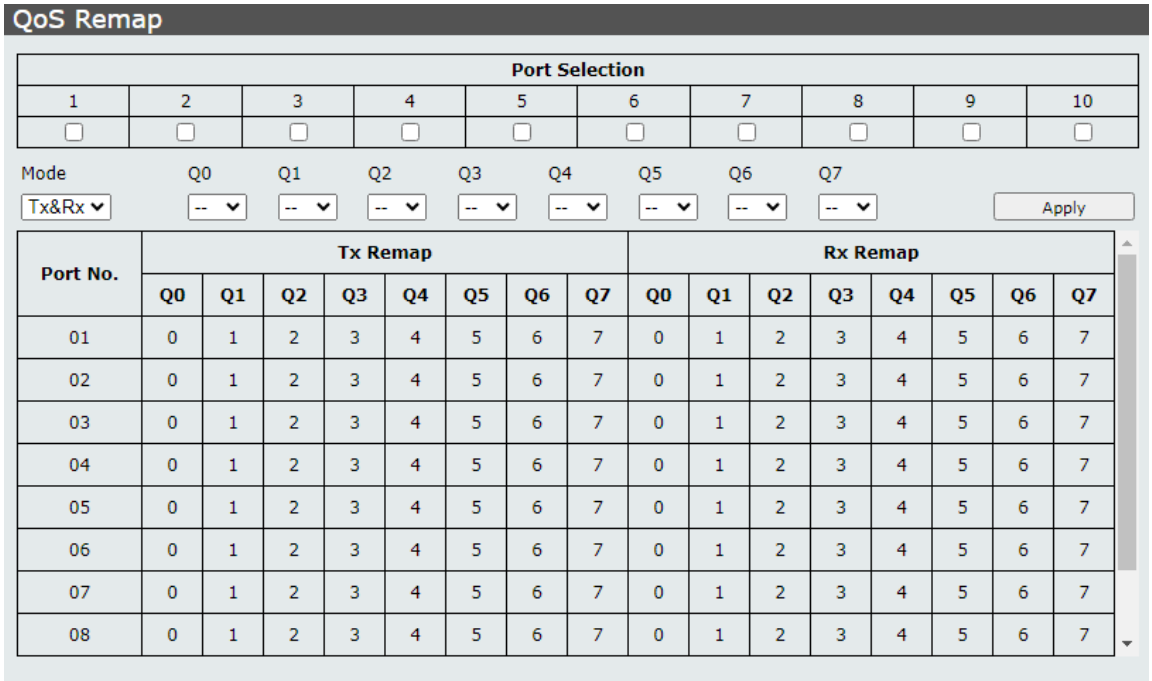


Figure 4-6-6: QoS Class of Service Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Selection**	Select specific port for QoS Class of Service settings.
• **ACL**	Enable or disable the ACL function for specific port. Also display per port ACL status.
• **IGMP**	Enable or disable the IGMP function for specific port. Also display per port ICMP status.
• **IP Addr**	Enable or disable the IP Address function for specific port. Also display per port IP Address status.
• **MAC Addr**	Enable or disable the MAC Address function for specific port. Also display per port MAC Address status.
• **VID**	Enable or disable the VID function for specific port. Also display per port VID status.
• **TCP/UDP Port**	Enable or disable the TCP/UDP Port function for specific port. Also display per port TCP/UDP Port status.
• **DSCP**	Enable or disable the DSCP function for specific port. Also display per port DSCP status.
• **802.1p**	Enable or disable the 802.1p function for specific port. Also display per port 802.1p status.
• **Physical Port**	Select Queue ratio for specific port and the available range is **Queue0-Queue7**. Also display per port Queue status.
• **Port No.**	Display per port list.

Button

: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.6.7 802.1p-based QoS

This page allows you to configure the 802.1p-based QoS settings for Managed PoE+ Switch as the 802.1p-based QoS screen in Figure 4-6-7 appears.

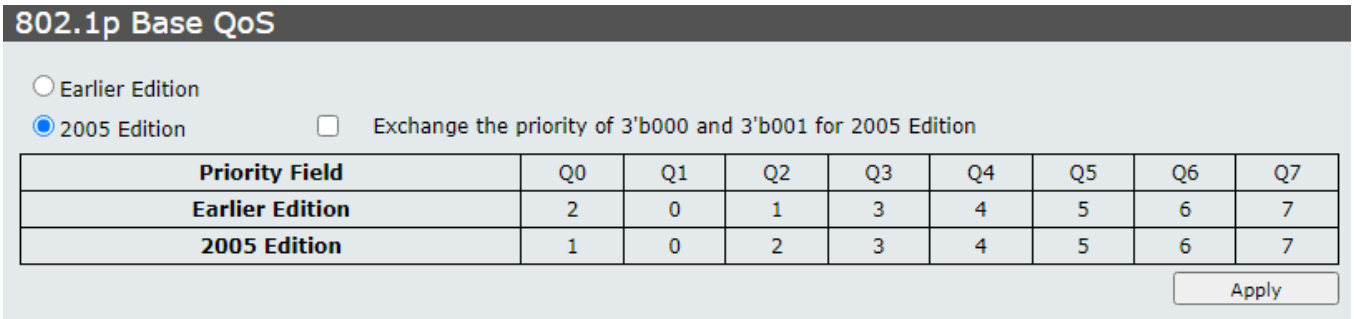
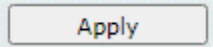


Figure 4-6-7: 802.1p-based QoS Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Earlier Edition**	Click to select the Eariler Edition for 802.1p-based QoS.
• **2005 Edition**	Click to select the 2005 Edition for 802.1p-based QoS.
• **Exchange the priority of 3'b001 for 2005 Edition**	Click to select the Exchange the priority of 3'b001 for 2005 Edition for 802.1p-base QoS.
• **Priority Field**	Display priority field of Q0 to Q7.
• **Earlier Edition**	Display earlier edition for 802.1p-based QoS.
• **2005 Edition**	Display 2005 edition for 802.1p-based QoS.

Button



: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.6.8 DSCP-based Priority

This page allows you to configure the DSCP-based Priority settings for Managed PoE+ Switch as the DSCP-based Priority screen in Figure 4-6-8 appears.

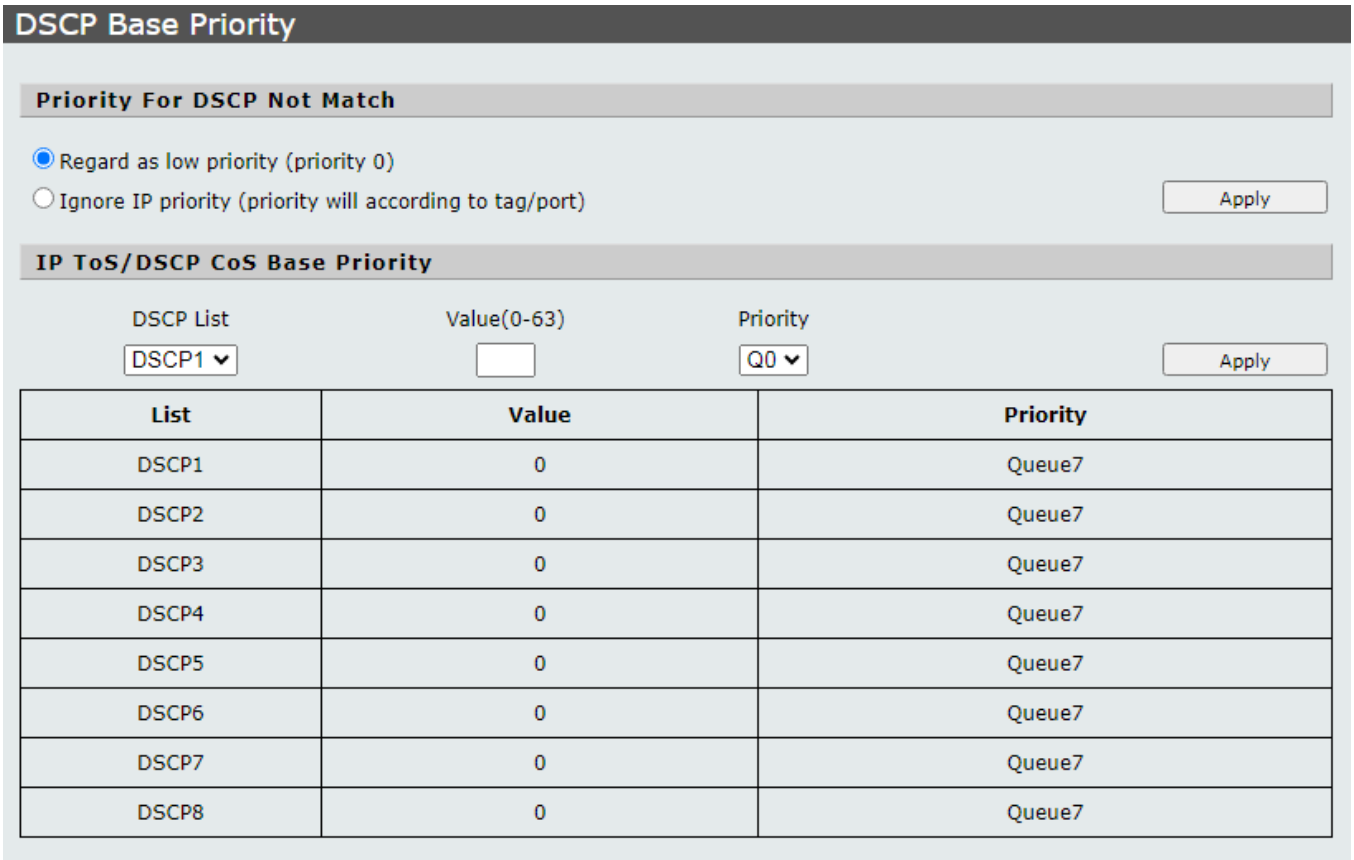


Figure 4-6-8: DSCP-based Priority Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Priority For DSCP Not Match**	Provide two options for selection. **Regard as low priority (priority 0)** **Ignore IP priority (priority will according to tag/port)**
• **IP ToS/DSCP CoS Base Priority**	Provide three functions for setting. **DSCP List**: provide DSCP1 to DSCP8 options to choose. **Value(0-63):**allow input the value range from 0 to 63. **Priority:** provide Q0 to Q7 options to choose.
• **List**	Display DSCP1 to DSCP8.
• **Value**	Display the value setting of per DSCP1 to DSCP8.
• **Priority**	Display the priority setting of per DSCP1 to DSCP8.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.6.9 TCP/UDP Port-based QoS

This page allows you to configure the TCP/UDP Port-based QoS settings for Managed PoE+ Switch as the TCP/UDP Port-based QoS screen in Figure 4-6-9 appears.

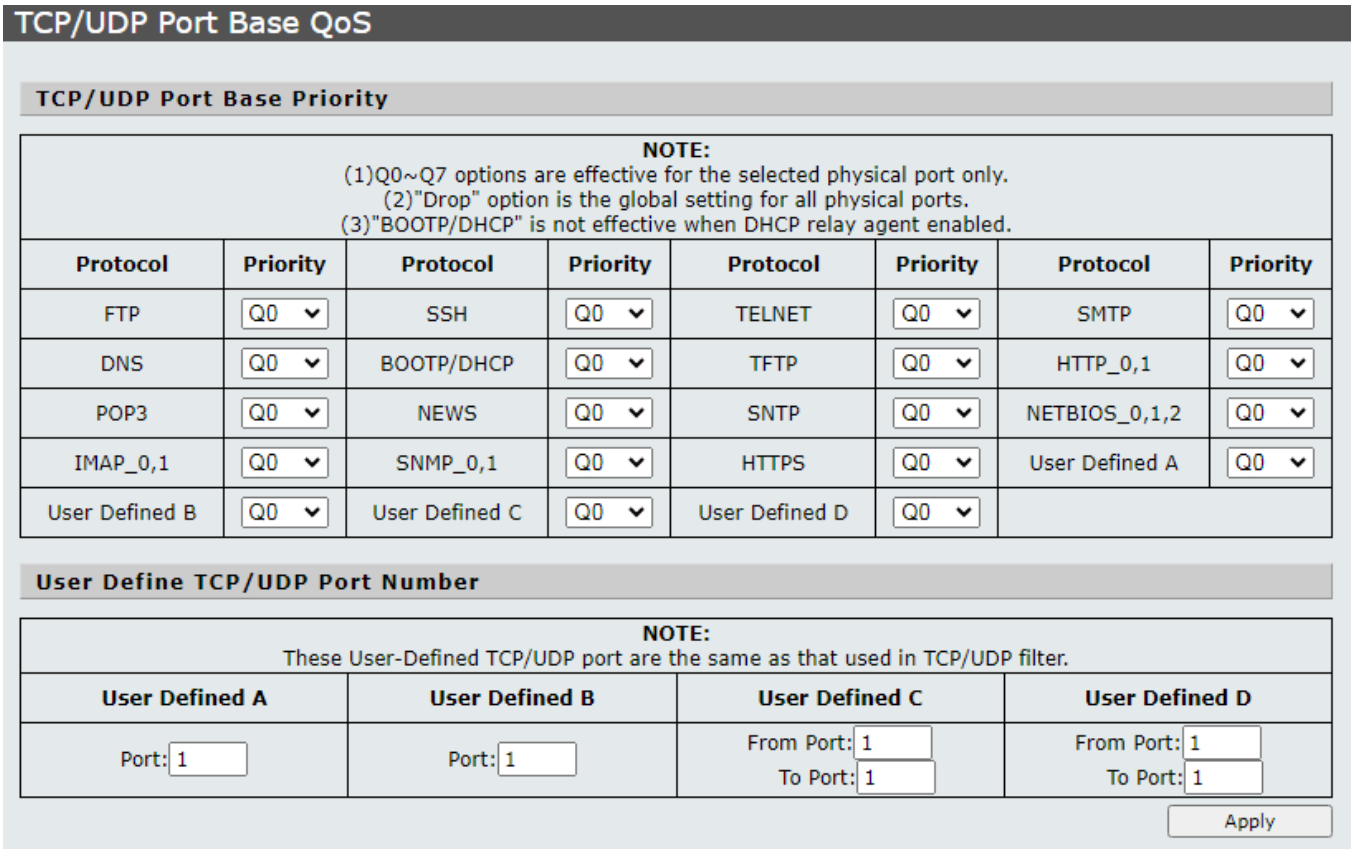
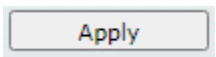


Figure 4-6-9: TCP/UDP Port-based QoS Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **TCP/UDP Port-based Priority**	Provides Q0 to Q7 and Drop options for the following protocols. **FTP/SSH/TELNET/SMTP/DNS/BOOTP/DHCP/TFTP/HTTP_0.1/POP3/NEWS/ SNTP/NETBIOS_0.1.2/IMAP_0.1/SNMP_0.1/HTTPS/User Defined A/ User Defined B/ User Defined C/ User Defined D.**
• **User Defined TCP/UDP Port Number**	Provides four functions for setting. **User Defined A (Port #)** **User Defined B (Port #)** **User Defined C (From Port# To Port#)** **User Defined D (From Port# To Port#)**

Button



: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.7 ACL Configuration

4.7.1 Understanding ACL

ACL is an acronym for Access Control List. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

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

ACE is an acronym for Access Control Entry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

On the Access ACL configuration web page, you can view ACL management function information of the Managed PoE+ Switch as the screen in Figure 4-7-1 appears.

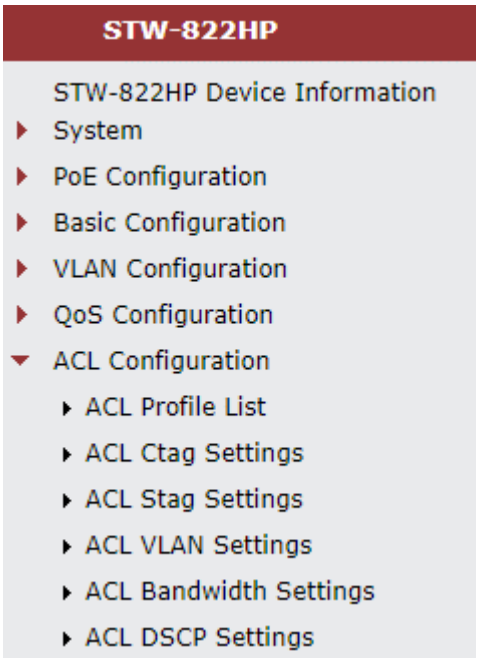


Figure 4-7-1: Managed PoE+ Switch ACL Configuration Web Page

ACL Configuration	
Item	**Description**
ACL Profile List	Configure and display ACL Profile List configuration settings on this web page.
ACL Ctag Settings	Configure and display ACL Ctag Settings configuration settings on this web page.
ACL Stag Settings	Configure and display ACL Stag Settings configuration settings on this web page.
ACL VLAN Settings	Configure and display ACL VLAN Settings configuration settings on this web page.
ACL Bandwidth Settings	Configure and display ACL Bandwidth Settings configuration settings on this web page.
ACL DSCP Settings	Configure and display ACL DSCP Settings configuration settings on this web page.

Table 4-7-1: Desciptions of ACL Configuration

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.7.2 ACL Profile List

This page allows you to configure the ACL Profile List settings for Managed PoE+ Switch as the ACL Profile List screen in Figure 4-7-2 appears.

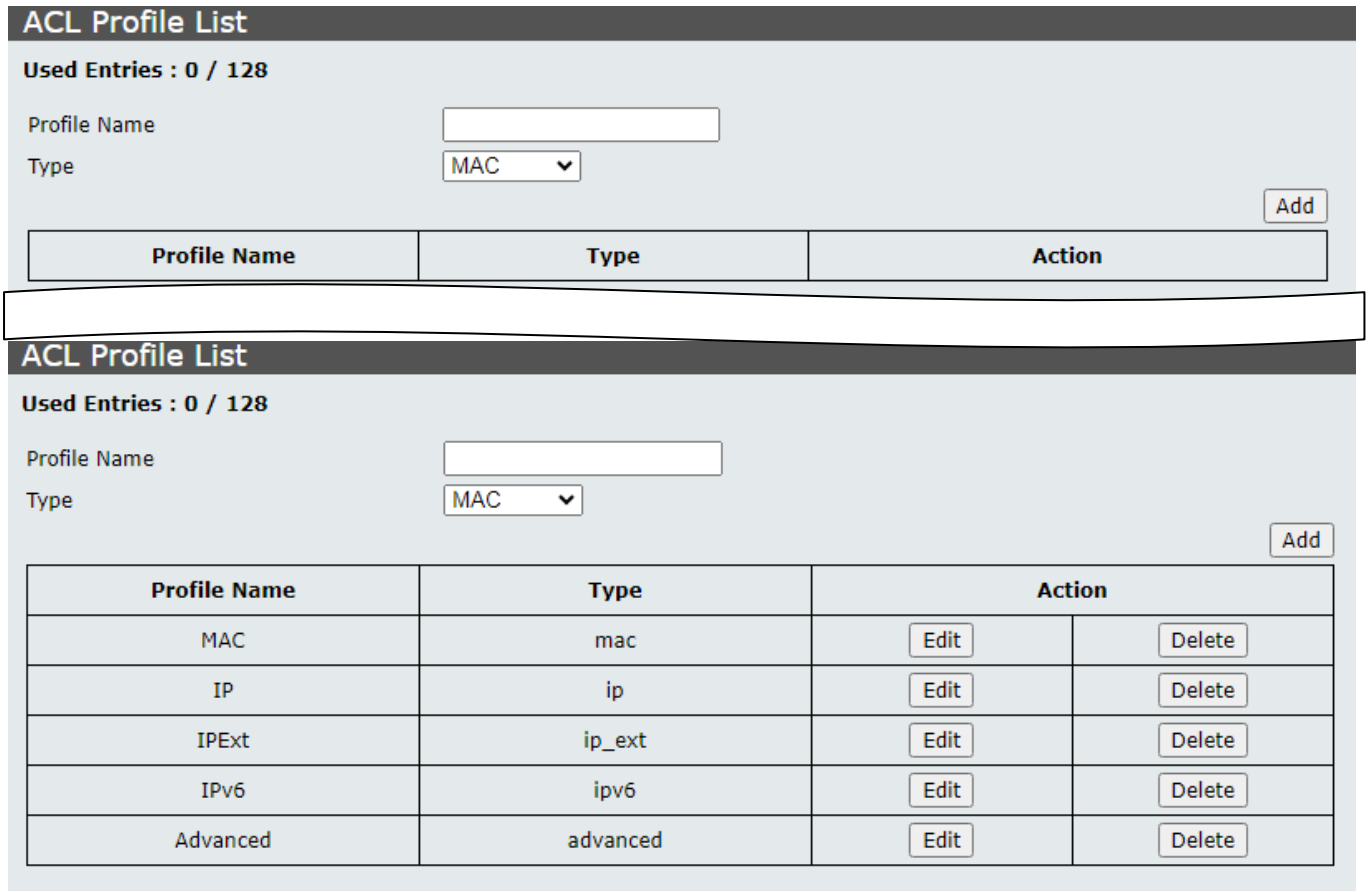


Figure 4-7-2: ACL Profile List Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **User Entries**	Display the amount of entry occupied by rules that has been set up successfully, with a maximum of 128. It is not a rule that takes up an entry; the number of entry occupied by a rule is automatically calculated according to the setting.
• **Profile Name**	Display and configure the name of a specific ACL Profile; the maximum length is 20 characters.
• **Type**	Indicates the frame type of the ACL Profile. Possible values are: **MAC**: The ACL will match the MAC address. **IP**: The ACL will match all IPv4 frames. **IP_Ext**: The ACL will match all IPv4 frames with VID/CoS/TCP Flag/ DSCP/IP protocol. **IPv6**: The ACL will match all IPv6 standard frames. **Advanced**: The ACL will match all MAC address and IPv4 frames with VID/CoS/TCP Flag/ DSCP/IP protocol.
• **Action**	Indicates the forwarding action of the ACL Profile.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	Add: press this button to edit the specific ACL Profile. Delete: press this button to delete the specific ACL Profile.

Buttons

Add: press this button to complete the add ACL Profile procedure.

Edit: press this button to edit the specific ACL Profile.

Delete: press this button to delete the specific ACL Profile.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.7.2.1 MAC

The Access Control List configuration includes the function that is based on MAC address as the screen in Figure 4-7-3 appears.

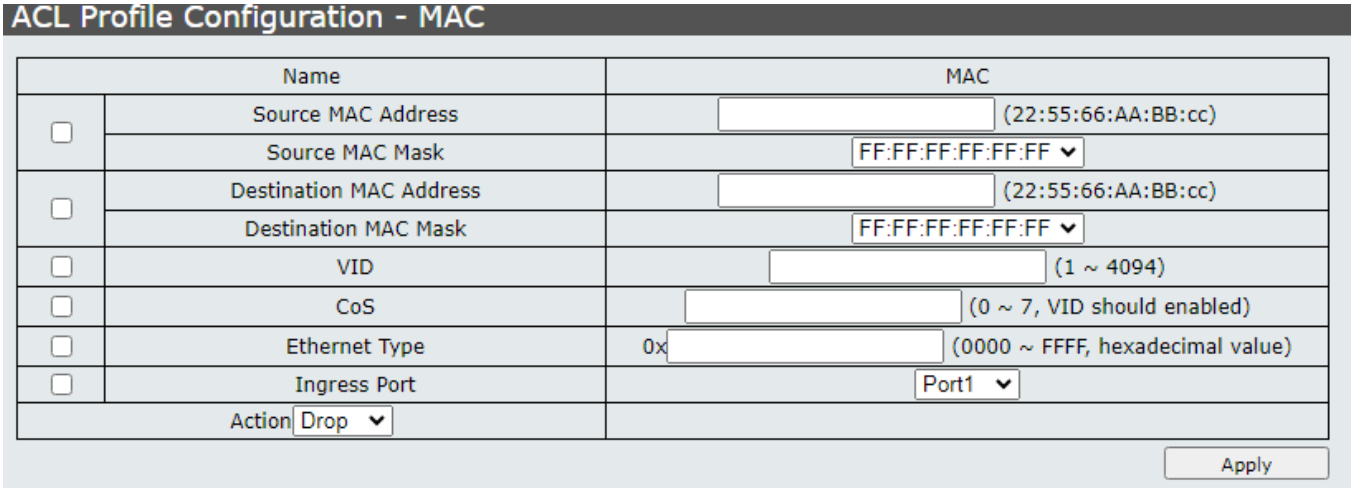


Figure 4-7-3: ACL Profile List-MAC Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Name**	Display the ACL profile name.
• **Source MAC Address**	Configure the Source MAC Address.
• **Source MAC Mask**	Configure the Source MAC Mask and the available options are shown below: **FF:FF:FF:FF:FF:FF** **FF:FF:FF:00:00:00** **FF:FF:00:00:00:00**
• **Destination MAC Address**	Configure the Destination MAC Address.
• **Destination MAC Mask**	Configure the Destination MAC Mask and the available options are shown below: **FF:FF:FF:FF:FF:FF** **FF:FF:FF:00:00:00** **FF:FF:00:00:00:00**
• **VID**	Configure the VID and the available range is **1-4094**.
• **CoS**	Configure the CoS and the available range is **0-7**.
• **Ethernet Type**	Configure the Ethernet Type.
• **Ingress Port**	Select the specific port as Ingress port.
• **Action**	Select the action and the available options are shown below: **Drop** **Type 1** **Type 2**

Button

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Apply : press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.7.2.2 IP

The Access Control List configuration includes the function that is based on IP address as the screen in Figure 4-7-4 appears.

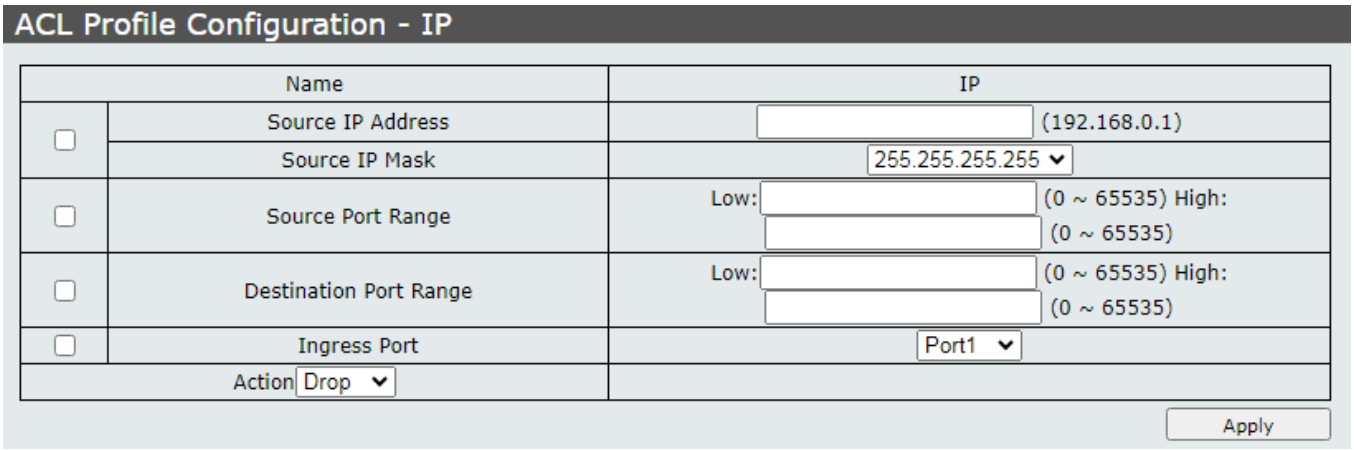


Figure 4-7-4: ACL Profile List-IP Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Name**	Display the ACL profile name.
• **Source IP Address**	Configure the Source IP Address.
• **Source IP Mask**	Configure the Source IP Mask and the available options are shown below: **255:255:255:255** **255:255:255:240** **255:255:255:0** **255:255:240:0** **255.255:0:0** **255.0.0.0** **240.0.0.0**
• **Source Port Range**	Configure the Source Port Range of Low and High.
• **Destination Port Range**	Configure the Destination Port Range of Low and High.
• **Ingress Port**	Select the specific port as Ingress port.
• **Action**	Select the action and the available options are shown below: **Drop** **Type 1** **Type 2**

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.7.2.3 IP_EXT

The Access Control List configuration includes the function that is based on IP address extension as the screen in Figure 4-7-5 appears.

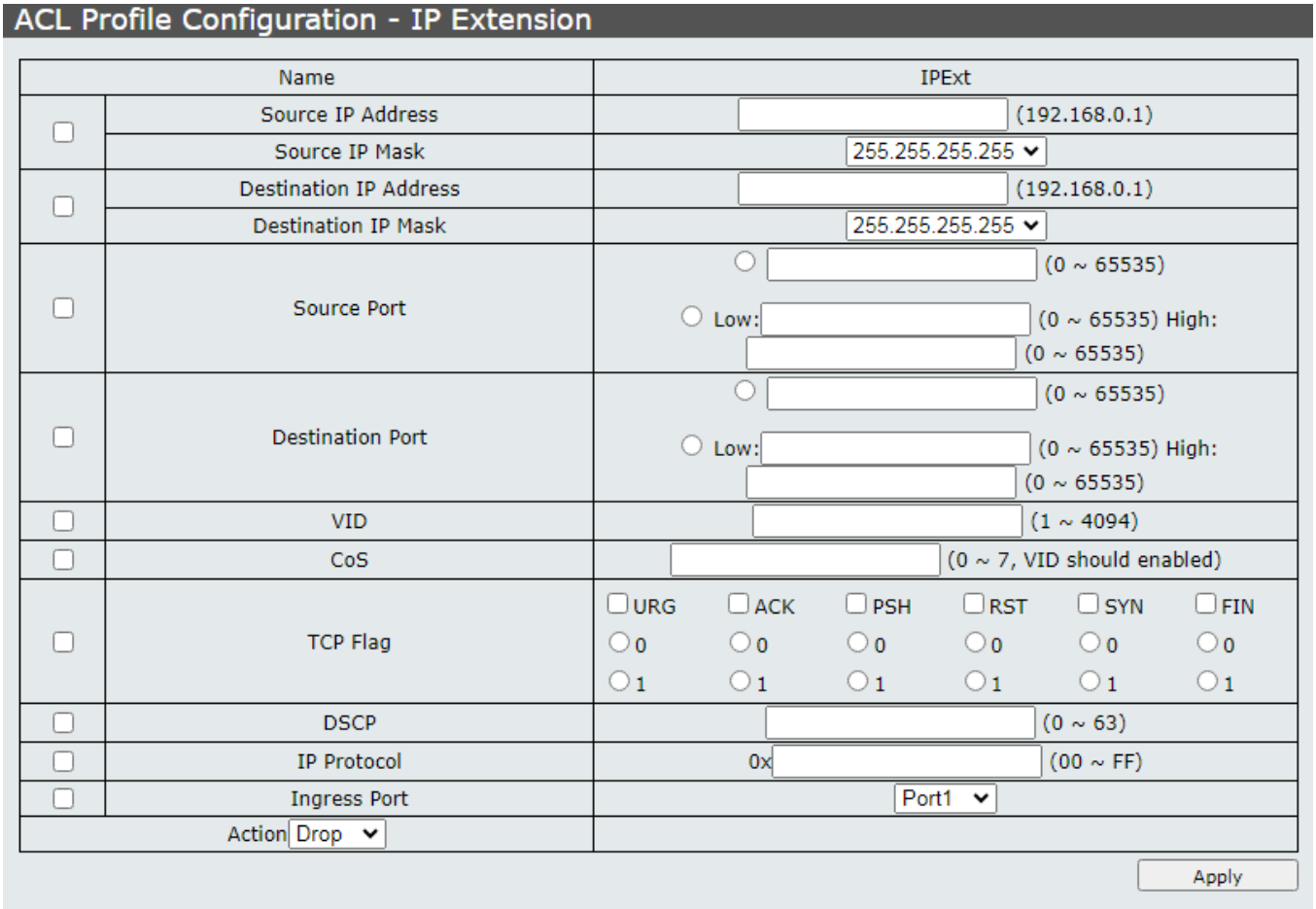


Figure 4-7-5: ACL Profile List-IP Address Extension Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Name**	Display the ACL profile name.
• **Source IP Address**	Configure the Source IP Address.
• **Source IP Mask**	Configure the Source IP Mask and the available options are shown below: **255:255:255:255** **255:255:255:240** **255:255:255:0** **255:255:240:0** **255.255:0:0** **255.0.0.0** **240.0.0.0**
• **Destination IP Address**	Configure the Destination IP Address.
• **Destination IP Mask**	Configure the Destination IP Mask and the available options are shown below: **255:255:255:255** **255:255:255:240**

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	255:255:255:0 **255:255:240:0** **255.255:0:0** **255.0.0.0** **240.0.0.0**
• **Source Port**	Configure the Source Port of Low and High.
• **Destination Port**	Configure the Destination Port of Low and High.
• **VID**	Configure the VID and the available range is **1-4094**.
• **CoS**	Configure the CoS and the vailable range is **0-7**.
• **TCP Flag**	Configure the TCP Flag and available options are shown below: **URG/0/1** **ACK/0/1** **PSH/0/1** **RST/0/1** **SYN/0/1** **FIN/0/1**
• **DSCP**	Configure the DSCP and the available range is **0-63**.
• **IP Protocol**	Configure the IP Protocol.
• **Ingress Port**	Select the specific port as Ingress port.
• **Action**	Select the action and the available options are shown below: **Drop** **Type 1** **Type 2**

Button

Apply : press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.7.2.4 IPv6

The Access Control List configuration includes the function that is based on IPv6 address as the screen in Figure 4-7-6 appears.

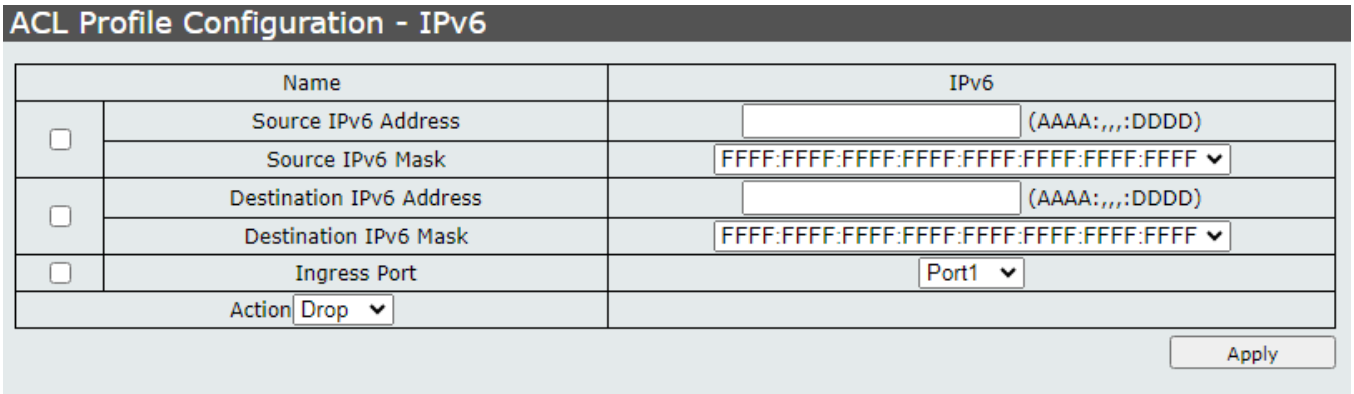


Figure 4-7-6: ACL Profile List-IPv6 Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Name**	Display the ACL profile name.
• **Source IPv6 Address**	Configure the Source IPv6 Address.
• **Source IPv6 Mask**	Configure the Source IPv6 Mask and the available options are shown below: **FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF** **FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:0000:0000** **FFFF:FFFF:FFFF:0000:0000:0000:0000:0000** **FFFF:0000:0000:0000:0000:0000:0000:0000**
• **Destination IPv6 Address**	Configure the Destination IPv6 Address.
• **Destination IPv6 Mask**	Configure the Destination IPv6 Mask and the available options are shown below: **FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF** **FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:0000:0000** **FFFF:FFFF:FFFF:0000:0000:0000:0000:0000** **FFFF:0000:0000:0000:0000:0000:0000:0000**
• **Ingress Port**	Select the specific port as Ingress port.
• **Action**	Select the action and the available options are shown below: **Drop** **Type 1** **Type 2**

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.7.2.5 Advanced

The Access Control List configuration includes the function that is based on IPv6 address as the screen in Figure 4-7-7appears.

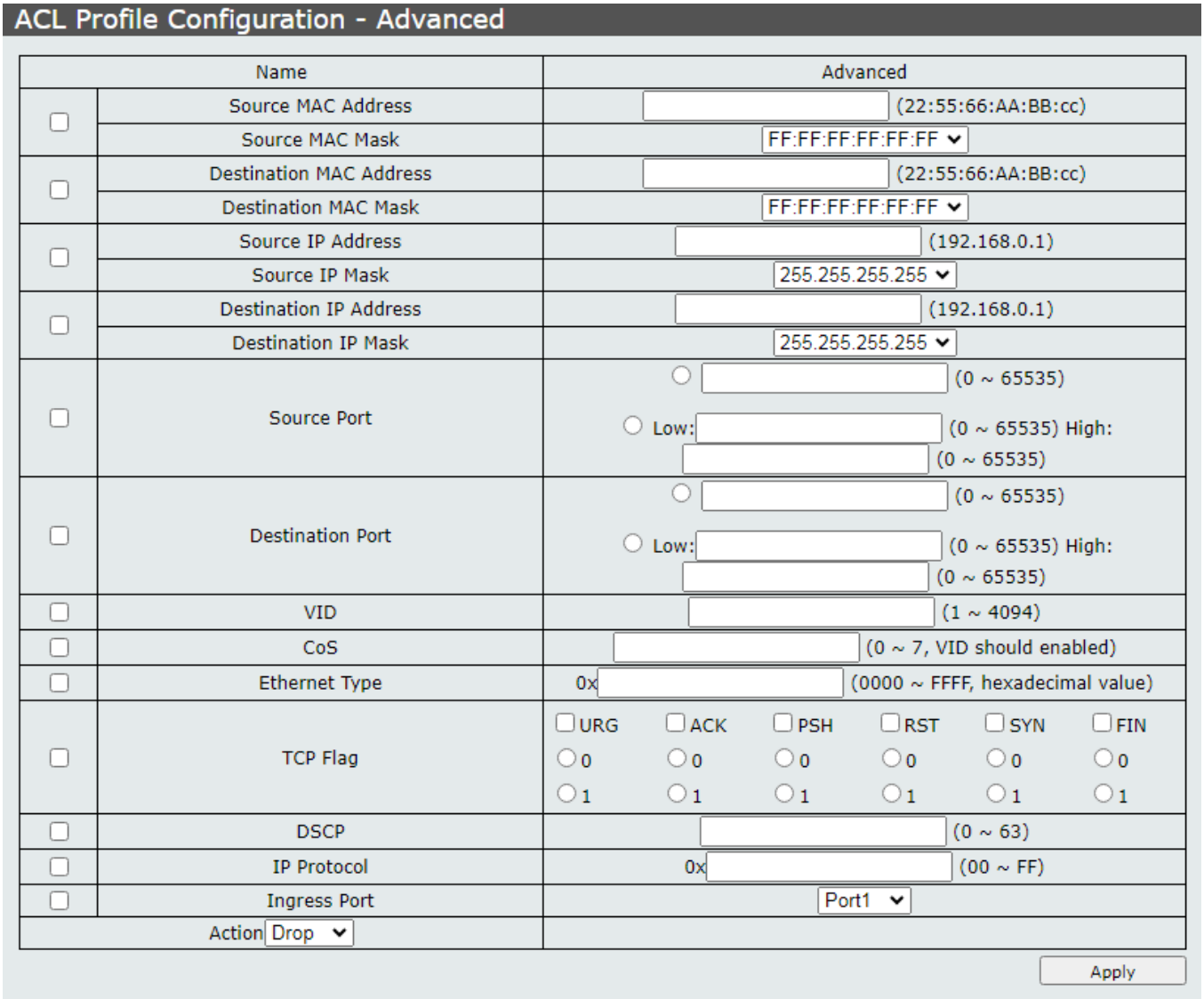


Figure 4-7-7: ACL Profile List-IPv6 Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Name**	Display the ACL profile name.
• **Source MAC Address**	Configure the Source MAC Address.
• **Source MAC Mask**	Configure the Source MAC Mask and the available options are shown below: **FF:FF:FF:FF:FF:FF** **FF:FF:FF:00:00:00** **FF:FF:00:00:00:00**
• **Destination MAC Address**	Configure the Destination MAC Address.
• **Destination MAC Mask**	Configure the Destination MAC Mask and the available options are shown below: **FF:FF:FF:FF:FF:FF** **FF:FF:FF:00:00:00** **FF:FF:00:00:00:00**

SEC.RU | Короткий путь к информации
Скачано с sec.ru

• **Source IP Address**	Configure the Source IP Address.
• **Source IP Mask**	Configure the Source IP Mask and the available options are shown below: **255:255:255:255** **255:255:255:240** **255:255:255:0** **255:255:240:0** **255.255:0:0** **255.0.0.0** **240.0.0.0**
• **Destination IP Address**	Configure the Destination IP Address.
• **Destination IP Mask**	Configure the Destination IP Mask and the available options are shown below: **255:255:255:255** **255:255:255:240** **255:255:255:0** **255:255:240:0** **255.255:0:0** **255.0.0.0** **240.0.0.0**
• **Source Port**	Configure the Source Port of Low and High.
• **Destination Port**	Configure the Destination Port of Low and High.
• **VID**	Configure the VID and the available range is **1-4094**.
• **CoS**	Configure the CoS and the vailable range is **0-7**.
• **Ethernet Port**	Configure the Ethernet Type.
• **TCP Flag**	Configure the TCP Flag and available options are shown below: **URG/0/1** **ACK/0/1** **PSH/0/1** **RST/0/1** **SYN/0/1** **FIN/0/1**
• **DSCP**	Configure the DSCP and the available range is **0-63**.
• **IP Protocol**	Configure the IP Protocol.
• **Ingress Port**	Select the specific port as Ingress port.
• **Action**	Select the action and the available options are shown below: **Drop** **Type 1** **Type 2** **Type 3** **Type 4**

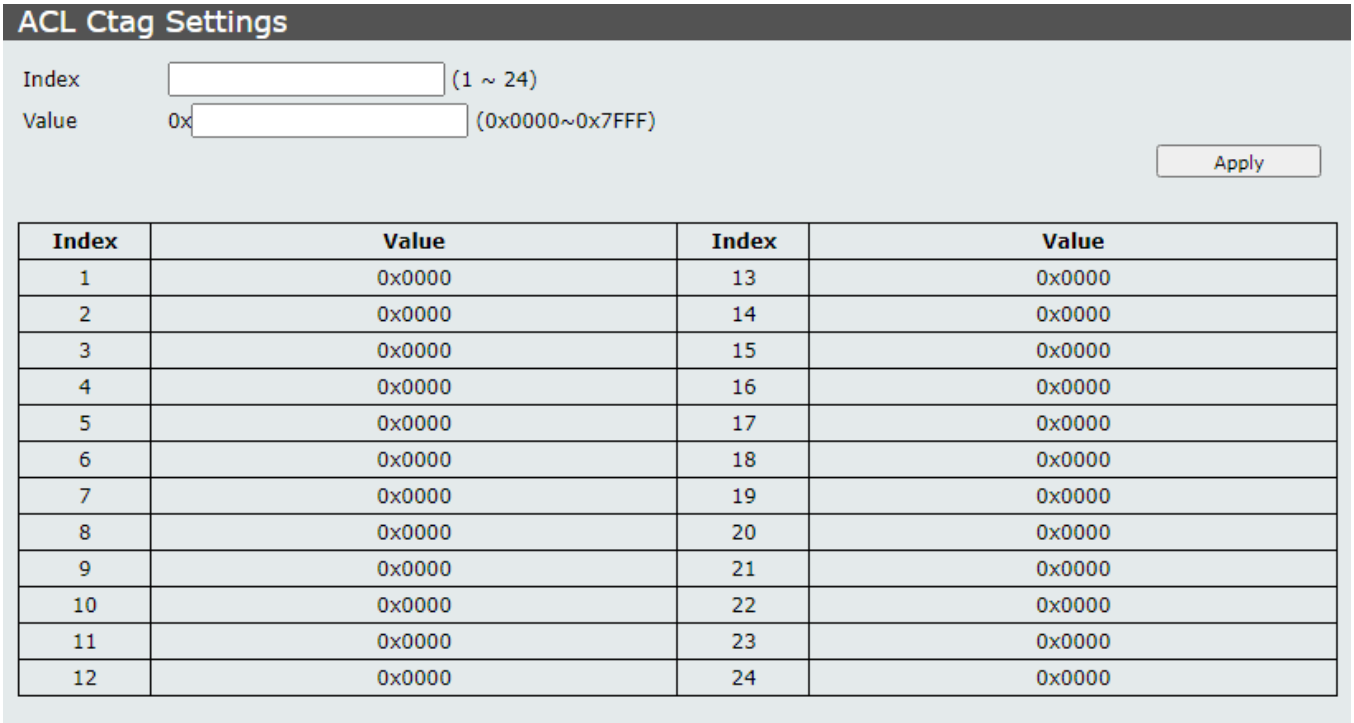
Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.7.3 ACL Ctag Settings

This page allows you to configure the ACL Ctag settings for Managed PoE+ Switch as the ACL Ctag settings configuration screen in Figure 4-7-8 appears.



Index	Value	Index	Value
1	0x0000	13	0x0000
2	0x0000	14	0x0000
3	0x0000	15	0x0000
4	0x0000	16	0x0000
5	0x0000	17	0x0000
6	0x0000	18	0x0000
7	0x0000	19	0x0000
8	0x0000	20	0x0000
9	0x0000	21	0x0000
10	0x0000	22	0x0000
11	0x0000	23	0x0000
12	0x0000	24	0x0000

Figure 4-7-8: ACL Ctag Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Index**	Select specific index for ACL Ctag settings, the available range is **1 to 24**.
• **Value**	Configure and indicate per index value of the ACL Ctag settings; the value must be hexadecimal and available range is **0x0000 to 0x7FFF**.

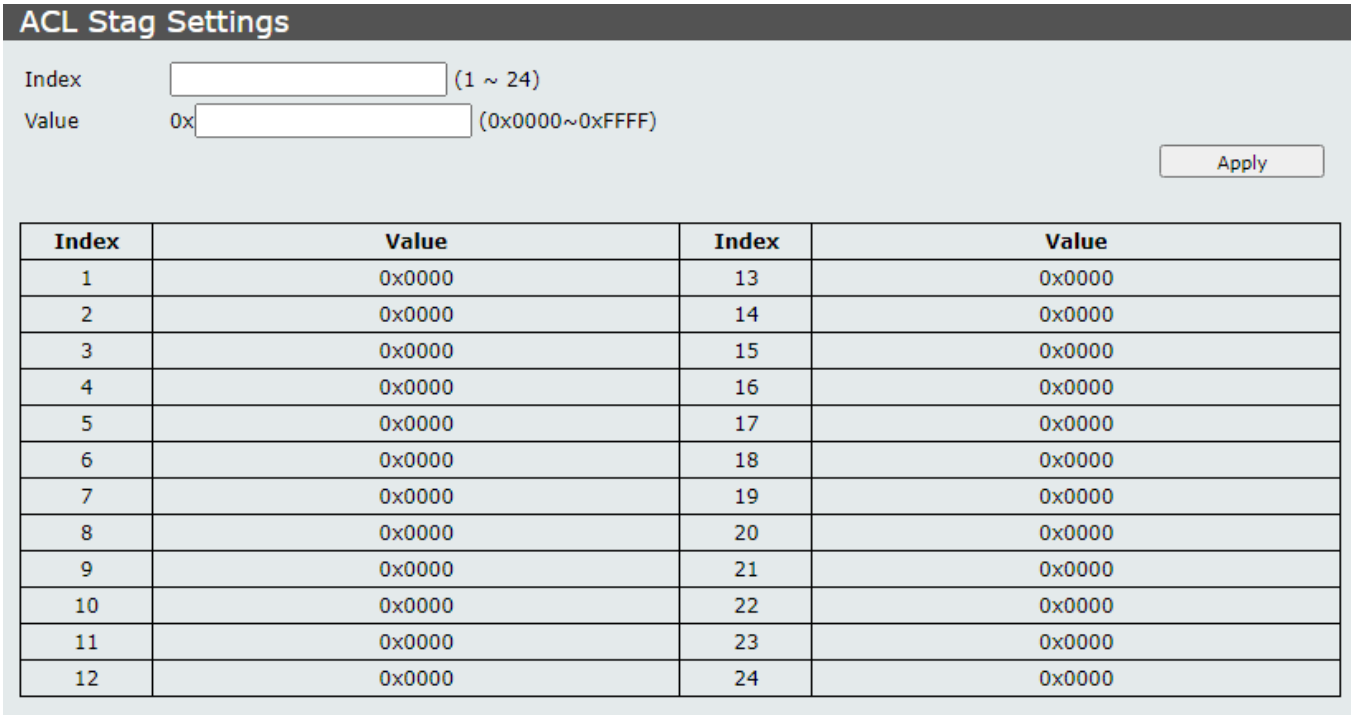
Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.7.4 ACL Stag Settings

This page allows you to configure the ACL Stag settings for Managed PoE+ Switch as the ACL Stag settings configuration screen in Figure 4-7-9 appears.



Index	Value	Index	Value
1	0x0000	13	0x0000
2	0x0000	14	0x0000
3	0x0000	15	0x0000
4	0x0000	16	0x0000
5	0x0000	17	0x0000
6	0x0000	18	0x0000
7	0x0000	19	0x0000
8	0x0000	20	0x0000
9	0x0000	21	0x0000
10	0x0000	22	0x0000
11	0x0000	23	0x0000
12	0x0000	24	0x0000

Figure 4-7-9: ACL Stag Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Index**	Select specific index for ACL Stag settings and the available range is **1 to 24**.
• **Value**	Configure and indicate per index value of the ACL Stag settings; the value must be hexadecimal and available range is **0x0000 to 0xFFFF**.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.7.5 ACL VLAN Settings

This page allows you to configure the ACL VLAN settings for Managed PoE+ Switch as the ACL VLAN settings configuration screen in Figure 4-7-10 appears.

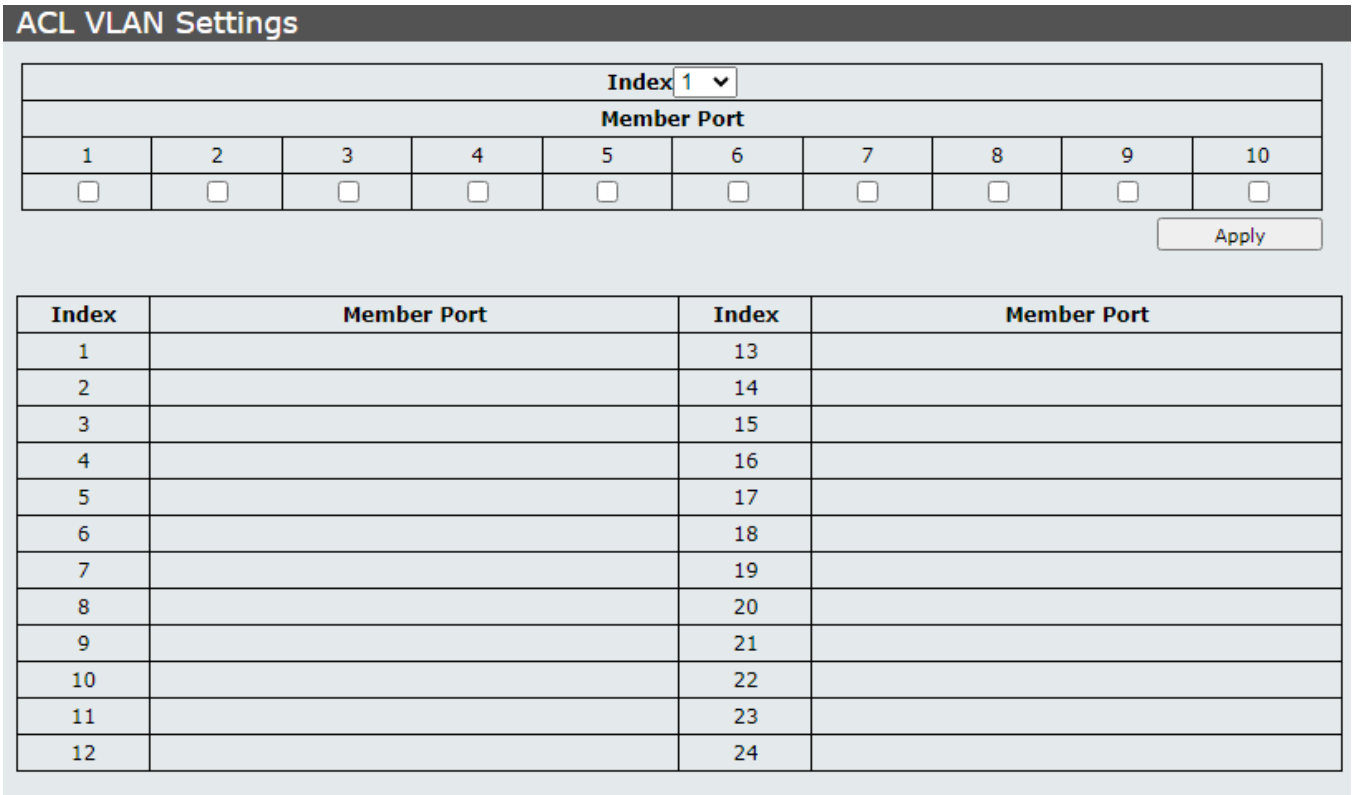


Figure 4-7-10: ACL VLAN Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Index**	Select specific index for ACL VLAN settings; the available range is **1 to 24**.
• **Member Port**	Configure and indicate per index member port of the ACL VLAN settings.

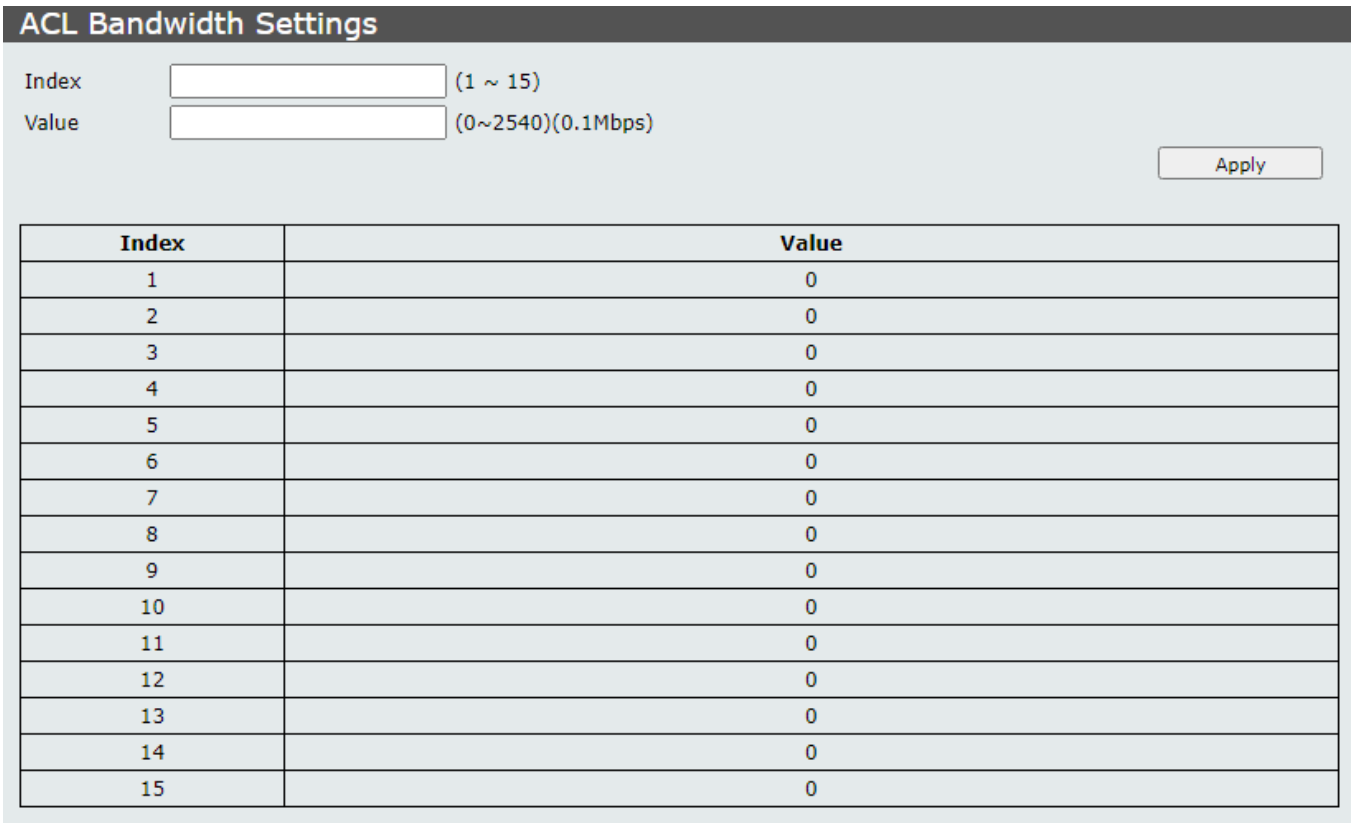
Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.7.6 ACL Bandwidth Settings

This page allows you to configure the ACL bandiwdth settings for Managed PoE+ Switch as the ACL bandiwdth settings configuration screen in Figure 4-7-11 appears.



Index	Value
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0
13	0
14	0
15	0

Figure 4-7-11: ACL Bandwidth Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Index**	Configure specific index for ACL bandiwdth settings; the available range is **1 to 15**.
• **Value**	Configure and indicate per index value of the ACL bandwidth settings; the value available range is **0 to 2540**.

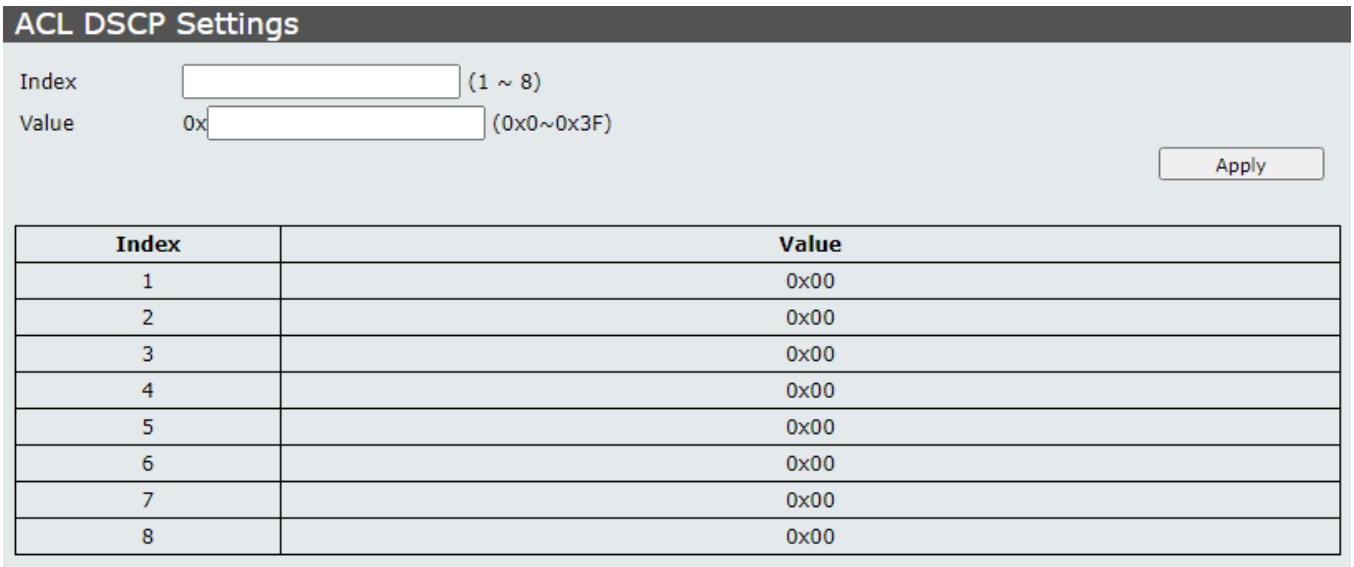
Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.7.7 ACL DSCP Settings

This page allows you to configure the ACL DSCP settings for Managed PoE+ Switch as the ACL DSCP settings configuration screen in Figure 4-7-12 appears.



Index	Value
1	0x00
2	0x00
3	0x00
4	0x00
5	0x00
6	0x00
7	0x00
8	0x00

Figure 4-7-12: ACL DSCP Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Index**	Configure specific index for ACL DSCP settings; the available range is **1 to 8**.
• **Value**	Configure and indicate per index value of the ACL DSCP setting; the value must be hexadecimal and available range is **0x0 to 0x3F**.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.8 Security

On the Access Security configuration web page, you can view and configure Security functions of the Managed PoE+ Switch as the screen in Figure 4-8-1 appears:

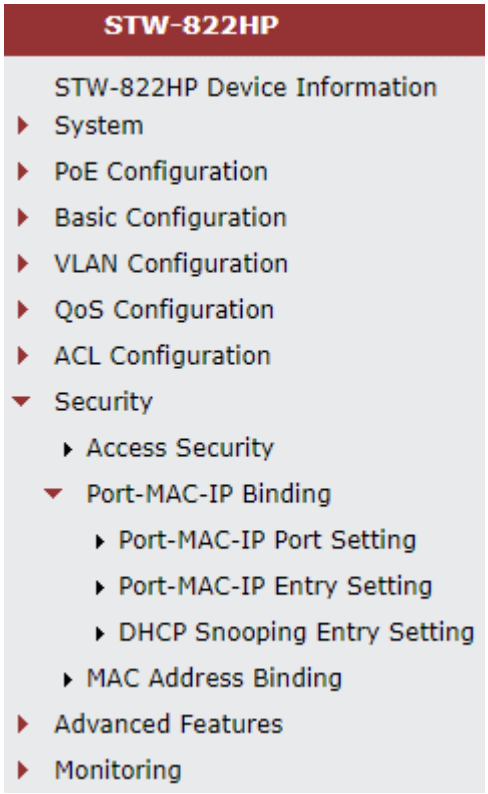


Figure 4-8-1: Managed PoE+ Switch Security Configuration Web Page

Security Configuration	
Item	**Description**
Access Security	Configure and display Access Security configuration settings on this web page.
Port-MAC-IP Binding	Configure and display Port-MAC-IP Binding configuration settings on this web page.
MAC Address Binding	Configure and display MAC Address Binding configuration settings on this web page.

Table 4-8-1: Descriptions of Security Configuration

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.8.1 Access Security

This page allows you to configure the Access Security settings for Managed PoE+ Switch as the Access Security configuration screen in Figure 4-8-2 appears.

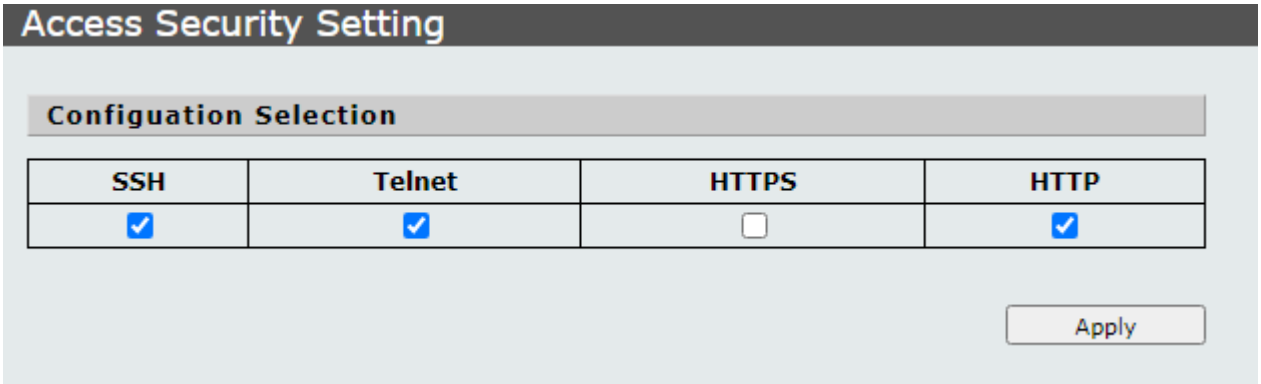


Figure 4-8-2: Access Security Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **SSH**	Configure enable or disable the SSH function and default mode is enable.
• **Telnet**	Configure enable or disable the Telnet function and default mode is enable.
• **HTTPS**	Configure enable or disable the HTTPS function and default mode is enable.
• **HTTP**	Configure enable or disable the HTTP function and default mode is enable.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.8.2 Port-MAC-IP Binding

The Port-MAC-IP Binding configuration provides the IPv4/IPv6 for basic security protection and filtering by checking the source IP address of the packet. Each port can be configured on the page to check whether the source IP address and the source port match. The matching packets are further acted by the two filtering modes selected.

The Port-MAC-IP Binding configuration includes the Port-MAC-IP Port Setting, Port-MAC-IP Entry Setting and DHCP Snooping Entry Setting. Table 4-8-2 shows the items of Port-MAC-IP Binding functions.

Security Configuration	
Item	**Description**
Port-MAC-IP Port Setting	Configure and display Port-MAC-IP Port settings on this web page.
Port-MAC-IP Entry Setting	Configure and display Port-MAC-IP Entry settings on this web page.
DHCP Snooping Entry Setting	Configure and display DHCP Snooping Entry settings on this web page.

Table 4-8-2: Descriptions of Port-MAC-IP Binding Configuration

4.8.2.1 Port-MAC-IP Port Setting

This page allows you to configure the Port-MAC-IP Port settings for Managed PoE+ Switch as the screen in Figure 4-8-3 appears.

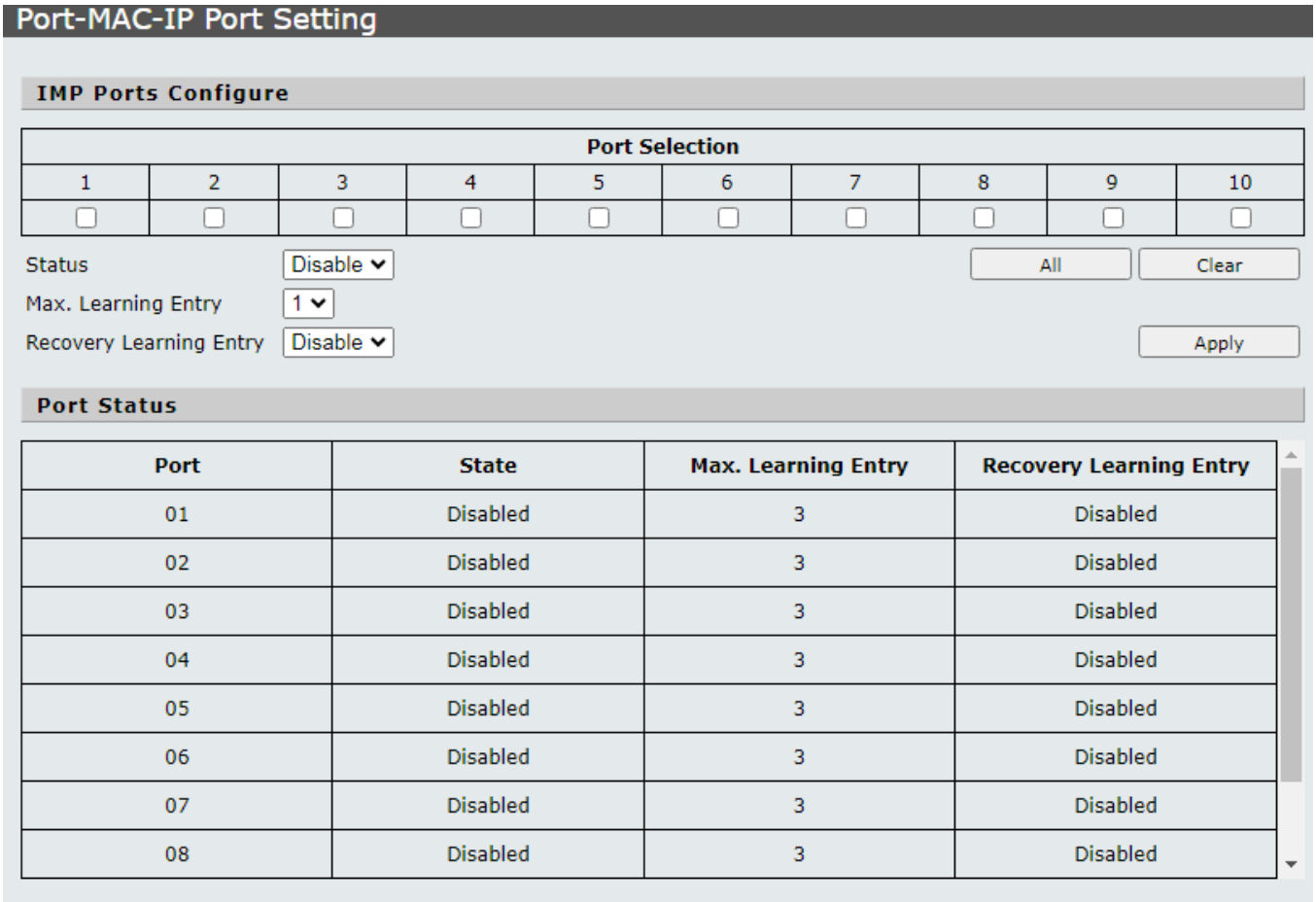


Figure 4-8-3: Port-MAC-IP Port Setting Configuration Screen Page Screenshot

SEC.RU | Короткий путь к информации
Скачано с sec.ru

The page includes the following fields:

Object	Description
• **Port Selection**	Select specific port for Port-MAC-IP Port settings.
• **Status**	Configure enable or disable the Port-MAC-IP Port setting and default mode is disable.
• **Max. Learning Entry**	Configure maximum number of dynamic binding groups for each port, the available range is **1 to 3**.
• **Recovery Learning Entry**	Configure enable or disable the automatically overrides the earliest bound group when the number of dynamically bound groups reaches the upper limit. The default mode is disable.
Port Status	
• **Port**	Display per port list.
• **State**	Display per port current operation mode.
• **Max. Learning Entry**	Display per port maximum number of Max. Learning Entry function.
• **Recovery Learning Entry**	Display per port current operation mode of Recovery Learning Entry function.

Buttons

All : press this button to select all ports.

Clear : press this button to clear all ports selection.

Apply : press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.8.2.2 Port-MAC-IP Entry Setting

This page allows you to configure the Port-MAC-IP Entry settings for Managed PoE+ Switch as the screen in Figure 4-8-4 appears.

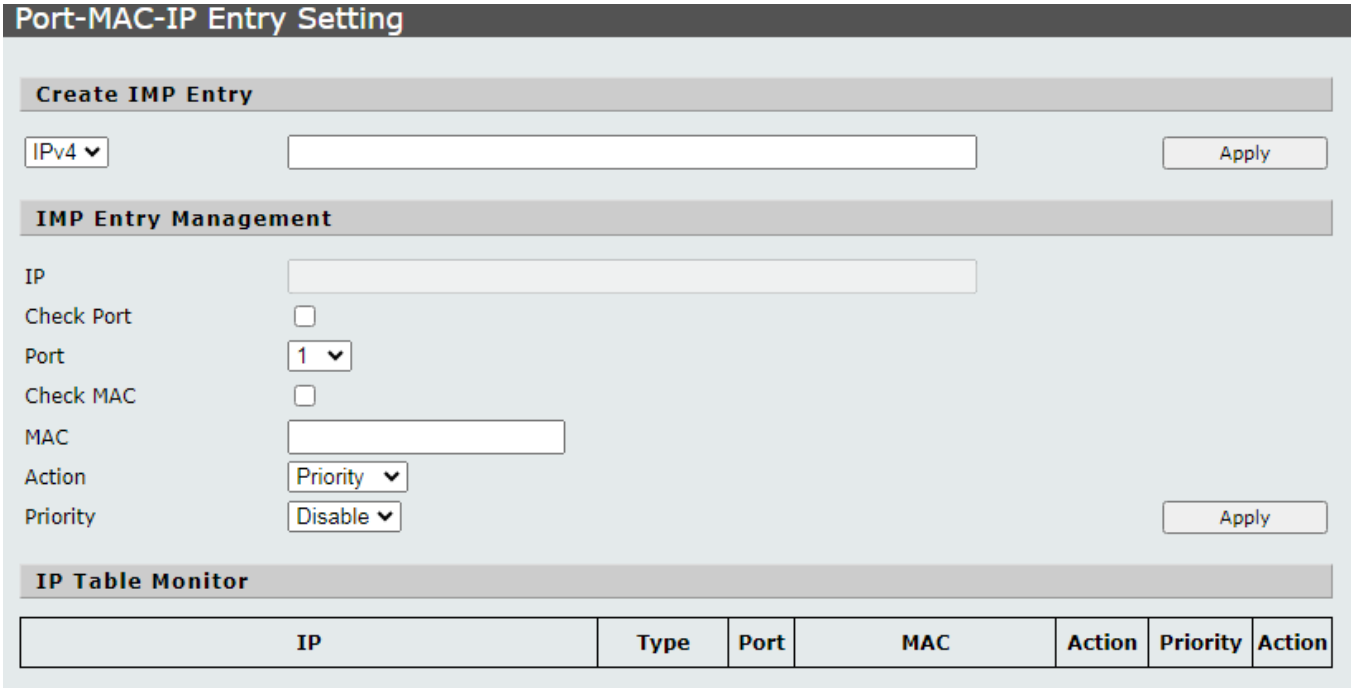


Figure 4-8-4: Port-MAC-IP Entry Setting Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
Create IMP Entry	
• **IPv4/IPv6**	This column allows user to establish the IMP Entry as IPv4 or IPv6, and enter IPv4 or IPv6 IP Address in the right space.
IMP Entry Management	
• **IP**	This column provides corresponding to the selected IMP Entry IP Address.
• **Check Port**	This column provides configuring enable or disable the check source port compliance.
• **Port**	This column provides selecting the port for this IP address.
• **Check MAC**	This column provides configuring enable or disable the check source MAC compliance.
• **MAC**	This column provides configuring the corresponding source MAC for this IP address.
• **Action**	This column provides configuring the corresponding action filter / priority when the condition is met.
• **Priority**	This column provides configuring the queue for this IMP Entry when the action is selected as priority; the available range is **0 to 7**.
IP Table Monitor	
• **IP**	Display the IPv4 or IPv6 address.
• **Type**	Display the type information.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

• **Port**	Display the port information.
• **MAC**	Display the MAC information.
• **Action**	Display the Action status.
• **Priority**	Display the priority status.
• **Action**	Edit: press this button to edit specific Port-MAC-IP Entry setting. Delete: press this button to delete Port-MAC-IP Entry setting.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.8.2.3 DHCP Snooping Entry Setting

This page allows you to configure the DHCP Snooping Entry settings for Managed PoE+ Switch as the screen in Figure 4-8-5 appears.

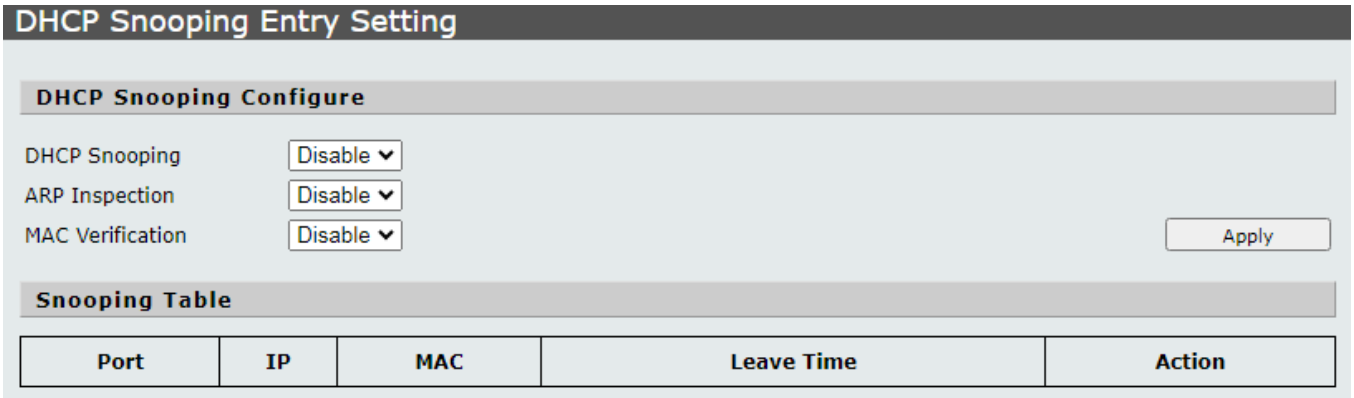


Figure 4-8-5: DHCP Snooping Entry Setting Configuration Screen Page Screenshot

The page includes the following fields:

Object	Description
DHCP Snooping Configure	
• **DHCP Snooping**	This column provides configuring enable or disable the DHCP snooping function. The DHCP Snooping is used to block intruder on the untrusted ports of DUT when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.
• **ARP Inspection**	This column provides configuring enable or disable the ARP inspection function. The ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through DUT.
• **MAC Verification**	This column provides configuring enable or disable the MAC vertification function.
Snooping Table	
• **Port**	Display the port information.
• **IP**	Display the IPv4 or IPv6 address.
• **MAC**	Display the MAC information.
• **Leave Time**	Display the leave time information.
• **Action**	Edit: press this button to edit specific DHCP Snooping Entry setting. Delete: press this button to delete DHCP Snooping Entry setting.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.8.3 MAC Address Binding

The MAC Address Binding configuration provides MAC address-based security function. When this function is enabled, the port will discard packet which does not conform to the MAC table or discard a specific MAC address, mirror forwarding and sampling to the CPU port and other activities.

Only when the port learning function is disabled, can the MAC address in the non-MAC table be effectively prevented from entering the device by the port it binds. Without the broadcast port learning function, only the MAC address existing in the MAC table can be limited to enter the device by its bound port. The MAC address in the non-MAC table cannot be assigned to any port.

The MAC Address Binding Configuration screen in Figure 4-8-6 is shown below.

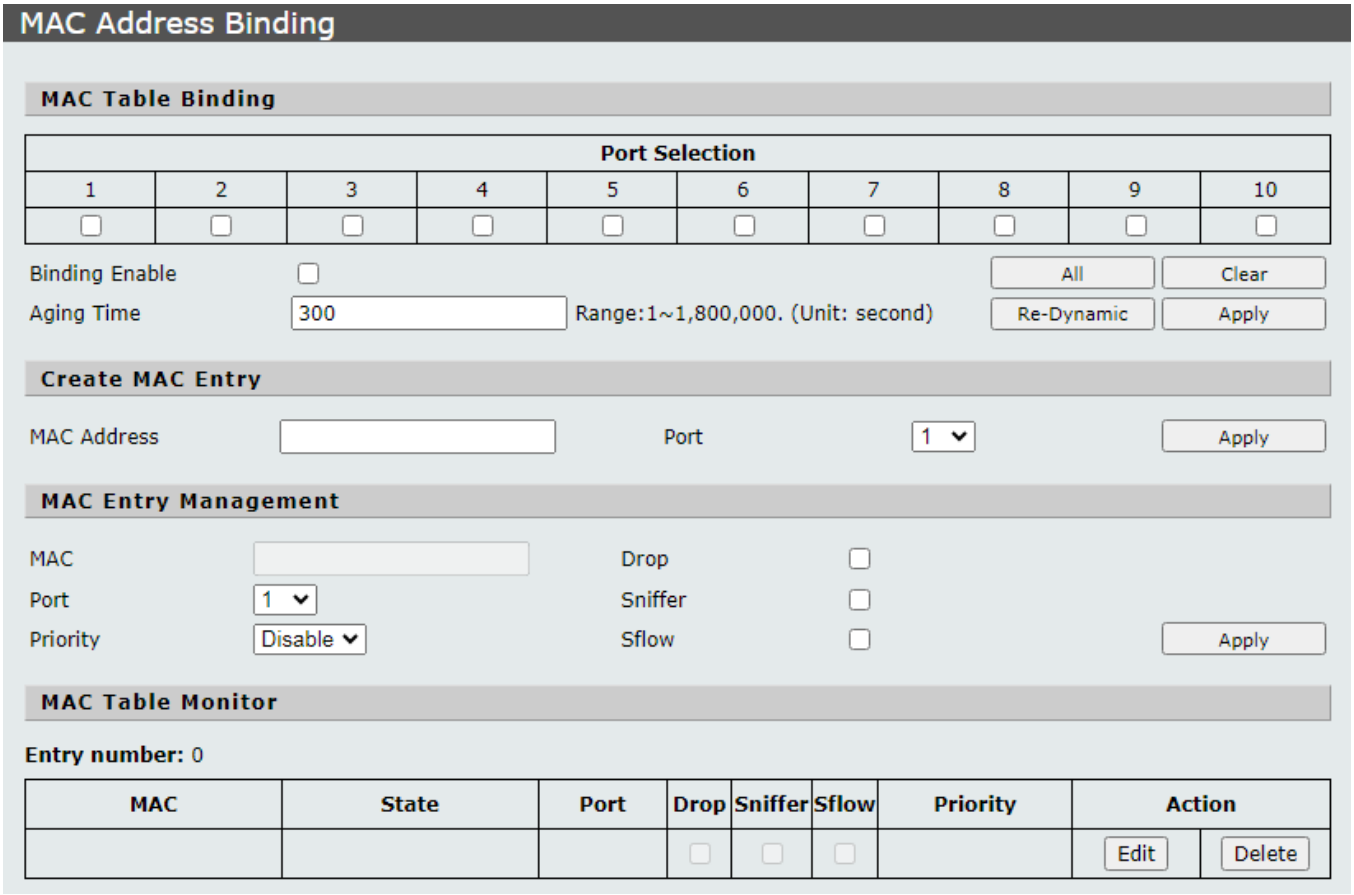


Figure 4-8-6: MAC Address Binding Configuration Screen Page Screenshot

SEC.RU | Короткий путь к информации
Скачано с sec.ru

The page includes the following fields:

Object	Description
MAC Table Binding	
• **Port Selection**	Select specific port for MAC Address Binding settings.
• **Binding Enable**	Click to enable the MAC Binding function.
• **Aging Time**	This column provides configuring the Aging time for MAC address table refresh; the default aging time is **300** seconds and available range is **1 to 1800000** seconds.
MAC Entry Creation	
• **MAC**	This column provides configuring the MAC address for specific port.
• **Port**	This column provides selecting the port for this MAC address.
MAC Entry Management	
• **MAC**	Display the MAC information.
• **Port**	Select specific port for MAC Address Binding settings.
• **Priority**	Select specific priority for MAC Address Binding settings; the default is **Disable** and available options are from **0 to 7**.
• **Drop**	Click to enable the Drop function.
• **Sniffer**	Click to enable the Sniffer function.
• **Sflow**	Click to enable the Sflow function.
MAC Table Monitor	
• **Entry Number**	Display the MAC Address Binding entry number information.
• **MAC**	Display the MAC information.
State	Display the MAC Address state information.
Port	Display the Port information.
Drop	Display the Drop status information.
Sniffer	Display the Sniffer status information.
Sflow	Display the Sflow status information.
Priority	Display the Priority status information.
• **Action**	Edit: press this button to edit specific MAC Address Binding setting. Delete: press this button to delete MAC Address Binding setting.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Buttons

All: press this button to select all ports.

Clear: press this button to clear all ports selection.

Re-Dynamic: press this button to re-dynamic.

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9 Advanced Features

On the Access Advanced Features configuration web page, you can view and configure Advanced Features functions of the Managed PoE+ Switch as the screen in Figure 4-9-1 appears.

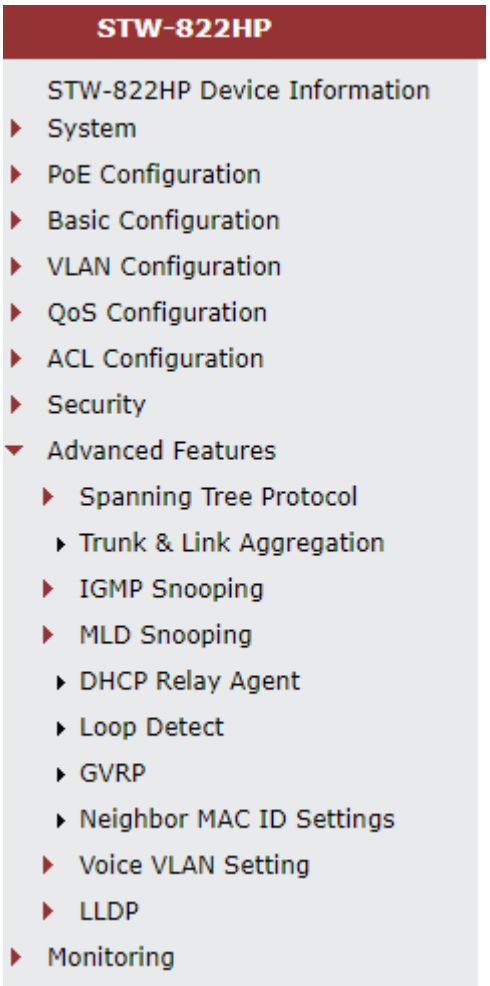


Figure 4-9-1: Managed PoE+ Switch Advanced Features Configuration Web Page

Advanced Features Configuration	
Item	**Description**
Spanning Tree Protocol	Configure and display Spanning Tree Protocol configuration settings on this web page.
Trunk & Link Aggregation	Configure and display Trunk & Link Aggregation configuration settings on this web page.
IGMP Snooping	Configure and display IGMP Snooping configuration settings on this web page.
MLD Snooping	Configure and display MLD Snooping configuration settings on this web page.
DHCP Relay Agent	Configure and display DHCP Relay Agent configuration settings on this web page.
Loop Detect	Configure and display Loop Detect configuration settings on this web page.
GVRP	Configure and display GVRP configuration settings on this web page.
Neighbor MAC ID Settings	Configure and display Neighbor MAC ID settings on this web page.
Voice VLAN Settings	Configure and display Voice VLAN settings on this web page.
LLDP	Configure and display LLDP configuration settings on this web page.

Table 4-9-1: Descriptions of Advanced Features Configuration

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.1 Spanning Tree Protocol

Theory

The Spanning Tree protocol can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the switch to interact with other bridging devices in your network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down. The spanning tree algorithms supported by this switch include these versions:

- **STP – Spanning Tree Protocol (IEEE 802.1D)**
- **RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)**
- **MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)**

The **IEEE 802.1D Spanning Tree** Protocol and **IEEE 802.1w Rapid Spanning Tree** Protocol allow for the blocking of links between switches that form loops within the network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. The protocol allows for the duplicate links to be used in the event of a failure of the primary link. Once the Spanning Tree Protocol is configured and enabled, primary links are established and duplicated links are blocked automatically. The reactivation of the blocked links (at the time of a primary link failure) is also accomplished automatically without operator intervention.

This automatic network reconfiguration provides maximum uptime to network users. However, the concepts of the Spanning Tree Algorithm and protocol are a complicated and complex subject and must be fully researched and understood. It is possible to cause serious degradation of the performance of the network if the Spanning Tree is incorrectly configured. Please read the following before making any changes from the default values.

The Switch STP performs the following functions:

- Creates a single spanning tree from any combination of switching or bridging elements.
- Creates multiple spanning trees – from any combination of ports contained within a single switch, in user specified groups.
- Automatically reconfigures the spanning tree to compensate for the failure, addition, or removal of any element in the tree.
- Reconfigures the spanning tree without operator intervention.

Bridge Protocol Data Units

For STP to arrive at a stable network topology, the following information is used:

- The unique switch identifier
- The path cost to the root associated with each switch port
- The port identifier

STP communicates between switches on the network using Bridge Protocol Data Units (BPDUs). Each BPDU contains the following information:

- The unique identifier of the switch that the transmitting switch currently believes is the root switch
- The path cost to the root from the transmitting port
- The port identifier of the transmitting port

The switch sends BPDUs to communicate and construct the spanning-tree topology. All switches connected to the LAN on which the packet is transmitted will receive the BPDU. BPDUs are not directly forwarded by the switch, but the receiving switch uses the information in the frame to calculate a BPDU, and, if the topology changes, initiates a BPDU transmission.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

The communication between switches via BPDUs results in the following:

- One switch is elected as the root switch
- The shortest distance to the root switch is calculated for each switch
- A designated switch is selected. This is the switch closest to the root switch through which packets will be forwarded to the root.
- A port for each switch is selected. This is the port providing the best path from the switch to the root switch.
- Ports included in the STP are selected.

Creating a Stable STP Topology

It is to make the root port a fastest link. If all switches have STP enabled with default settings, the switch with the lowest MAC address in the network will become the root switch. By increasing the priority (lowering the priority number) of the best switch, STP can be forced to select the best switch as the root switch.

When STP is enabled using the default parameters, the path between source and destination stations in a switched network might not be ideal. For instance, connecting higher-speed links to a port that has a higher number than the current root port can cause a root-port change.

STP Port States

The BPDUs take some time to pass through a network. This propagation delay can result in topology changes where a port that transitioned directly from a Blocking state to a Forwarding state could create temporary data loops. Ports must wait for new network topology information to propagate throughout the network before starting to forward packets. They must also wait for the packet lifetime to expire for BPDU packets that were forwarded based on the old topology. The forward delay timer is used to allow the network topology to stabilize after a topology change. In addition, STP specifies a series of states a port must transition through to further ensure that a stable network topology is created after a topology change.

Each port on a switch using STP exists is in one of the following five states:

- **Blocking** – the port is blocked from forwarding or receiving packets
- **Listening** – the port is waiting to receive BPDU packets that may tell the port to go back to the blocking state
- **Learning** – the port is adding addresses to its forwarding database, but not yet forwarding packets
- **Forwarding** – the port is forwarding packets
- **Disabled** – the port only responds to network management messages and must return to the blocking state first

Port transitions from one state to another are as follows:

- From initialization (switch boot) to blocking
- From blocking to listening or to disable
- From listening to learning or to disable
- From learning to forwarding or to disable
- From forwarding to disable
- From disable to blocking

SEC.RU | Короткий путь к информации
Скачано с sec.ru

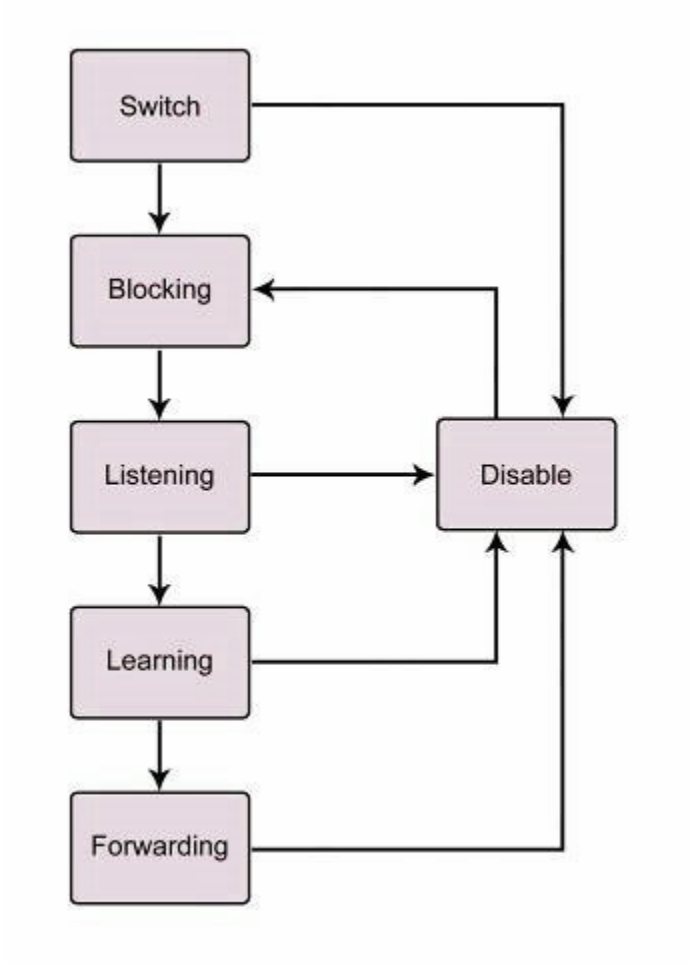


Figure 4-9-2: STP Port State Transitions

You can modify each port state by using management software. When you enable STP, every port on every switch in the network goes through the blocking state and then transitions through the states of listening and learning at power up. If properly configured, each port stabilizes to the forwarding or blocking state. No packets (except BPDUs) are forwarded from, or received by, STP enabled ports until the forwarding state is enabled for that port.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

2. STP Parameters

STP Operation Levels

The Switch allows for two levels of operation: the switch level and the port level. The switch level forms a spanning tree consisting of links between one or more switches. The port level constructs a spanning tree consisting of groups of one or more ports. The STP operates in much the same way for both levels.

Note

On the switch level, STP calculates the Bridge Identifier for each switch and then sets the Root Bridge and the Designated Bridges.

On the port level, STP sets the Root Port and the Designated Ports.

The following are the user-configurable STP parameters for the switch level:

Parameter	Description	Default Value
Bridge Identifier (Not user configurable except by setting priority below)	A combination of the User-set priority and the switch's MAC address. The Bridge Identifier consists of two parts: a 16-bit priority and a 48-bit Ethernet MAC address 32768 + MAC	32768 + MAC
Priority	A relative priority for each switch – lower numbers give a higher priority and a greater chance of a given switch being elected as the root bridge	32768
Hello Time	The length of time between broadcasts of the hello message by the switch	2 seconds
Maximum Age Timer	Measures the age of a received BPDU for a port and ensures that the BPDU is discarded when its age exceeds the value of the maximum age timer.	20 seconds
Forward Delay Timer	The amount time spent by a port in the learning and listening states waiting for a BPDU that may return the port to the blocking state.	15 seconds

The following are the user-configurable STP parameters for the port or port group level:

Variable	Description	Default Value
Port Priority	A relative priority for each port – lower numbers give a higher priority and a greater chance of a given port being elected as the root port	128
Port Cost	A value used by STP to evaluate paths – STP calculates path costs and selects the path with the minimum cost as the active	200,000-100Mbps Fast Ethernet ports 20,000-1000Mbps Gigabit Ethernet ports

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	path	0 - Auto

Default Spanning-Tree Configuration

Feature	Default Value
Enable state	STP disabled for all ports
Port priority	128
Port cost	0
Bridge Priority	32,768

User-Changeable STA Parameters

The Switch's factory default setting should cover the majority of installations. However, it is advisable to keep the default settings as set at the factory; unless, it is absolutely necessary. The user changeable parameters in the Switch are as follows:

Priority – A Priority for the switch can be set from 0 to 65535. 0 is equal to the highest Priority.

Hello Time – The Hello Time can be from 1 to 10 seconds. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other Switches that it is indeed the Root Bridge. If you set a Hello Time for your Switch, and it is not the Root Bridge, the set Hello Time will be used if and when your Switch becomes the Root Bridge.

Note

The Hello Time cannot be longer than the Max. Age; otherwise, a configuration error will occur.

Max. Age – The Max Age can be from 6 to 40 seconds. At the end of the Max Age, if a BPDU has still not been received from the Root Bridge, your Switch will start sending its own BPDU to all other Switches for permission to become the Root Bridge. If it turns out that your Switch has the lowest Bridge Identifier, it will become the Root Bridge.

Forward Delay Timer – The Forward Delay can be from 4 to 30 seconds. This is the time any port on the

Switch spends in the listening state while moving from the blocking state to the forwarding state.

Note

Observe the following formulas when setting the above parameters:

Max. Age _ 2 x (Forward Delay - 1 second)

Max. Age _ 2 x (Hello Time + 1 second)

Port Priority – A Port Priority can be from 0 to 240. The lower the number, the greater the probability the port will be chosen as the Root Port.

Port Cost – A Port Cost can be set from 0 to 200000000. The lower the number, the greater the probability the port will be chosen to forward packets.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

3. Illustration of STP

A simple illustration of three switches connected in a loop is depicted in the below diagram. In this example, you can anticipate some major network problems if the STP assistance is not applied.

If switch A broadcasts a packet to switch B, switch B will broadcast it to switch C, and switch C will broadcast it to back to switch A and so on. The broadcast packet will be passed indefinitely in a loop, potentially causing a network failure. In this example, STP breaks the loop by blocking the connection between switch B and C. The decision to block a particular connection is based on the STP calculation of the most current Bridge and Port settings.

Now, if switch A broadcasts a packet to switch C, then switch C will drop the packet at port 2 and the broadcast will end there. Setting-up STP using values other than the defaults, can be complex. Therefore, you are advised to keep the default factory settings and STP will automatically assign root bridges/ports and block loop connections. Influencing STP to choose a particular switch as the root bridge using the Priority setting, or influencing STP to choose a particular port to block using the Port Priority and Port Cost settings is, however, relatively straight forward.

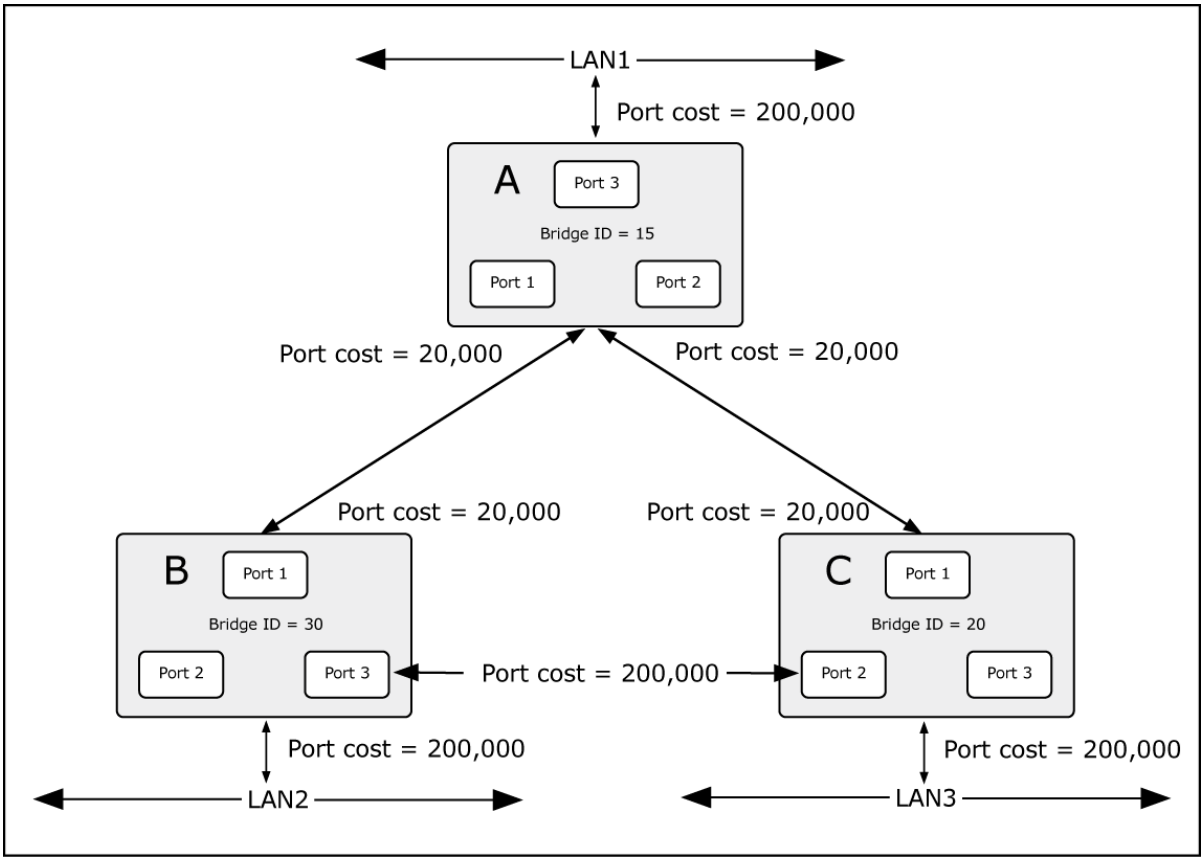


Figure 4-9-3: Before Applying the STA Rules

SEC.RU | Короткий путь к информации
Скачано с sec.ru

In this example, only the default STP values are used.

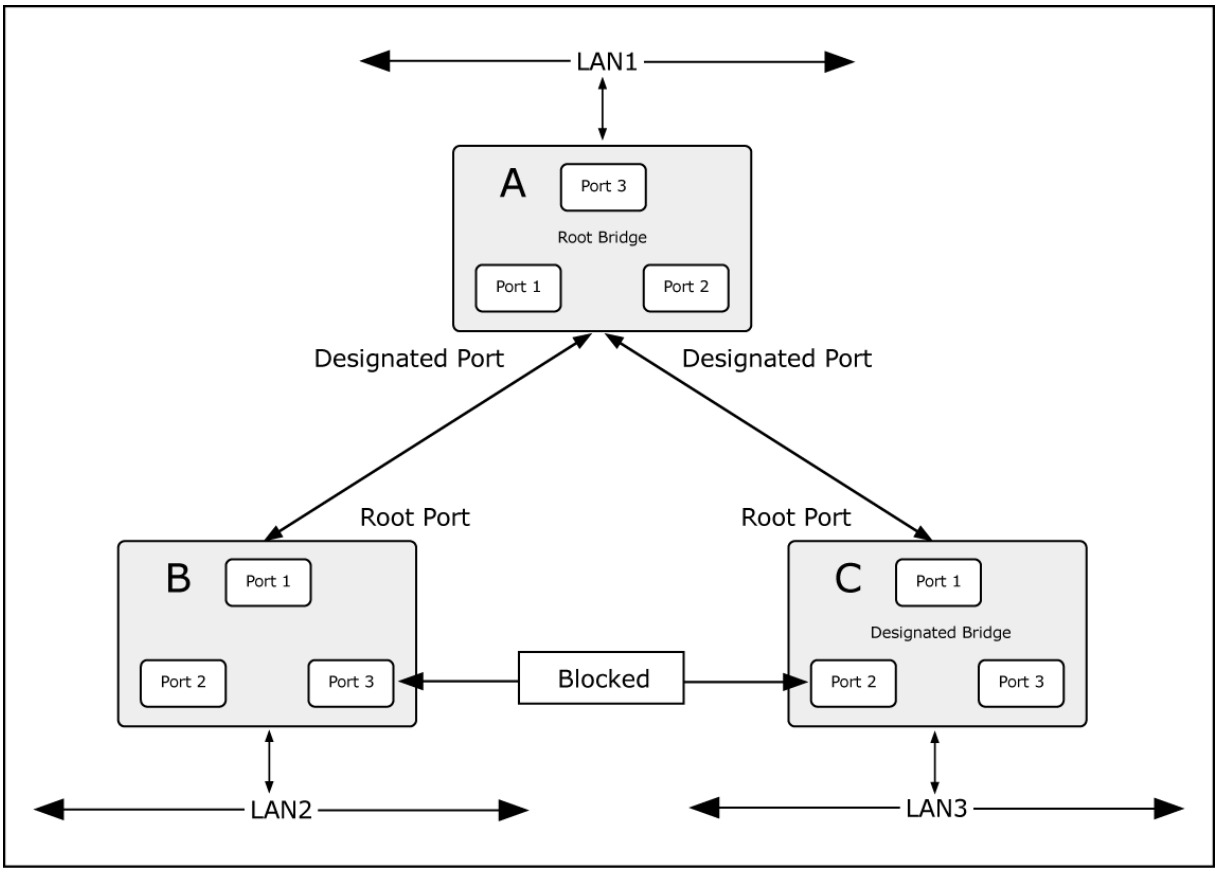


Figure 4-9-4: After Applying the STA Rules

The switch with the lowest Bridge ID (switch C) was elected the root bridge, and the ports were selected to give a high port cost between switches B and C. The two (optional) Gigabit ports (default port cost = 20,000) on switch A are connected to one (optional) Gigabit port on both switch B and C. The redundant link between switch B and C is deliberately chosen as a 100 Mbps Fast Ethernet link (default port cost = 200,000). Gigabit ports could be used, but the port cost should be increased from the default to ensure that the link between switch B and switch C is the blocked link.

The Spanning Tree Protocol configuration includes the Port-MAC-IP Port Setting, Port-MAC-IP Entry Setting and DHCP Snooping Entry Setting and table 4-9-2 show the items of Port-MAC-IP Binding functions.

Spanning Tree Protocol Configuration	
Item	**Description**
STP Global Settings	Configure and display STP Global settings on this web page.
STP Port Settings	Configure and display STP Port settings on this web page.
MST Configuration Identification	Configure and display MST Configuration Identification settings on this web page.
STP Instance Settings	Configure and display STP Instance settings on this web page.
MSTP Port Information	Configure and display MSTP Port Information on this web page.
STP Loop Detect Settings	Configure and display STP Loop Detect settings on this web page.

Table 4-9-2: Descriptions of Spanning Tree Protocol Configuration

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.1.1 STP Global Settings

This page allows you to configure the STP Global settings for Managed PoE+ Switch as the screen in Figure 4-9-5 appears.

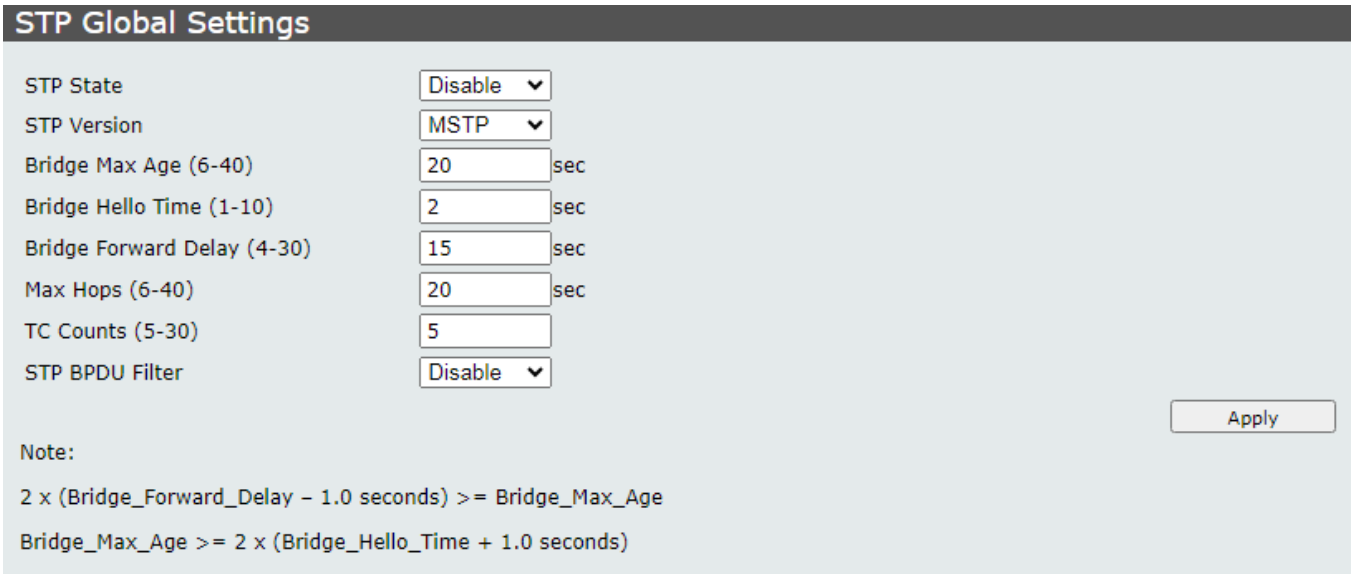
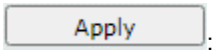


Figure 4-9-5: STP Global Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **STP State**	This column provides configuring enable or disable the spanning tree function.
• **STP Version**	This column provides selecting the spanning tree operation version; the default version is MSTP and available options are **STP**, **RSTP** and **MSTP**.
• **Bridge Max Age (6-40)**	This column provides configuring the value for Bridge Max Age; the default value is 20 seconds and the available range is **6** to **40** seconds.
• **Bridge Hello Time (1-10)**	This column provides configuring the value for Bridge Hello Time; the default value is 2 seconds and the available range is **1** to **10** seconds.
• **Bridge Forward Delay (4-30)**	This column provides configuring the value for Bridge Forward Delay; the default value is 15 seconds and the available range is **4** to **30** seconds.
• **Max Hops (6-40)**	This column provides configuring the value for Max Hops; the default value is 20 seconds and the available range is **6** to **40** seconds.
• **TC Counters (5-30)**	This column provides configuring the value for TC Counters; the default value is 5 and the available range is 5 to 30.
• **STP BPDU Filter**	This column provides configuring enable or disable the spanning BPDU Filter function.

Button



: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.1.2 STP Port Settings

This page allows you to configure the STP Port settings for Managed PoE+ Switch as the screen in Figure 4-9-6 appears.

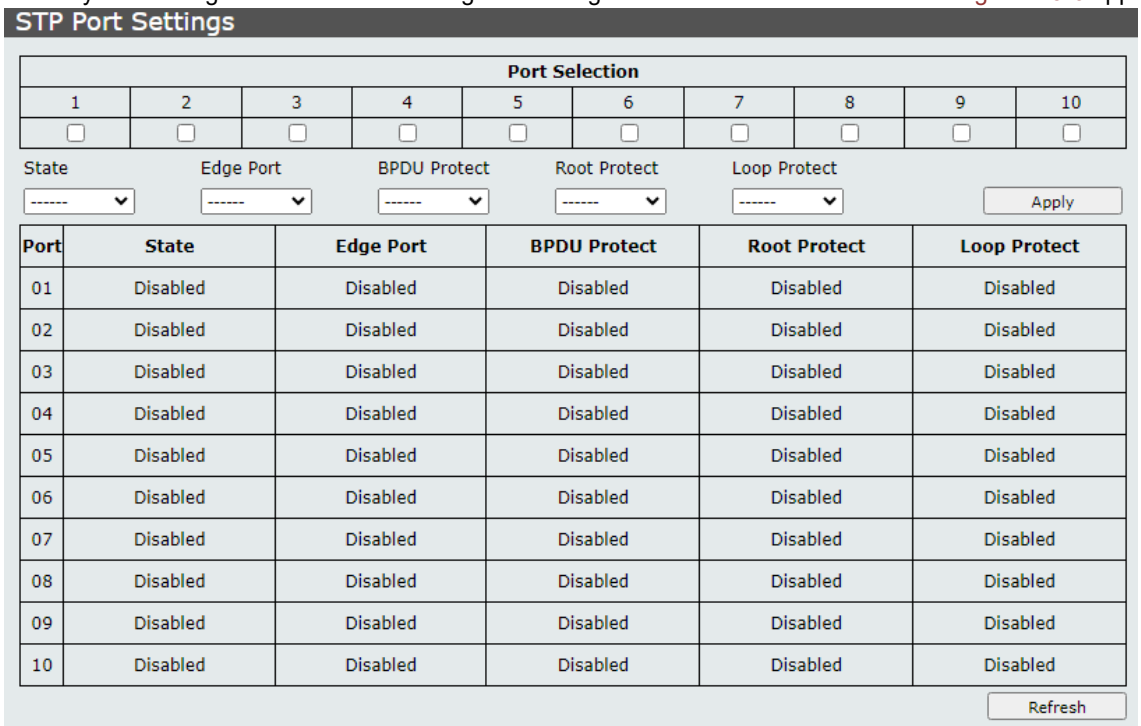


Figure 4-9-6: STP Port Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Selection**	Select specific port for further configuration.
• **State**	This column provides configuring enable or disable the spanning tree function on specific port; the default mode is Disable. Also display current status of per port.
• **Edge Port**	This column provides configuring enable or disable the Edge Port function on specific port; the default mode is Disable. Also display current status of per port.
• **BPDU Protect**	This column provides configuring enable or disable the BPDU Protect function on specific port; the default mode is Disable. Also display current status of per port.
• **Root Protect**	This column provides configuring enable or disable the Root Protect function on specific port; the default mode is Disable. Also display current status of per port.
• **Loop Protect**	This column provides configuring enable or disable the Loop Protect function on specific port; the default mode is Disable. Also display current status of per port.
• **Port**	Display per port list.

Buttons

Apply: press this button to confirm the changes.

Refresh: press this button to refresh current status.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.1.3 MST Configuration Identification

This page allows you to configure the MST Configuration Identification settings for Managed PoE+ Switch as the screen in Figure 4-9-7 appears.

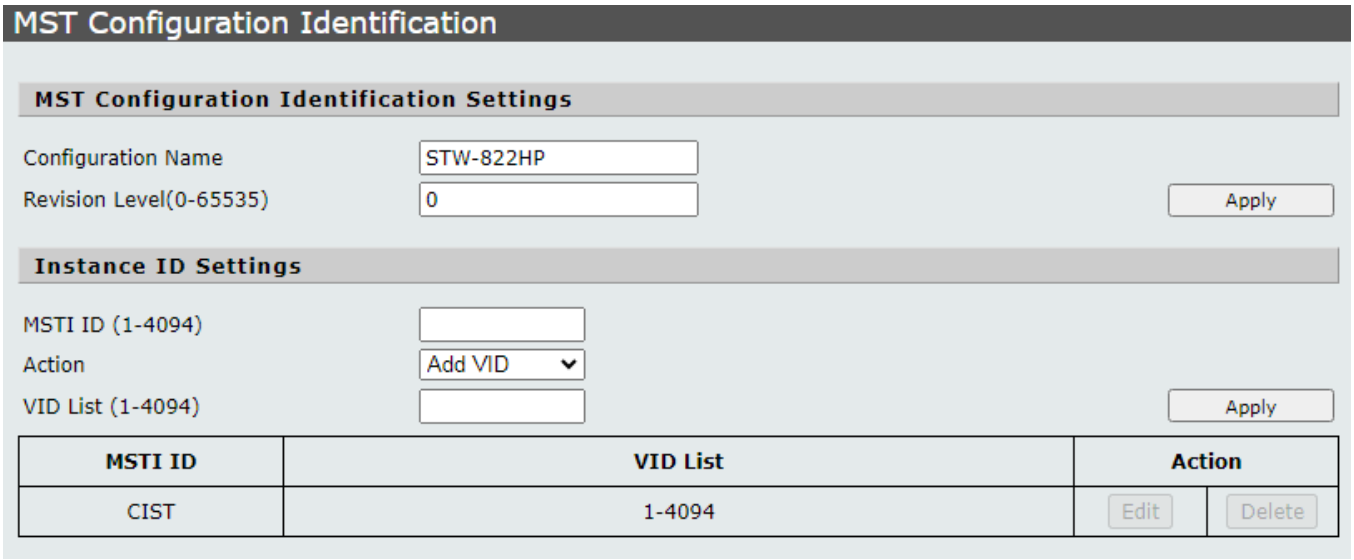


Figure 4-9-7: MST Configuration Identification Configuration Page Screenshot

The page includes the following fields:

Object	Description
MST Configuration Identification Settings	
• **Configuration Name**	This column provides configuring the configuration name and the available characters is 32.
• **Revision Level**	This column provides configuring the Revision Level settings and the available range is **0** to **65535**.
Instance ID Settings	
• **MSTI ID (1-4094)**	This column provides configuring the MSTI ID settings and the available range is **1** to **4094**.
• **Action**	This column provides selecting the Action of MSTI; the default version is Add VID and available options are **Add VID** and **Remove VID**.
• **VID List (1-4094)**	This column provides configuring the VID List settings f MSTI; the available VID range is **1** to **4094**.
• **MTSI ID**	Display MSTI ID information.
• **VID List**	Display VID List information.
• **Action**	Edit: press this button to edit specific Instance ID Settings. Delete: press this button to delete specific Instance ID Settings.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.1.4 STP Instance Settings

This page allows you to configure the STP Instance settings for Managed PoE+ Switch as the screen in Figure 4-9-8 appears.

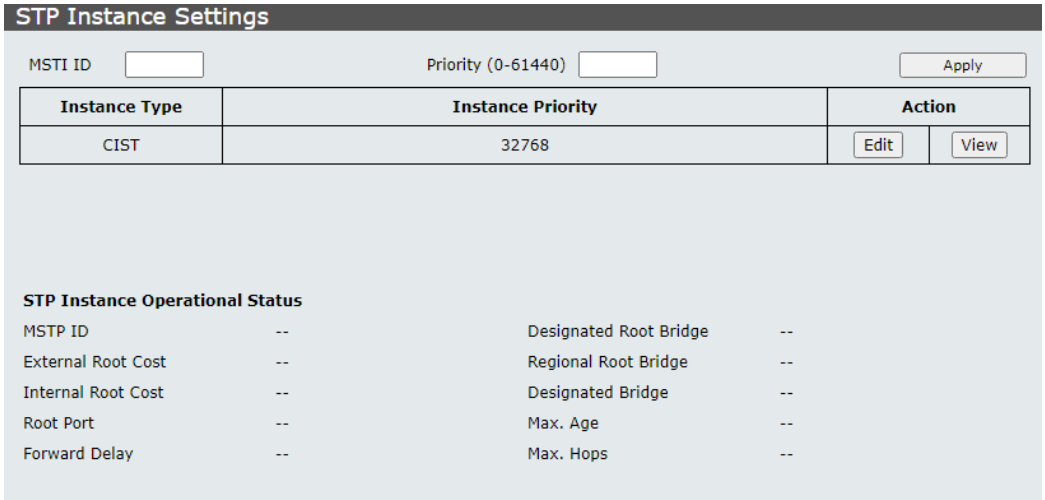


Figure 4-9-8: STP Instance Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **MSTI ID**	This column provides configuring the MSTI ID settings.
• **Priority**	This column provides configuring the Priority settings and the available range is **0** to **61440**.
• **Instance Type**	Display the instance type information.
• **Instance Priority**	Display the instance priority information.
• **Action**	Edit: press this button to edit specific Instance ID Settings. View: press this button to view STP Instance operational status.
STP Instance Operational Status	
• **MSTP ID**	Display MSTP ID information.
• **External Root Cost**	Display External Root Cost information.
• **Internal Root Cost**	Display Internal Root Cost information.
• **Root Port**	Display Root Port information.
• **Forward Delay**	Display Forward Delay information.
• **Designated Root Bridge**	Display Designated Root Bridge information.
• **Regional Root Bridge**	Display Regional Root Bridge information.
• **Designated Bridge**	Display Designated Bridge information.
• **Max. Age**	Display Max. Age information.
• **Max. Hops**	Display Max. Hops information.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.1.5 MSTP Port Information

This page allows you to configure the MSTP Port Information settings for Managed PoE+ Switch as the screen in Figure 4-9-9 appears.

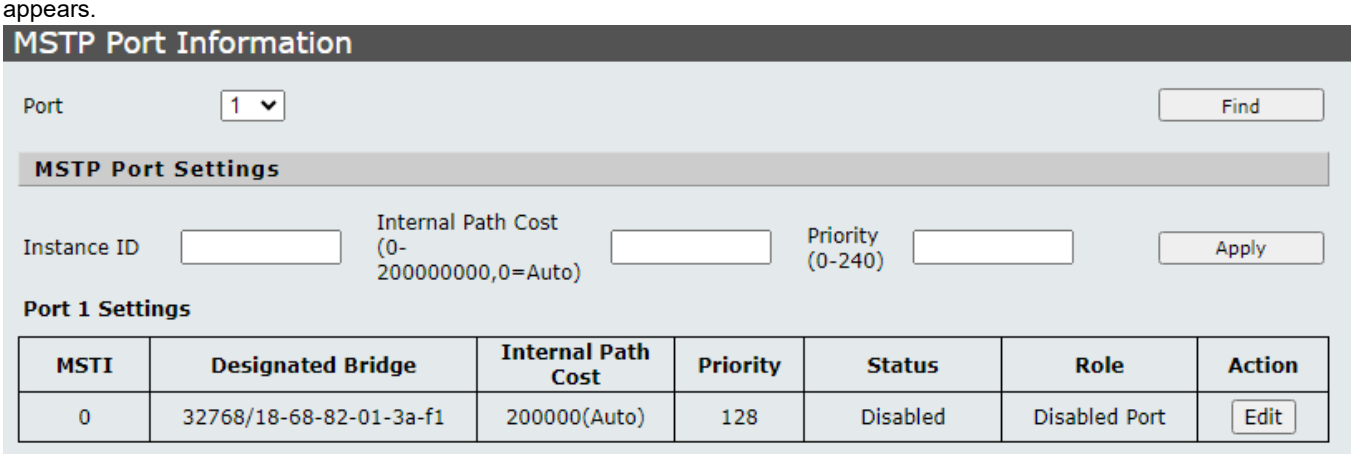


Figure 4-9-9: MSTP Port Information Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	Select specific port for further configuration.
MSTP Port Settings	
• **Instance ID**	This column provides configuring the Instance ID settings.
• **Internal Path Cost** • **(0-200000000,0=Auto)**	This column provides configuring the Internal Path Cost settings; the available range is **0** to **200000000, 0=Auto**.
• **Priority** • **(0-240)**	This column provides configuring the Priority settings; the available VID range is **0** to **240**.
• **MTSI**	Display MSTI information.
• **Designated Bridge**	Display Designated Bridge information.
• **Internal Path Cost**	Display Internal Path Cost information.
• **Priority**	Display Priority information.
• **Status**	Display Status information.
• **Role**	Display Role information.
• **Action**	Edit: press this button to edit specific MSTP Port Settings.

Buttons

Find: press this button to find MSTP Port information.

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.1.6 STP Loop Detect Settings

This page allows you to configure the STP Loop Detect settings for Managed PoE+ Switch as the screen in Figure 4-9-10 appears.

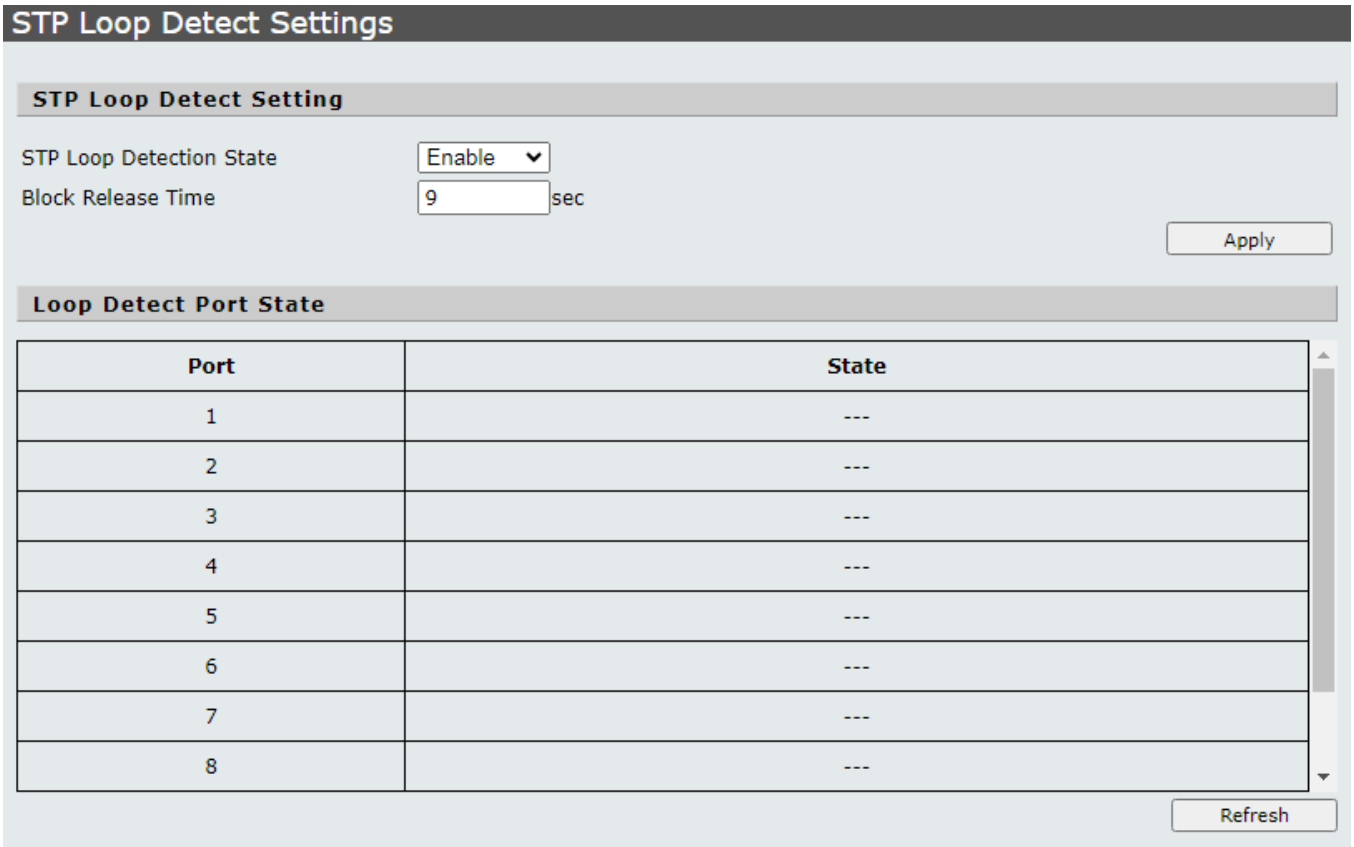


Figure 4-9-10: STP Loop Detect Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
STP Loop Detect Setting	
• **SFP Loop Detection State**	This column provides configuring enable or disable the SFP Loop Detection State function on specific port; the default mode is Enable.
• **Block Release Time**	This column providesconfiguring the Block Release Time settings; the available range is **1** to **255**.
Loop Detect Port State	
• **Port**	Display per port list.
• **State**	Display per port state information.

Buttons

Apply: press this button to confirm the changes.

Refresh: press this button to refresh current status.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.2 Trunk & Link Aggregation

Theory

Port Aggregation optimizes port usage by linking a group of ports together to form a single Link Aggregated Groups (LAGs). Port Aggregation multiplies the bandwidth between the devices, increases port flexibility, and provides link redundancy.

Each LAG is composed of ports of the same speed, set to full-duplex operations. Ports in a LAG, can be of different media types (UTP/Fiber, or different fiber types), provided they operate at the same speed.

Aggregated Links can be assigned manually (**Port Trunk**) or automatically by enabling Link Aggregation Control Protocol (**LACP**) on the relevant links.

Aggregated Links are treated by the system as a single logical port. Specifically, the Aggregated Link has similar port attributes to a non-aggregated port, including auto-negotiation, speed, Duplex setting, etc.

The device supports the following Aggregation links :

- **Static LAGs** (**Port Trunk**) – Force aggregared selected ports to be a trunk group.
- **Link Aggregation Control Protocol** (**LACP**) LAGs - LACP LAG negotiate Aggregated Port links with other LACP ports located on a different device. If the other device ports are also LACP ports, the devices establish a LAG between them.

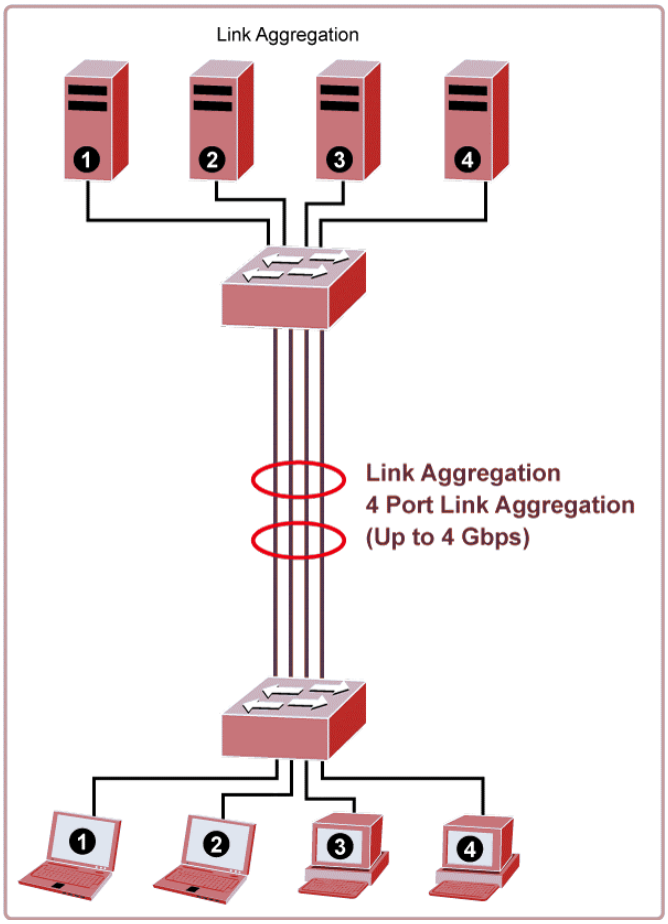


Figure 4-9-11: Link Aggregation

SEC.RU | Короткий путь к информации
Скачано с sec.ru

SEC.RU | Короткий путь к информации
Скачано с sec.ru

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

Port link aggregations can be used to increase the bandwidth of a network connection or to ensure fault recovery. Link aggregation lets you group up to 4 consecutive ports into a single dedicated connection between any two the Switch or other Layer 2 switches. However, before making any physical connections between devices, use the Link aggregation Configuration menu to specify the link aggregation on the devices at both ends. When using a port link aggregation, note that:

- The ports used in a link aggregation must all be of the same media type (RJ45, 100 Mbps fiber).
- The ports that can be assigned to the same link aggregation have certain other restrictions (see below).
- Ports can only be assigned to one link aggregation.
- The ports at both ends of a connection must be configured as link aggregation ports.
- None of the ports in a link aggregation can be configured as a mirror source port or a mirror target port.
- All of the ports in a link aggregation have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- The Spanning Tree Protocol will treat all the ports in a link aggregation as a whole.
- Enable the link aggregation prior to connecting any cable between the switches to avoid creating a data loop.
- Disconnect all link aggregation port cables or disable the link aggregation ports before removing a port link aggregation to avoid creating a data loop.

It allows a maximum of 10 ports to be aggregated at the same time. The Managed PoE+ Switch support Gigabit Ethernet ports (up to 5 groups). If the group is defined as a LACP static link aggregation group, then any extra ports selected are placed in a standby mode for redundancy if one of the other ports fails. If the group is defined as a local static link aggregation group, then the number of ports must be the same as the group member ports.

The aggregation code ensures that frames belonging to the same frame flow (for example, a TCP connection) are always forwarded on the same link aggregation member port. Recording of frames within a flow is therefore not possible. The aggregation code is based on the following information:

- **Source MAC**
- **Destination MAC**
- **Source and destination IPv4 address.**
- **Source and destination TCP/UDP ports for IPv4 packets**

Normally, all 5 contributions to the aggregation code should be enabled to obtain the best traffic distribution among the link aggregation member ports. Each link aggregation may consist of up to 10 member ports. Any quantity of link aggregation s may be configured for the device (only limited by the quantity of ports on the device.) To configure a proper traffic distribution, the ports within a link aggregation must use the same link speed.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

This page allows you to configure the Trunk & Link Aggregation settings for Managed PoE+ Switch as the screen in Figure 4-9-12 appears.

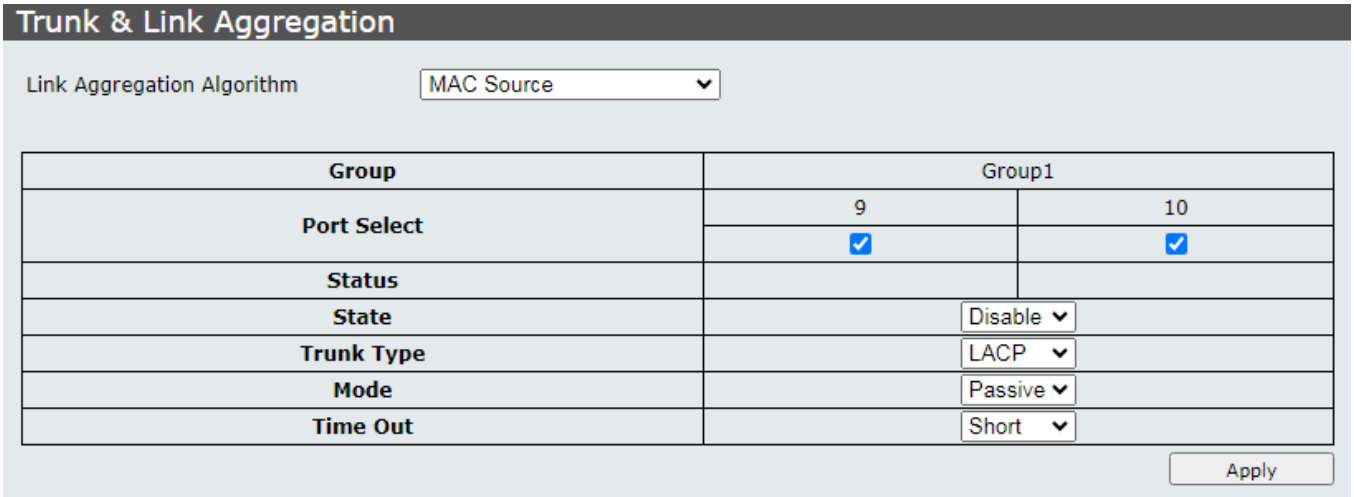
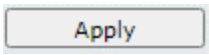


Figure 4-9-12: Trunk & Link Aggregation Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Link Aggregation Algorithm**	This column provides configuring Link Aggregation Algorithm and default is MAC Source, the available options are shown below: **Port** **MAC Source** **MAC Destination** **MAC Source Destination** **IP Source** **IP Destination** **TCP/UDP Destination Port** **TCP/UDP Source Port**
• **Group**	Display Trunk & Link Aggregation group information.
• **Port Select**	This column provides configuring and selecting the port for Trunk & Link Aggregation.
• **Status**	Display Trunk & Link Aggregation member port status.
• **State**	This column provides configuring enable or disable the Trunk & Link Aggregation function on specific port; the default mode is Disable.
• **Trunk Type**	This column provides configuring and selecting the Trunk type for Trunk & Link Aggregation function; the default mode is LACP and available options are **Static** and **LACP**.
• **Mode**	This column provides configuring and selecting the Trunk mode for Trunk & Link Aggregation function; the default mode is Passive and available options are **Active** and **Passive**.
• **Time Out**	This column provides configuring and selecting the Time Out for Trunk & Link Aggregation function; the default mode is Short and available options are **Short** and **Long**.

Button



: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.3 IGMP Snooping

Theory

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

About the Internet Group Management Protocol (IGMP) Snooping

Computers and network devices that want to receive multicast transmissions need to inform nearby routers that they will become members of a multicast group. The **Internet Group Management Protocol (IGMP)** is used to communicate this information. IGMP is also used to periodically check the multicast group for members that are no longer active. In the case where there is more than one multicast router on a sub network, one router is elected as the 'queried'. This router then keeps track of the membership of the multicast groups that have active members. The information received from IGMP is then used to determine if multicast packets should be forwarded to a given sub network or not. The router can check, using IGMP, to see if there is at least one member of a multicast group on a given subnet work. If there are no members on a sub network, packets will not be forwarded to that sub network.

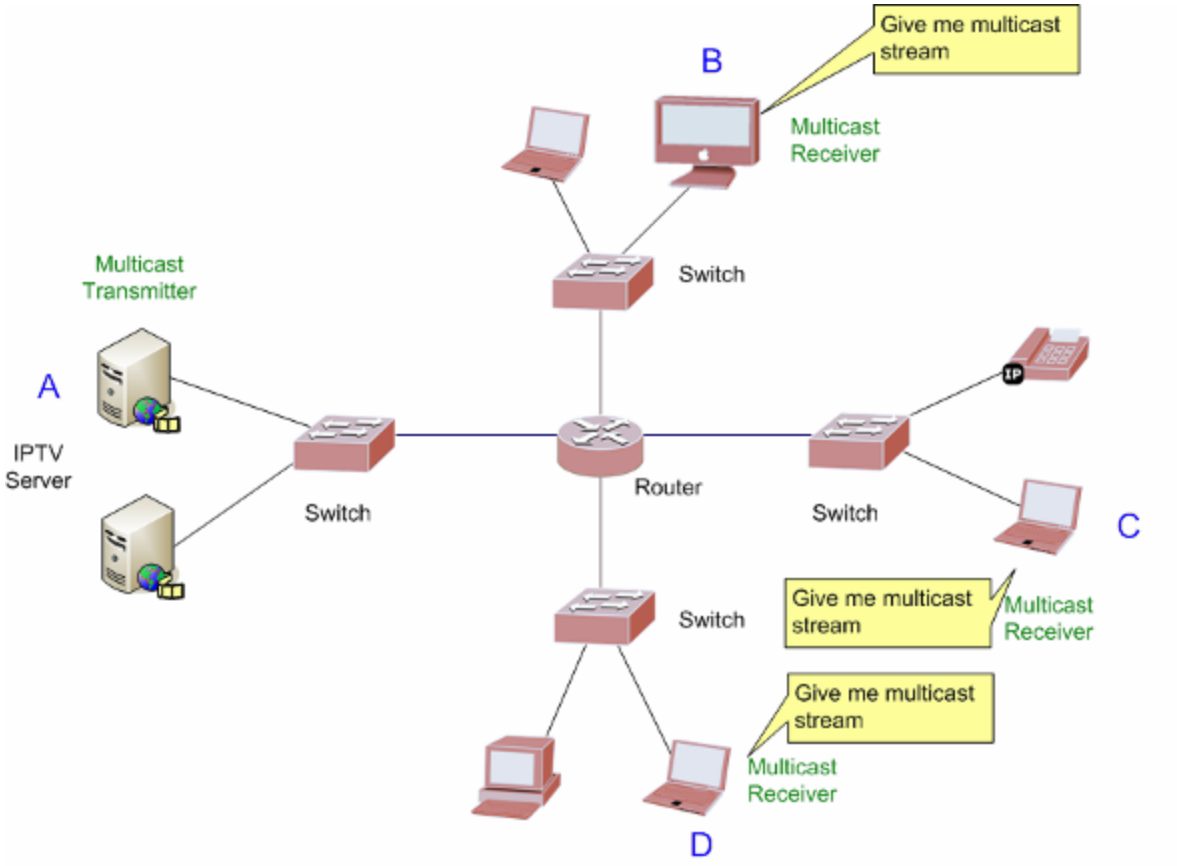


Figure 4-9-13: Multicast Service

SEC.RU | Короткий путь к информации
Скачано с sec.ru

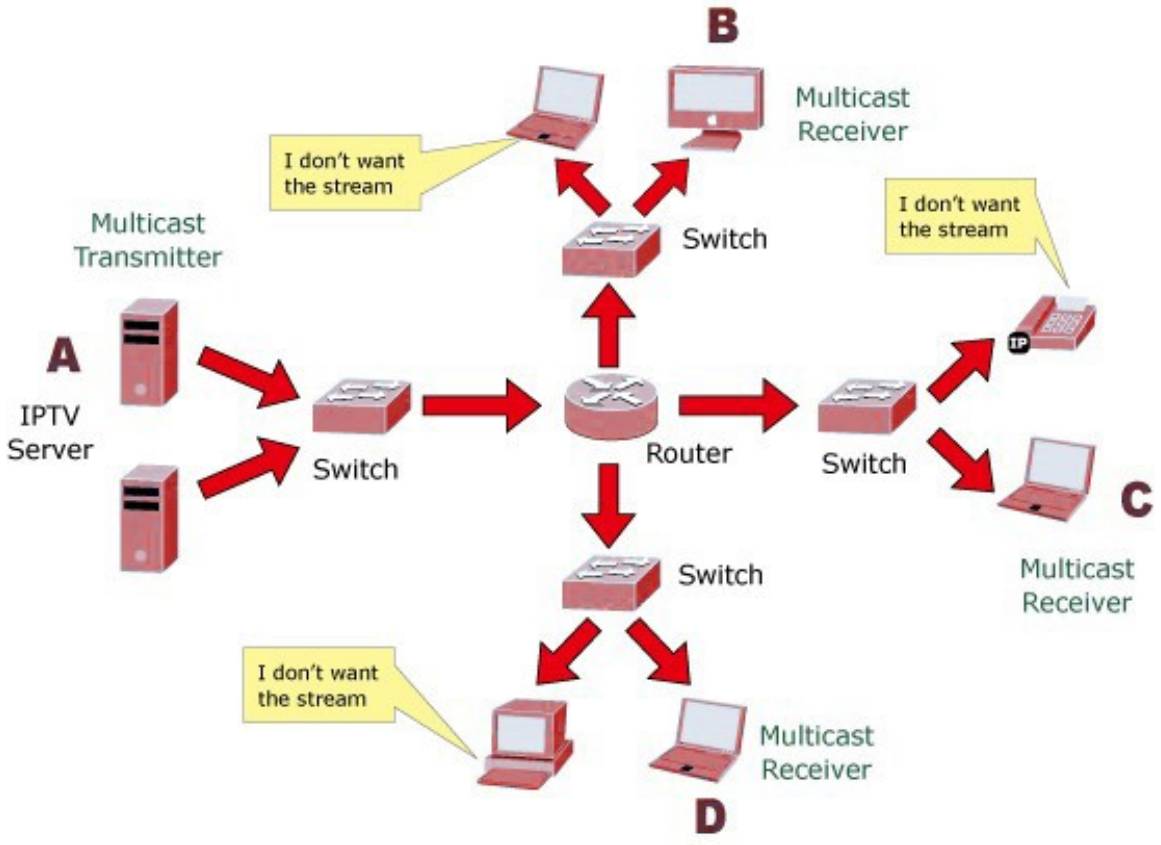


Figure 4-9-14: Multicast Flooding

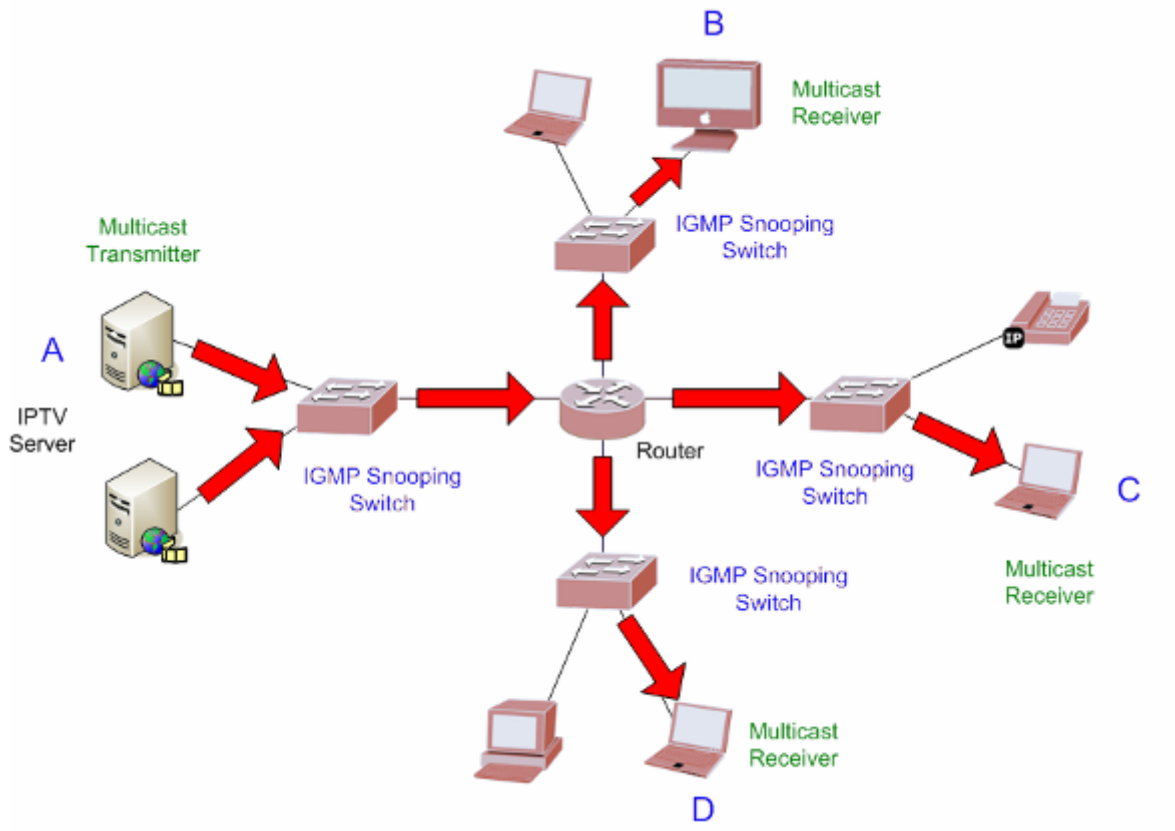


Figure 4-9-15: IGMP Snooping Multicast Stream Control

SEC.RU | Короткий путь к информации
Скачано с sec.ru

IGMP Versions 1 and 2

Multicast groups allow members to join or leave at any time. IGMP provides the method for members and multicast routers to communicate when joining or leaving a multicast group.

IGMP version 1 is defined in RFC 1112. It has a fixed packet size and no optional data.

The format of an IGMP packet is shown below:

IGMP Message Format

Octets

0	8	16	31
Type	Response Time	Checksum	
Group Address (all zeros if this is a query)			

The IGMP Type codes are shown below:

Type	Meaning
0x11	Membership Query (if Group Address is 0.0.0.0)
0x11	Specific Group Membership Query (if Group Address is Present)
0x16	**Membership Report (version 2)**
0x17	**Leave a Group (version 2)**
0x12	**Membership Report (version 1)**

IGMP packets enable multicast routers to keep track of the membership of multicast groups, on their respective sub networks. The following outlines what is communicated between a multicast router and a multicast group member using IGMP.

A host sends an IGMP **"report"** to join a group

A host will never send a report when it wants to leave a group (for version 1).

A host will send a **"leave"** report when it wants to leave a group (for version 2).

Multicast routers send IGMP queries (to the all-hosts group address: 224.0.0.1) periodically to see whether any group members exist on their sub networks. If there is no response from a particular group, the router assumes that there are no group members on the network.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

The Time-to-Live (TTL) field of query messages is set to 1 so that the queries will not be forwarded to other sub networks.

IGMP version 2 introduces some enhancements such as a method to elect a multicast queried for each LAN, an explicit leave message, and query messages that are specific to a given group.

The states a computer will go through to join or to leave a multicast group are shown below:

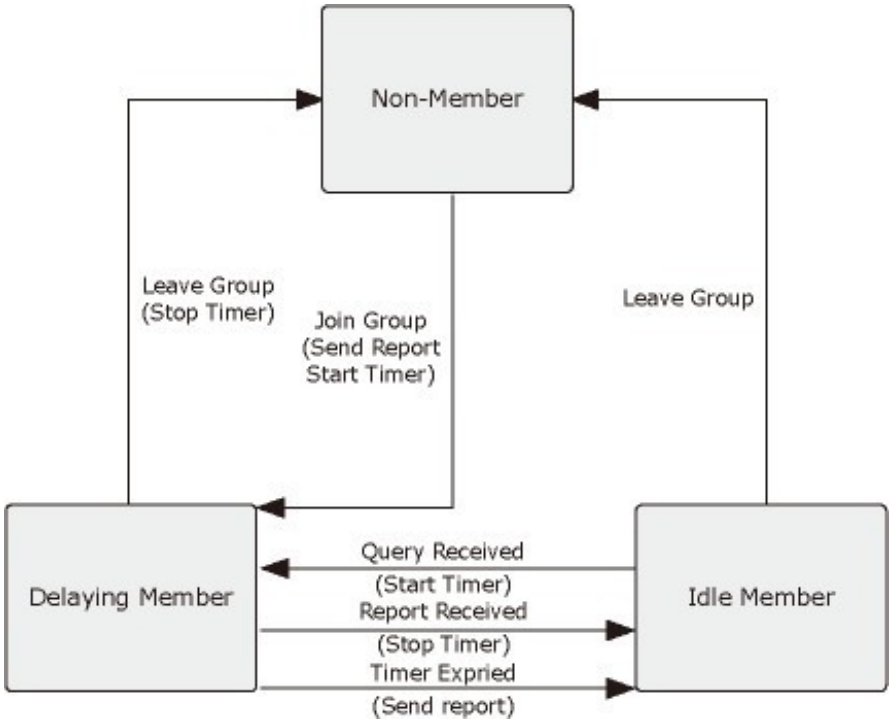


Figure 4-9-16: IGMP State Transitions

- **IGMP Querier –**

A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "**querier**" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Note

Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.3.1 IGMP Snooping Settings

This page allows you to configure the IGMP Snooping settings for Managed PoE+ Switch as the screen in Figure 4-9-17 appears.

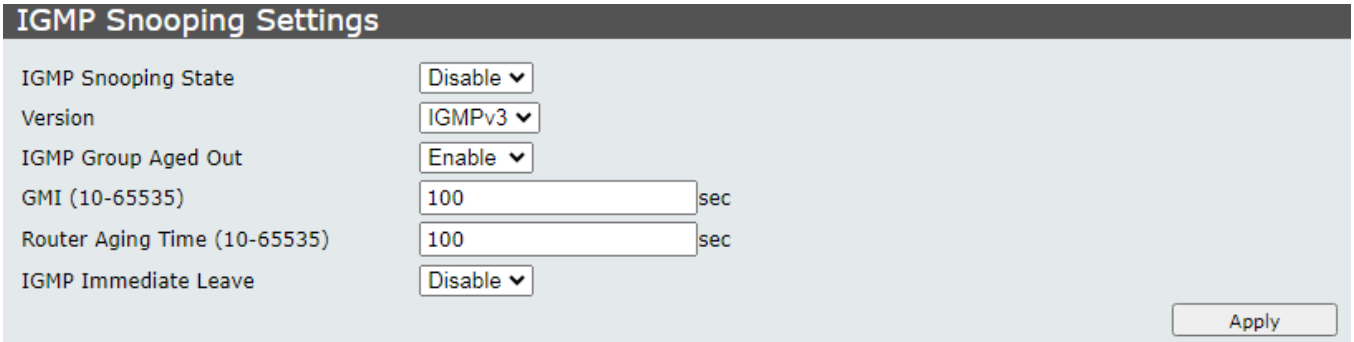


Figure 4-9-17: IGMP Snooping Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **IGMP Snooping State**	This column provides configuring enable or disable the IGMP Snooping function.
• **Version**	This column provides selecting the IGMP Snooping operation version; the default version is IGMPv3 and available options are **IGMPv1**, **IGMPv2** and **IGMPv3**.
• **IGMP Group Aged Out**	This column provides configuring enable or disable the IGMP Group Aged Out function.
• **GMI (10-65535)**	This column provides configuring the value for Group Member Interval Time; the default value is 100 seconds and the available range is **10** to **65535** seconds. After the dynamic Group is established, the time is used to ask if there is member.
• **Router Aging Time (10-65535)**	This column provides configuring the value for Router Aging Time; the default value is 100 seconds and the available range is **10** to **65535** seconds. The time the dynamic Router Port exists, and if the Query packet is not continuously received, the dynamic Router Port clears.
• **IGMP Immediate Leave**	This column provides configuring enable or disable the IGMP Immediate Leave function.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.3.2 IGMP Snooping Router Ports Settings

This page allows you to configure the IGMP Snooping Router Ports settings for Managed PoE+ Switch as the screen in Figure 4-9-18 appears.

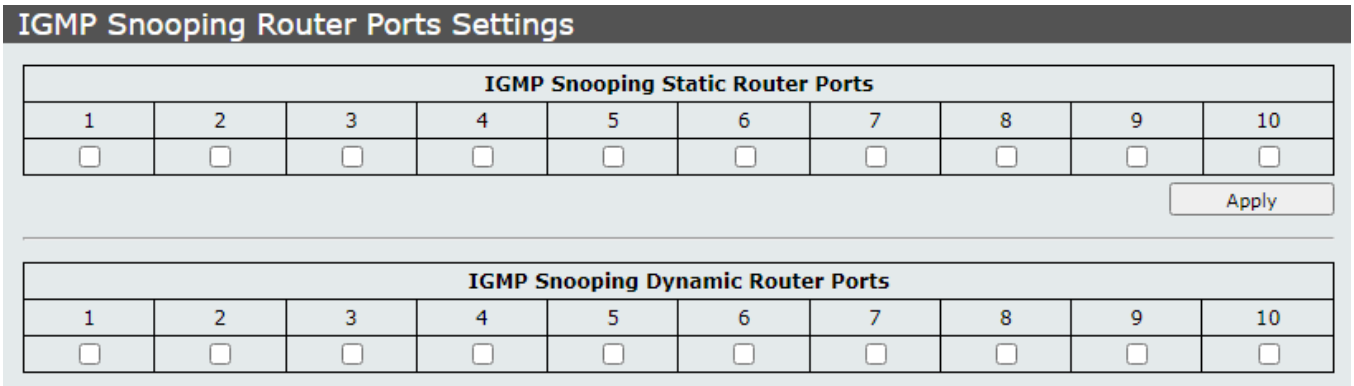


Figure 4-9-18: IGMP Snooping Router Ports Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **IGMP Snooping Static Router Ports**	This column provides configuring the IGMP Snooping Static Router Ports.
• **IGMP Snooping Dynamic Router Ports**	This column provides configuring them IGMP Snooping Dynamic Router Ports.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.3.3 IGMP Snooping Groups

This page allows you to configure the IGMP Snooping Groups settings for Managed PoE+ Switch as the screen in Figure 4-9-19 appears.

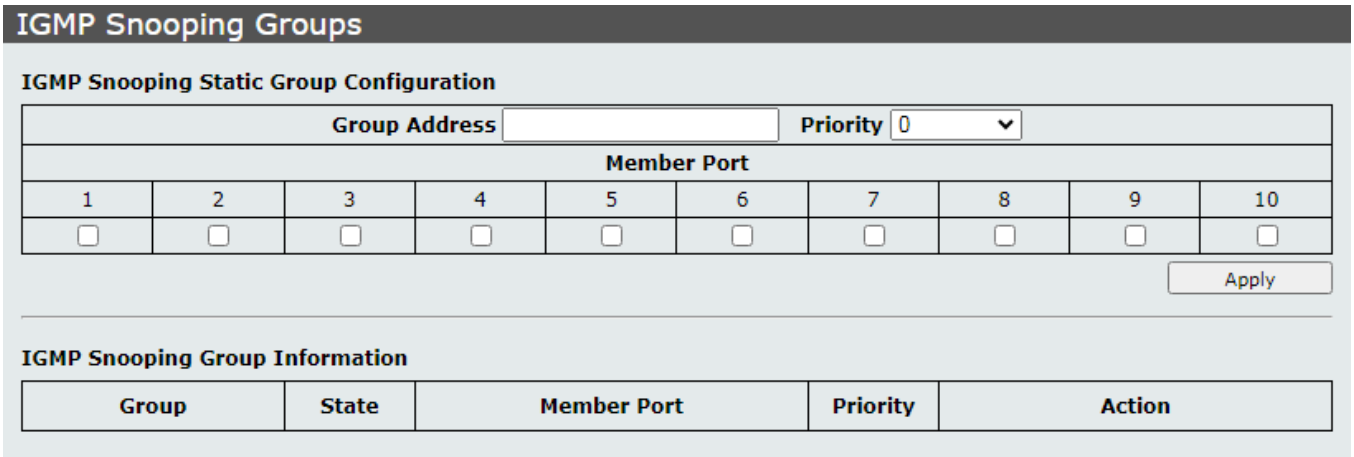


Figure 4-9-19: IGMP Snooping Groups Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
IGMP Snooping Static Group Configuration	
• **Group Address**	This column provides configuring the Group Address.
• **Priority**	This column provides configuring the value for Priority, the default value is 0 and the available range is **0** to **7**.
• **Member Port**	This column provides configuring to select specific ports for IGMP Snooping Groups settings.
IGMP Snooping Group Information	
• **Group**	Display per group list.
• **State**	Display per group status.
• **Member Port**	Display per group member port status.
• **Priority**	Display per group priority status.
• **Action**	Edit: press this button to edit specific IGMP Snooping Groups Settings. Delete: press this button to delete specific IGMP Snooping Groups Settings.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.3.4 IGMP Snooping Ports

This page allows you to configure the IGMP Snooping Groups settings for Managed PoE+ Switch as the screen in Figure 4-9-20 appears.

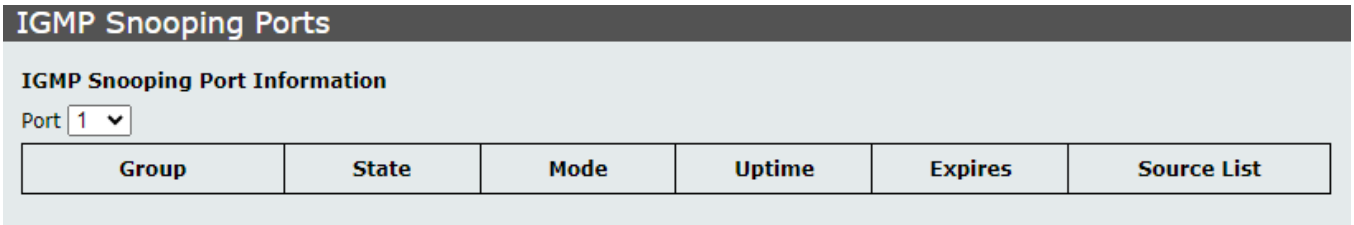


Figure 4-9-20: IGMP Snooping Groups Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
IGMP Snooping Port Information	
• **Port**	This column provides configuring to select specific ports for IGMP Snooping Ports settings.
• **Group**	Display per group list.
• **State**	Display per port status.
• **Mode**	Display per port status.
• **Uptime**	Display per port uptime status.
• **Expires**	Display per port expires status.
• **Source List**	Display per port source list status.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.4 MLD Snooping

4.9.4.1 MLD Snooping Settings

This page allows you to configure the MLD Snooping settings for Managed PoE+ Switch as the screen in Figure 4-9-21 appears.

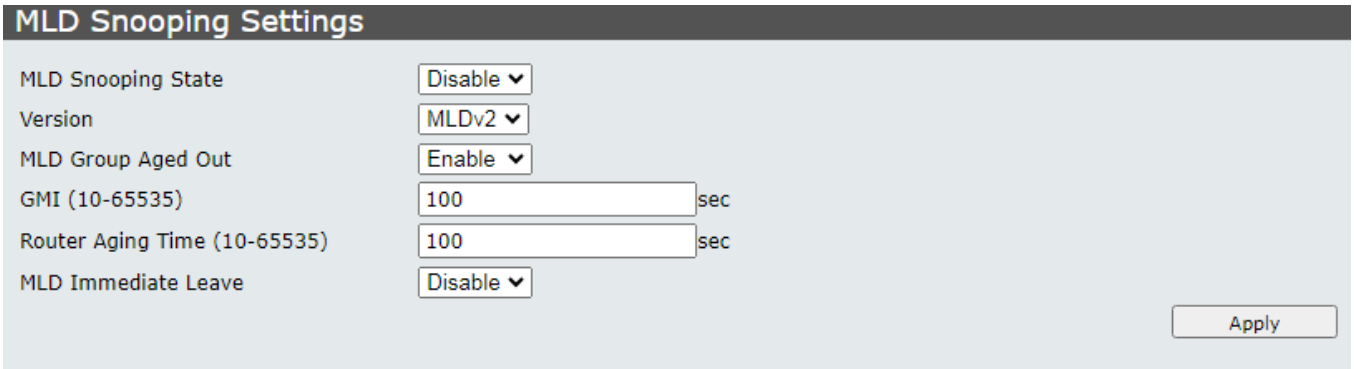
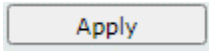


Figure 4-9-21: MLD Snooping Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **MLD Snooping State**	This column provides configuring enable or disable the MLD Snooping function.
• **Version**	This column provides selecting the IGMP Snooping operation version; the default version is MLDv2 and available options are **MLDv1** and **MLDv2**.
• **MLD Group Aged Out**	This column provides configuring enable or disable the MLD Group Aged Out function.
• **GMI (10-65535)**	This column provides configuring the value for Group Member Interval Time; the default value is 100 seconds and the available range is **10** to **65535** seconds. After the dynamic Group is established, the time is used to ask if there is member.
• **Router Aging Time (10-65535)**	This column provides configuring the value for Router Aging Time; the default value is 100 seconds and the available range is **10** to **65535** seconds. The time the dynamic Router Port exists, and if the Query packet is not continuously received, the dynamic Router Port clears.
• **MLD Immediate Leave**	This column provides configuring enable or disable the MLD Immediate Leave function.

Button



: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.4.2 MLD Snooping Router Ports Settings

This page allows you to configure the MLD Snooping Router Ports settings for Managed PoE+ Switch as the screen in Figure 4-9-22 appears.

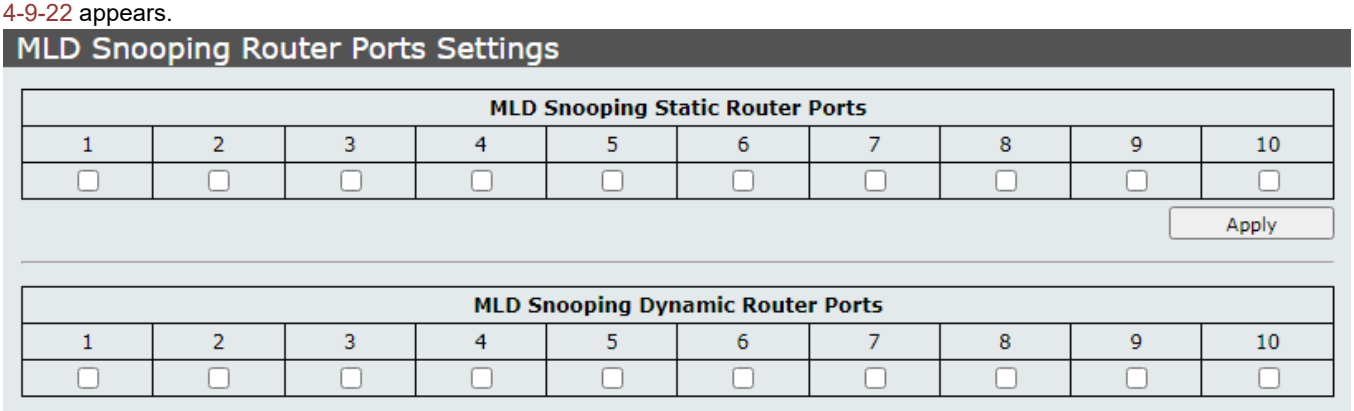
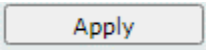


Figure 4-9-22: MLD Snooping Router Ports Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **MLD Snooping Static Router Ports**	This column provides configuring the MLD Snooping Static Router Ports.
• **MLD Snooping Dynamic Router Ports**	This column provides configuring them MLD Snooping Dynamic Router Ports.

Button



: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.4.3 MLD Snooping Groups

This page allows you to configure the MLD Snooping Groups settings for Managed PoE+ Switch; the screen in Figure 4-9-23 appears.

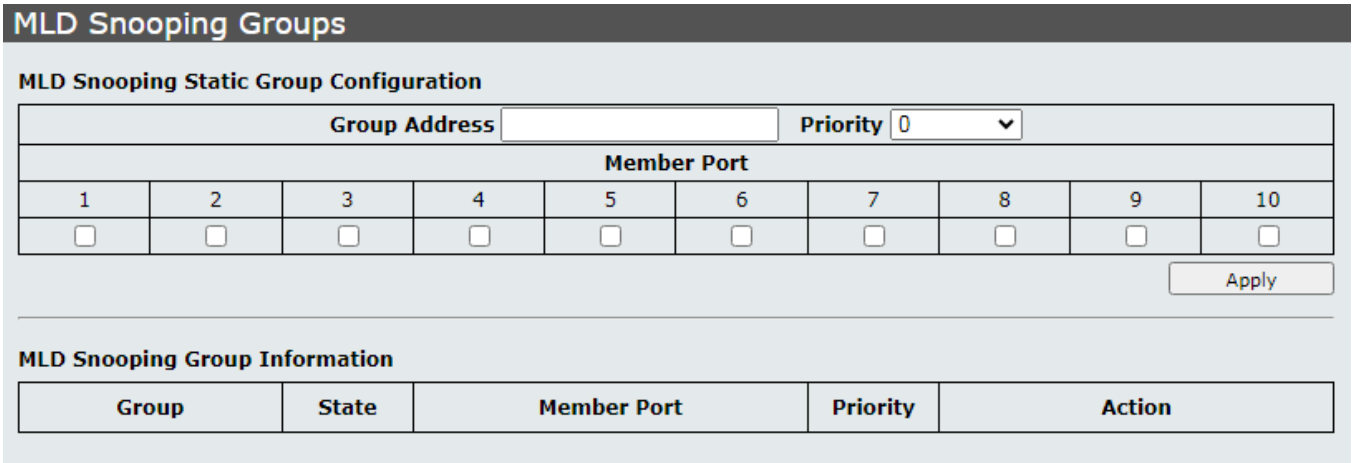


Figure 4-9-23: MLD Snooping Groups Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
MLD Snooping Static Group Configuration	
• **Group Address**	This column provides configuring the Group Address.
• **Priority**	This column provides configuring the value for Priority, the default value is 0 and the available range is **0** to **7**.
• **Member Port**	This column provides configuring to select specific ports for MLD Snooping Groups settings.
MLD Snooping Group Information	
• **Group**	Display per group list.
• **State**	Display per group status.
• **Member Port**	Display per group member port status.
• **Priority**	Display per group priority status.
• **Action**	Edit: press this button to edit specific MLD Snooping Groups Settings. Delete: press this button to delete specific MLD Snooping Groups Settings.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.4.4 MLD Snooping Ports

This page allows you to configure the MLD Snooping Groups settings for Managed PoE+ Switch as the screen in Figure 4-9-24 appears.

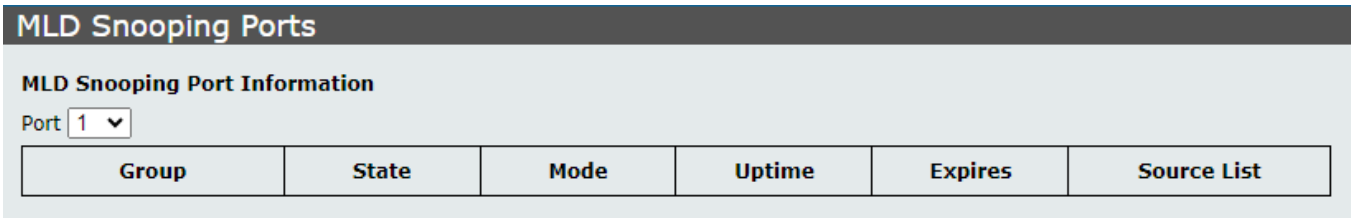


Figure 4-9-24: MLD Snooping Groups Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
MLD Snooping Port Information	
• **Port**	This column provides configuring to select specific ports for IGMP Snooping Ports settings.
• **Group**	Display per group list.
• **State**	Display per port status.
• **Mode**	Display per port status.
• **Uptime**	Display per port uptime status.
• **Expires**	Display per port expires status.
• **Source List**	Display per port source list status.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.5 DHCP Relay Agent

Configure DHCP Relay on this page. **DHCP Relay** is used to forward and transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The **DHCP option 82** enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options:

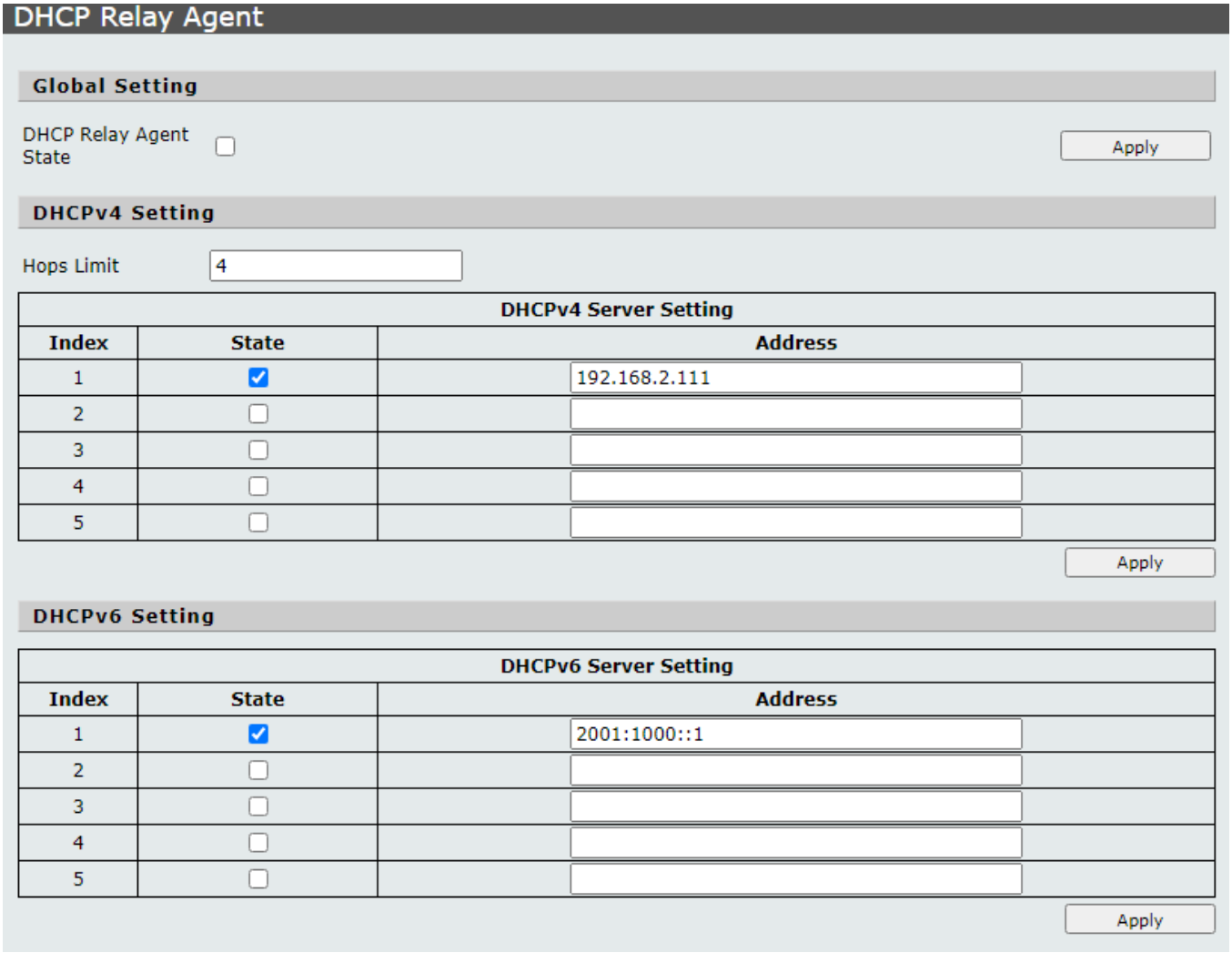
- **Circuit ID (option 1)**
- **Remote ID (option 2)**

The **Circuit ID** sub-option is supposed to include information specific to which circuit the request came in on.

The **Remote ID** sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes representing the VLAN ID. The parameter of "module_id" is the third byte for the module ID. The parameter of "port_no" is the fourth byte and it means the port number.

The Remote ID is 6 bytes in length, and the value equals the DHCP relay agent's MAC address. The DHCP Relay Agent Configuration screen in Figure 4-9-25 appears.



SEC.RU | Короткий путь к информации
Скачано с sec.ru

Figure 4-9-25: DHCP Relay Agent Settings Configuration Page Screenshot

SEC.RU | Короткий путь к информации
Скачано с sec.ru

The page includes the following fields:

Object	Description
Global Setting	
• **DHCP Relay Agent State**	Click to enable or disable the DHCP Relay Agent function.
DHCPv4 Setting	
• **Hops Limit**	This column provides configuring Hops Lmit settings, limit the number of times DHCP packets can be forwarded and the available range is **1** to **16**.
• **Index**	Display per index list (**1** to **5**).
• **State**	Click to enable or disable the per index function.
• **Address**	This column provides configuring the DHCPv4 server IP address.
DHCPv6 Setting	
• **Index**	Display per index list (**1** to **5**).
• **State**	Click to enable or disable the per index function.
• **Address**	This column provides configuring the DHCPv6 server IP address.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.6 Loop Detect

Configure Loop Detect on this page. **Loop Detect** is used to detects the loop connection generated on Managed PoE+ Switch, once detect the loop connection will block port to prevent loop connection affect Managed PoE+ Switch operation performance. The Loop Detect Configuration screen in Figure 4-9-26 appears.

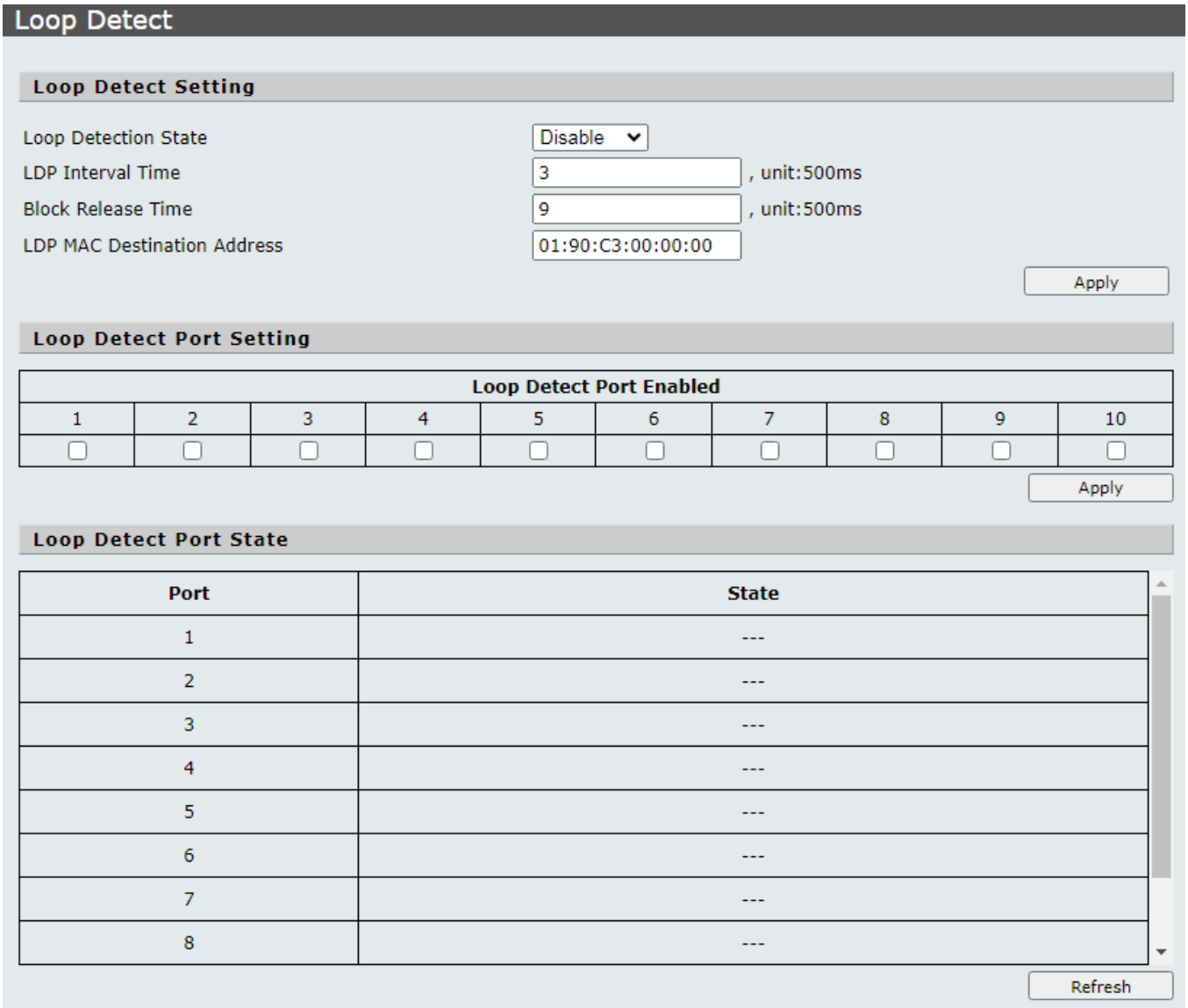


Figure 4-9-26: Loop Detect Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
Loop Detect Setting	
• **Loop Detection State**	This column provides configuring enable or disable the Loop Detection State function.
• **LDP Interval Time**	This column provides configuring LDP Interval Time settings, the default value is 3 and the available range is **1** to **255**. Unit is 500ms.
• **Block Release Time**	This column provides configuring Block Release Time settings, the default value is 9 and the available range is **1** to **255**. Unit is 500ms.
• **LDP MAC Destination Address**	This column provides configuring LDP MAC Destination Address settings.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Loop Detect Port Setting	
• **Loop Detect Port Enabled**	This column provides configuring to select specific port for Loop Detect Port Enabled settings.
Loop Detect Port State	
• **Port**	Display per port list.
• **State**	Display per port Loop Detect Port State.

Button

Apply: press this button to confirm the changes.

Refresh: press this button to refresh the port states.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.7 GVRP

On this page. **GVRP** (GARP VLAN Registration Protocol or Generic VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. The GVRP Configuration screen in Figure 4-9-27 appears.

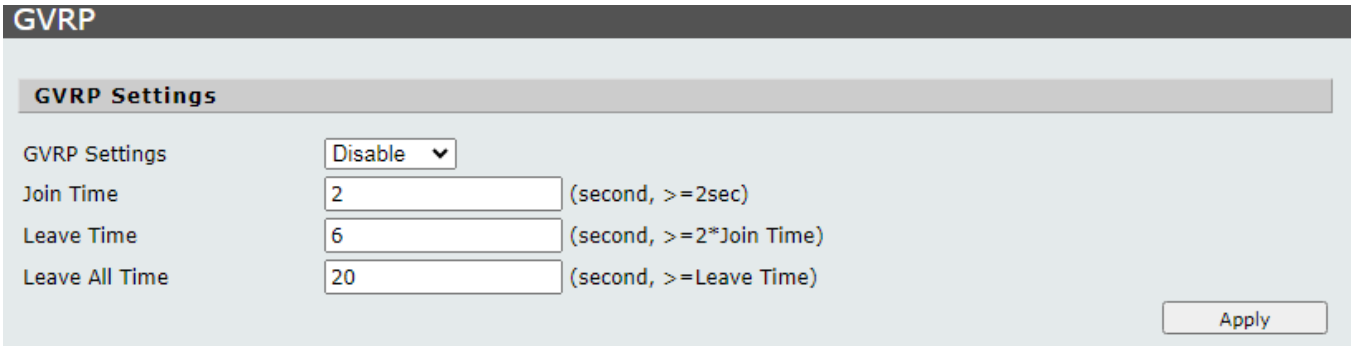
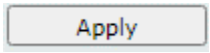


Figure 4-9-27: GVRP Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **GVRP Settings**	This column provides configuring enable or disable the GVRP function.
• **Join Time**	This column provides configuring Join Time settings; the default value is 2. The Join time must not be less than 2 seconds.
• **Leave Time**	This column provides configuring Leave Time settings; the default value is 6. The Leave time must not be less than 2 seconds.
• **Leave All Time**	This column provides configuring Leave All Time settings; the default value is 20. The Leave All time must not be less than Leave time.

Button



: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.8 Neighbor MAC ID Settings

On this page. **Neighbor MAC ID Settings** is used for searching for switch MAC Address ID from each port of Managed PoE+ Switch, according to send period setting for sending out the neighbor information packets. The Managed PoE+ Switch will add or update the MAC Address ID when receiving the neighbor information packets; also the switch neighbor MAC address ID information can be obtained by using the UDP NetCMD tools. The Neighbor MAC ID Settings Configuration screen in Figure 4-9-28 is shown below.

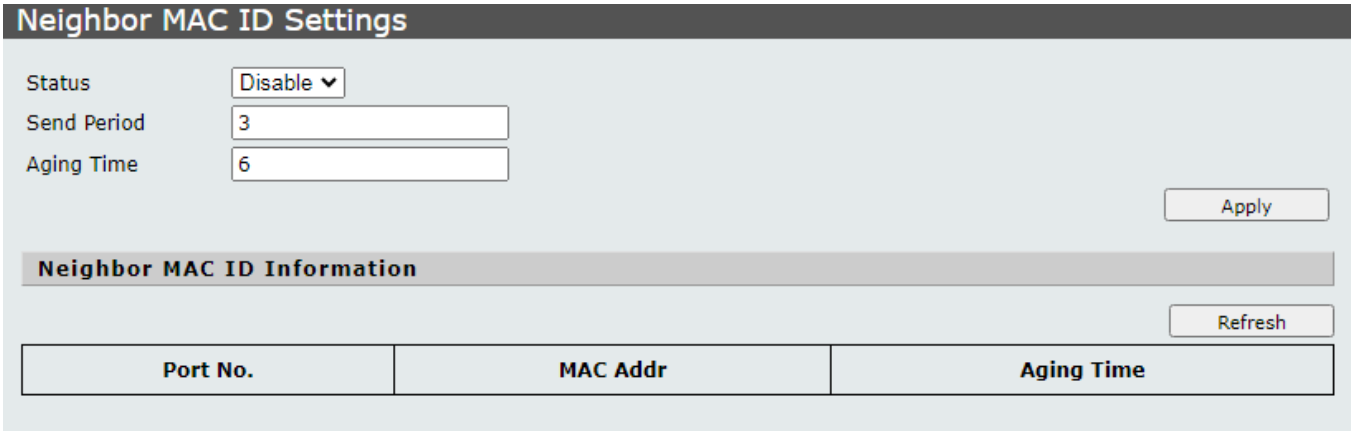


Figure 4-9-28: Neighbor MAC ID Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Status**	This column providesconfiguring enable or disable the Neighbor MAC ID settings function.
• **Send Period**	This column provides configuring Send Period settings; the default value is 3 and the available range is **1** to **65535**. Unit is second.
• **Aging Time**	This column provides configuring Aging Time settings; the default value is 6 and the available range is **1** to **65535**. Unit is second.
• **Neighbor MAC ID Information**	
• **Port No.**	Display the per port list.
• **MAC Add**	Display the MAC address from per port list.
• **Aging Time**	Display the Aging time from per port list.

Buttons

Apply: press this button to confirm the changes.

Refresh: press this button to refresh current status.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.9 Voice VLAN Setting

On this page. **Voice VLAN Setting** is enabled for voice traffic forwarding on the Voice VLAN. The Managed PoE+ Switch can classify and schedule network traffic. It is recommended that there be two VLANs on a port -- one for voice and one for data. Before connecting the IP device to the switch, the IP phone should configure the voice VLAN ID correctly. It should be configured through its own GUI. The Voice VLAN Setting configuration includes the Voice VLAN State, Voice VLAN Port Setting and OUI list. Table 4-9-3 shows the items of Voice VLAN Setting functions.

Voice VLAN Setting Configuration	
Item	**Description**
Voice VLAN State	Configure and display Voice VLAN State settings on this web page.
Voice VLAN Port Setting	Configure and display Voice VLAN Port Setting on this web page.
OUI List	Configure and display OUI List settings on this web page.

Table 4-9-3: Descriptions of Voice VLAN Setting Configuration

4.9.9.1 Voice VLAN State

This page allows you to configure the Voice VLAN State settings for Managed PoE+ Switch as the screen in Figure 4-9-29 appears.

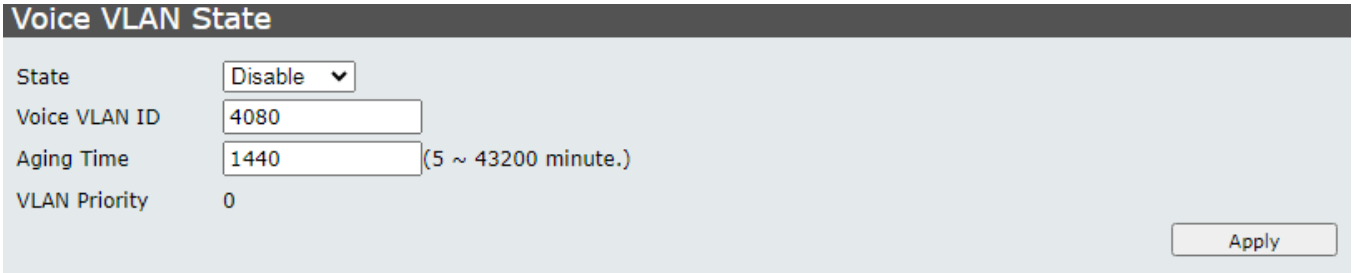


Figure 4-9-29: Voice VLAN State Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **State**	This column provides configuring enable or disable the Voice VLAN function.
• **Voice VLAN ID**	This column provides inputting the Voice VLAN ID; the default value is 4080.
• **Aging Time**	This column provides configuring the value for Bridge Max Age; the default value is 1440 minute and the available range is **5** to **43200** minute.
• **VLAN Priority**	This column provides displaying the VLAN priority information.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.9.2 Voice VLAN Port Setting

This page allows you to configure the Voice VLAN Port settings for Managed PoE+ Switch as the screen in Figure 4-9-30 appears.

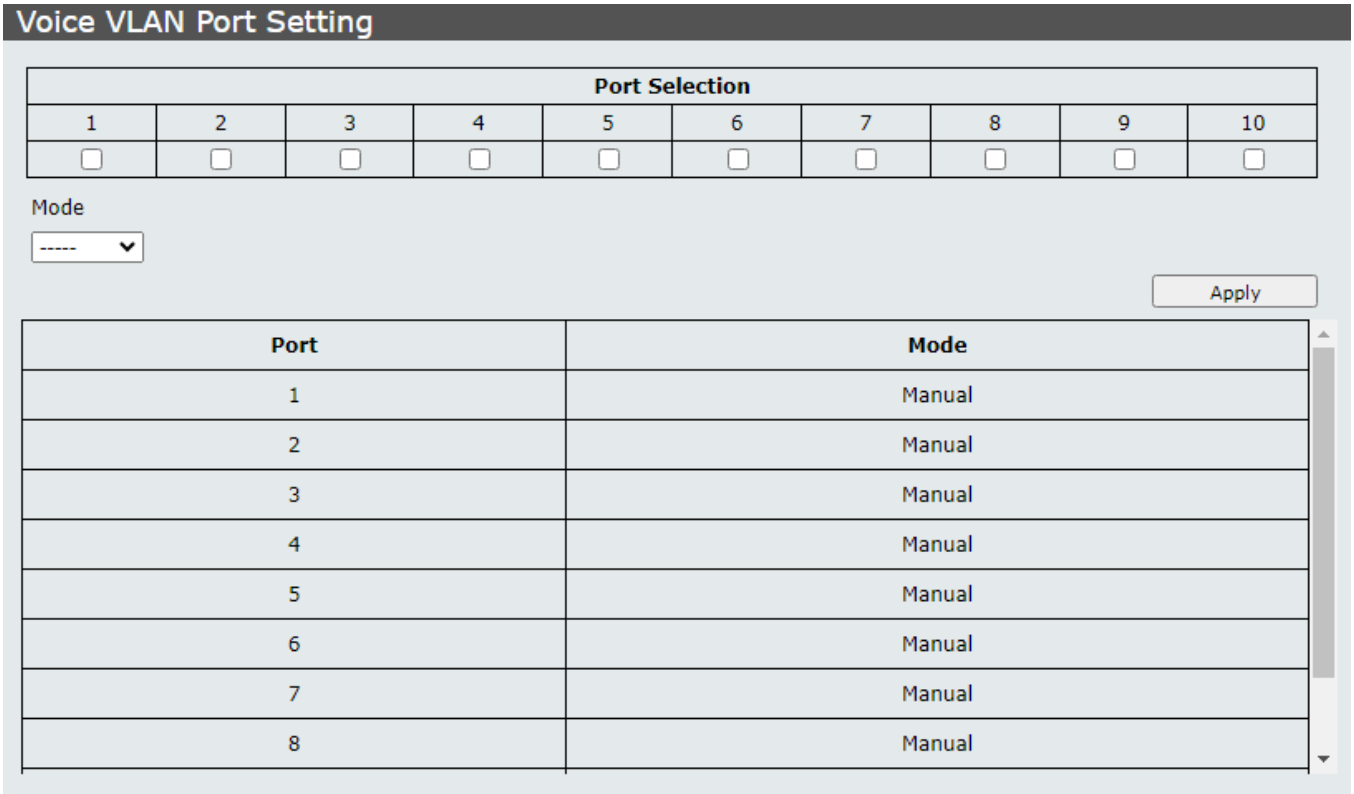


Figure 4-9-30: Voice VLAN Port Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Selection**	This column provides selecting specific port for Voice VLAN Port Settings function.
• **Mode**	This column provides automatically or manually configuring Voice VLAN Port Settings function.
• **Port**	Display per port list.
• **Mode**	Display per port Voice VLAN operation mode.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.9.3 OUI List

This page allows you to configure the Voice VLAN OUI settings for Managed PoE+ Switch as the screen in Figure 4-9-31 appears.

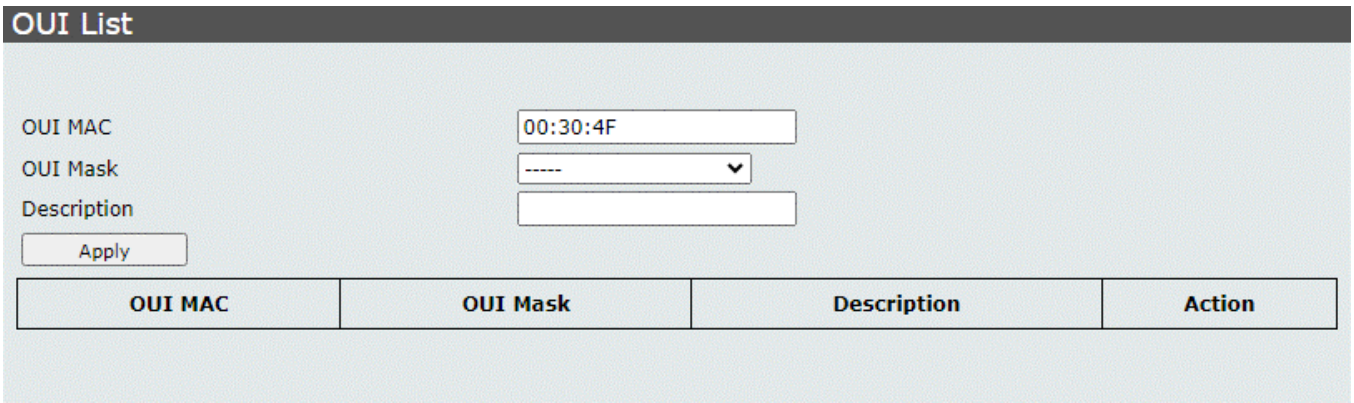


Figure 4-9-31: Voice VLAN OUI Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **OUI MAC**	This column provides configuring OUI MAC.
• **OUI Mask**	This column provides selecting the OUI Mask and the available options are : **FF:FF:FF:FF:FF:FF** **FF:FF:FF:00:00:00** **FF:FF:00:00:00:00**
• **Description**	This column provides configuring description of per OUI MAC address.
• **Action**	Delete: press this button to delete specific OUI List.

Button

Apply: press this button to confirm the changes.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.10 LLDP

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

The LLDP setting configuration includes the LLDP Global Setting, LLDP Port Setting and table 4-9-4 show the items of LLDP setting functions.

LLDP Configuration	
Item	**Description**
LLDP Global Setting	Configure and display LLDP Global Settings on this web page.
LLDP Port Setting	Configure and display LLDP Port Settings on this web page.

Table 4-9-4: Descriptions of LLDP Setting Configuration

4.9.10.1 LLDP Global Setting

This page allows you to configure the LLDP Global settings for Managed PoE+ Switch as the screen in Figure 4-9-32 appears.

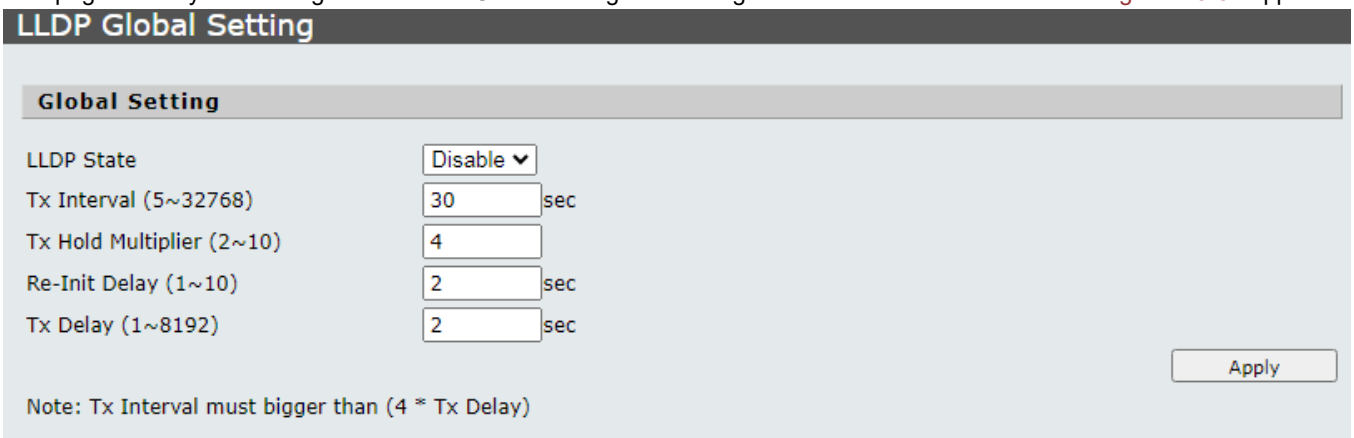


Figure 4-9-32: LLDP Global Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **LLDP State**	This column provides configuring enable or disable the LLDP function.
• **Tx Interval (5-32768)**	This column provides configuring Tx Interval settings; the default value is 30 and the available range is **5** to **32678**. Unit is second. The Managed PoE+ Switch is periodically transmitting LLDP frames to its neighbors for having the network discovery information up-to-date. The interval between each LLDP frame is determined by the **Tx Interval** value. This attribute must comply with the following rule: (Transmission Interval * Hold Time Multiplier) ≤65536, and Transmission Interval >= (4 * Delay Interval)
• **Tx Hold Multiplier (2-10)**	This column provides configuring the value for Tx Hold Multiplier; the default value is 4 minute and the available range is **2** to **10**. Each LLDP frame contains information about how long the information in the LLDP frame will be considered valid. The LLDP information valid period is set to **Tx Hold** multiplied by **Tx Interval** seconds. TTL in seconds is based on the following rule: (Transmission Interval * Holdtime Multiplier) ≤ 65536.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	Therefore, the default TTL is 4*30 = 120 seconds.
• **Re-Init Delay (1-10)**	This column provides configuring Re-Init Delay settings; the default value is 2 and the available range is **1** to **10**. Unit is second. When a port is disabled, LLDP is disabled or the Managed PoE+ Switch is rebooted a LLDP shutdown frame is transmitted to the neighboring units, signaling that the LLDP information isn't valid anymore. **Re-init Delay** controls the amount of seconds between the shutdown frame and a new LLDP initialization.
• **Tx Delay (1-8192)**	This column provides configuring Tx Delay settings; the default value is 2 and the available range is **1** to **8192**. Unit is second. If some configuration is changed (e.g. the IP address) a new LLDP frame is transmitted, but the time between the LLDP frames will always be at least the value of **Tx Delay** seconds. **Tx Delay** cannot be larger than 1/4 of the **Tx Interval** value. This attribute must comply with the rule: (4 * Delay Interval) ≤Transmission Interval

Button

Apply: press this button to take effect

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.9.10.2 LLDP Port Setting

This page allows you to configure the LLDP Port settings for Managed PoE+ Switch as the screen in Figure 4-9-33 appears.

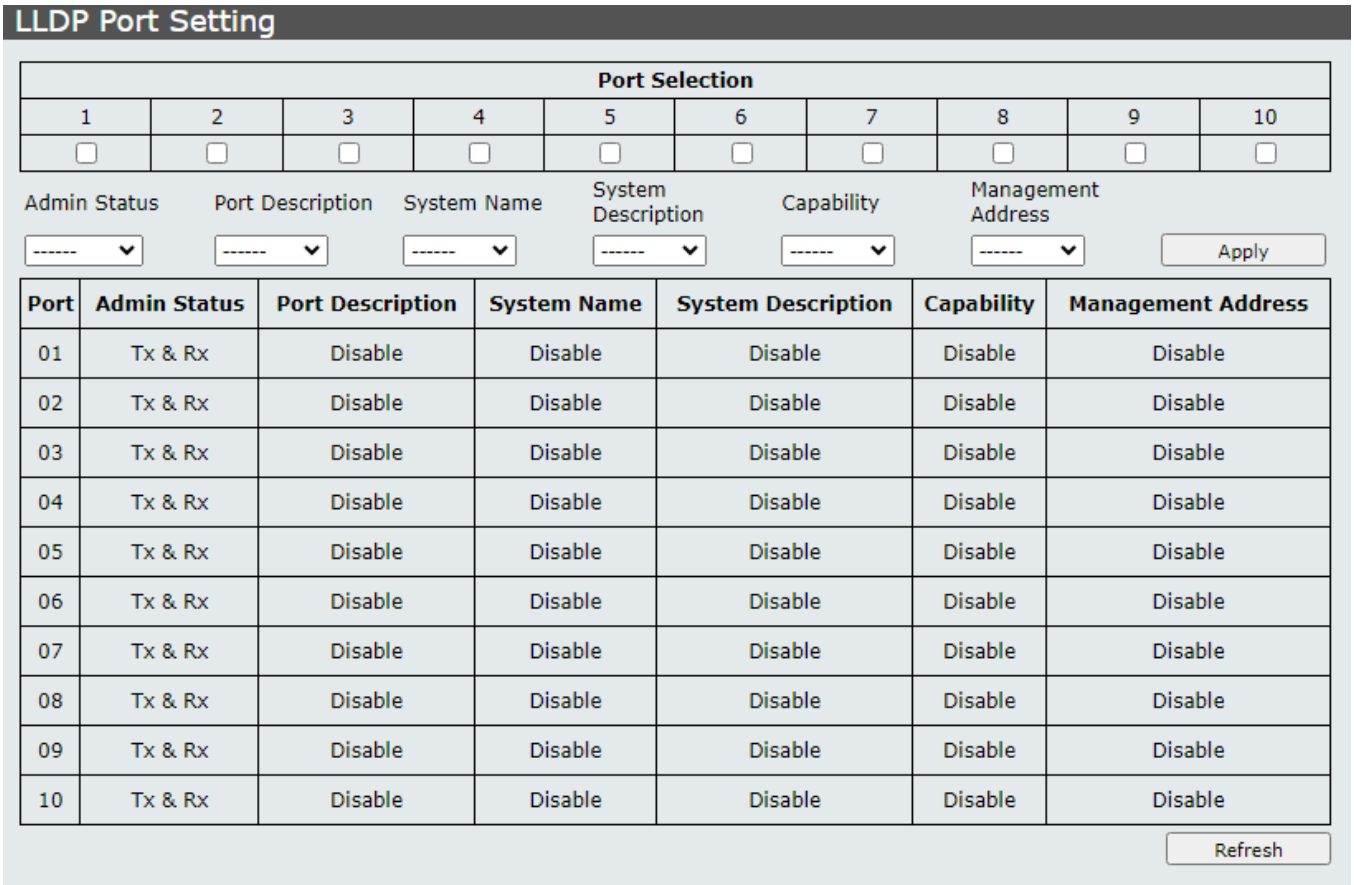


Figure 4-9-33: LLDP Port Settings Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port Selection**	This column provides selecting specific port for LLDP Port Settings function.
• **Port**	Display per port list.
• **Admin Status**	This column provides displaying and selecting the Admin status of LLDP and the available options are : **Disable** The Managed PoE+ Switch will not send out LLDP information, and will drop LLDP information received from neighbors. **Rx Only** The Managed PoE+ Switch will not send out LLDP information, but LLDP information from neighbor units is analyzed. **Tx Only** The Managed PoE+ Switch will drop LLDP information received from neighbors, but will send out LLDP information. **Tx & Rx** The switch will send out LLDP information, and will analyze LLDP information received from neighbors.
• **Port Description**	This column provides displaying and configuring enable or disable the Port Description function. When enabling the "Port Description", the LLDP information will be transmitted.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

• **System Name**	This column provides displaying and configuring enable or disable the System Name function. When enabling the "System Name", the LLDP information will be transmitted.
• **System Description**	This column provides displaying and configuring enable or disable the System Description function. When enabling the "System Description", the LLDP information will be transmitted.
• **Capability**	This column provides displaying and configuring enable or disable the Capability function. When enabling the "Capability", the LLDP information will be transmitted.
• **Management Address**	This column provides displaying and configuring enable or disable the Management Address function. When enabling the "Management Address", the LLDP information will be transmitted.

Buttons

Apply: press this button to confirm the changes.

Refresh: press this button to refresh current status.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.10 Monitoring

On the Access Monitoring configuration web page, you can view and configure Monitoring functions of the Managed PoE+ Switch as the screen in Figure 4-10-1 appears.

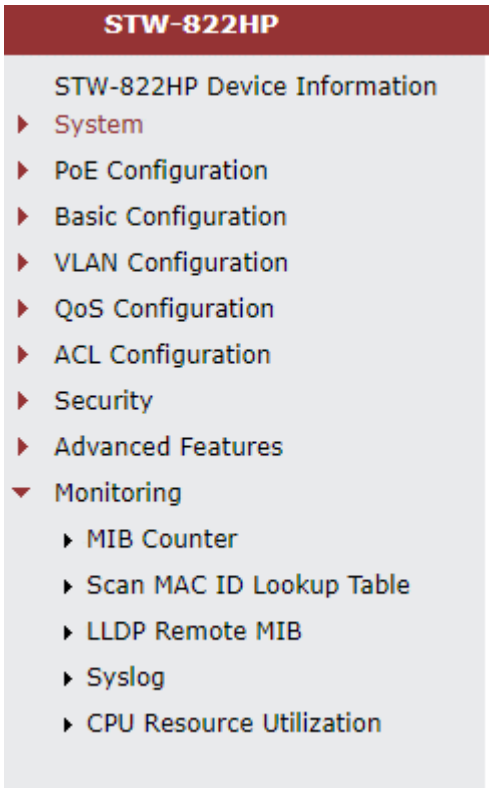


Figure 4-10-1: Managed PoE+ Switch Monitoring Configuration Web Page

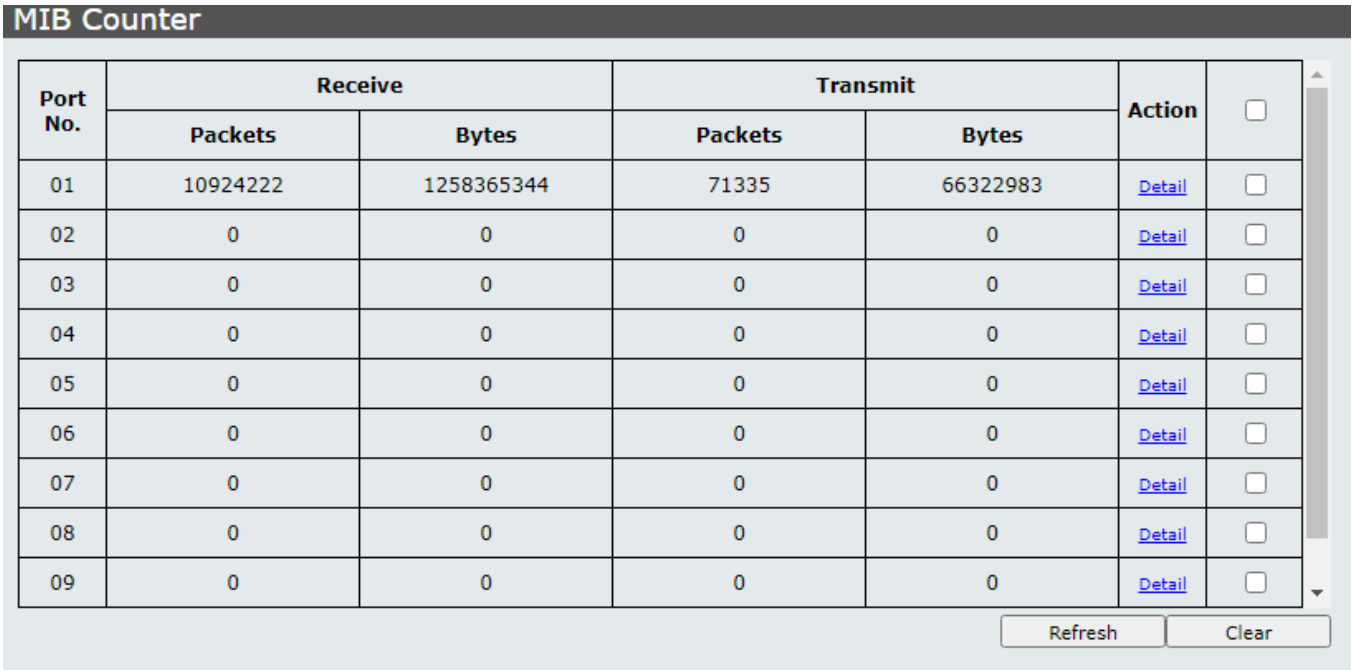
Monitoring Configuration	
Item	**Description**
MIB Counter	Configure and display MIB Counter settings on this web page.
Scan MAC ID Lookup Table	Configure and display Scan MAC ID Lookup Table settings on this web page.
LLDP Remote MIB	Configure and display LLDP Remote MIB settings on this web page.
Syslog	Display System Log informations on this web page.
CPU Resource Utilization	Display CPU Resource Utilization informations on this web page.

Table 4-10-1: Descriptions of Monitoring Configuration

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.10.1 MIB Counter

This page allows you to configure the MIB Counter settings for Managed PoE+ Switch as the screen in Figure 4-10-2 appears.



MIB Counter

Port No.	Receive		Transmit		Action	
	Packets	Bytes	Packets	Bytes		
01	10924222	1258365344	71335	66322983	Detail	
02	0	0	0	0	Detail	
03	0	0	0	0	Detail	
04	0	0	0	0	Detail	
05	0	0	0	0	Detail	
06	0	0	0	0	Detail	
07	0	0	0	0	Detail	
08	0	0	0	0	Detail	
09	0	0	0	0	Detail	

Refresh Clear

Figure 4-10-2: MIB Counter Configuration Page Screenshot

The page includes the following fields:

Object	Description
• **Port No.**	This column provides display per port list.
Receive	
• **Packets**	This column provides displaying per port traffic in packets receive counters.
• **Bytes**	This column provides displaying per port traffic in bytes receive counters.
Transmit	
• **Packets**	This column provides displaying per port traffic in packets transmit counters.
• **Bytes**	This column provides displaying per port traffic in bytes transmit counters.
• **Action**	This column provides click to select all port or specific port for refresh or clear current MIB counter information.
• **Detail**	This column provides click to enter advanced per port MIB counter web page.

Buttons

Refresh: press this button to refresh current MIB counter information.

Clear: press this button to clear current MIB counter information.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Press **"Detail"** from MIB Counter web page, which allows you to view advanced per port MIB counter information as the screen in Figure 4-10-3 appears

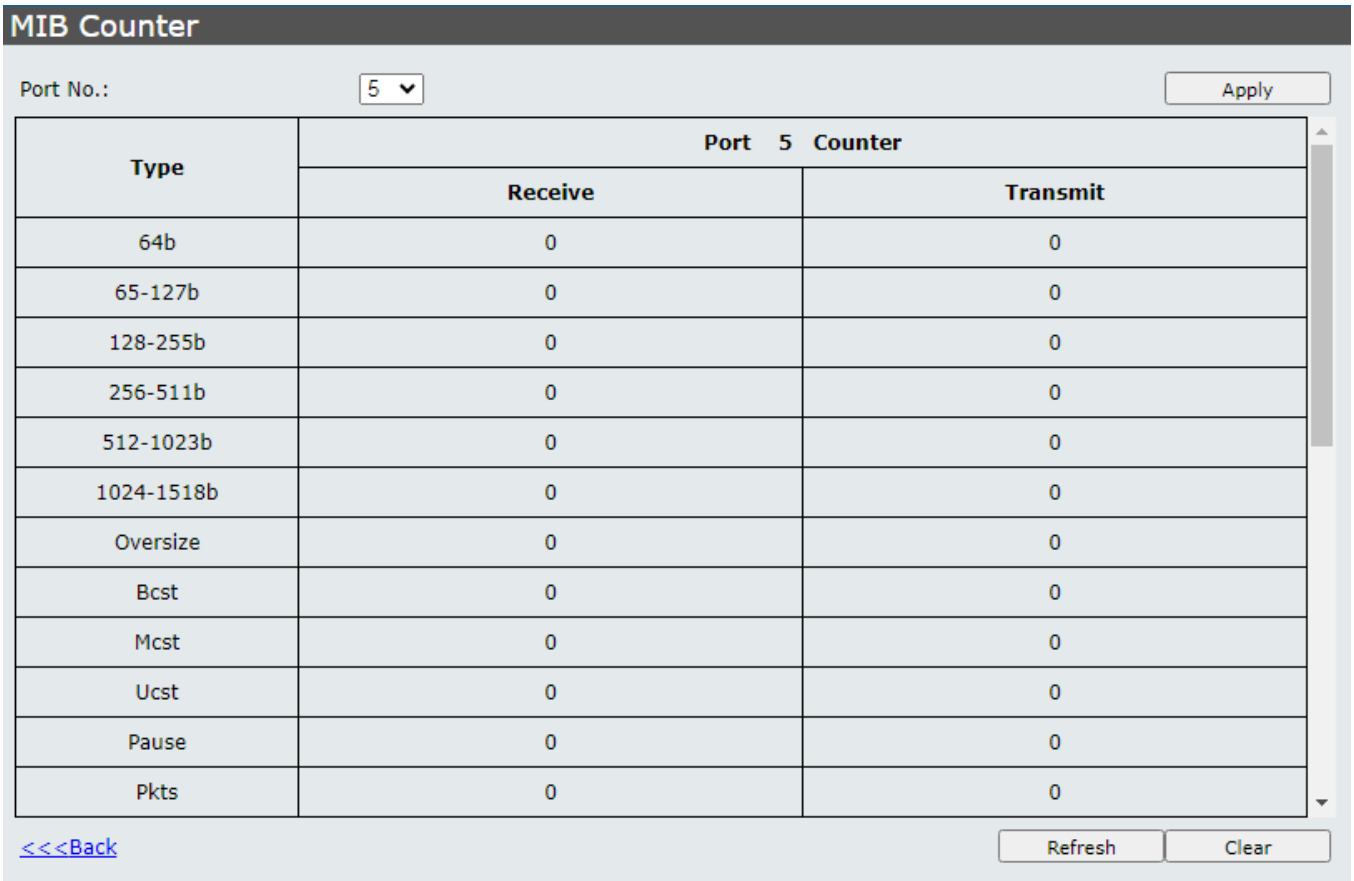


Figure 4-10-3: Per Port Detail MIB Counter Page Screenshot

The page includes the following fields:

Object	Description
• **Port No.**	This column provides displaying per port list.
• **Type**	This column provides displaying traffic with various packet lengths and types, and the available options are : **64b** **65-127b** **128-255b** **256-511b** **512-1023b** **1024-1518b** **Oversize** **Bcst: Broadcast** **Mcst:Multicast** **Ucst: Unicast** **Pause** **Pkts** **Bytes** **Drop** **Drop others** **CRC** **Alignment**

SEC.RU | Короткий путь к информации
Скачано с sec.ru

	Runt **Frag** **Jabber** **Symbol error** **ACL1** **ACL2** **Single Col** **Multiple Col** **Late Col** **Defered tx** **Excessive Col**
Port X Counter (X= Port Number)	
• **Receive**	This column displays the counters of per port traffic receive with various packet lengths and types .
• **Transmit**	This column displays the counters of per port traffic transmit with various packet lengths and types .

Buttons

Apply: press this button to confirm the changes.

Refresh: press this button to refresh current MIB counter information.

Clear: press this button to clear current MIB counter information.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.10.2 Scan MAC ID Lookup Table

This page allows you to configure the Scan MAC ID Lookup Table settings for Managed PoE+ Switch as the screen in Figure 4-10-4 appears.

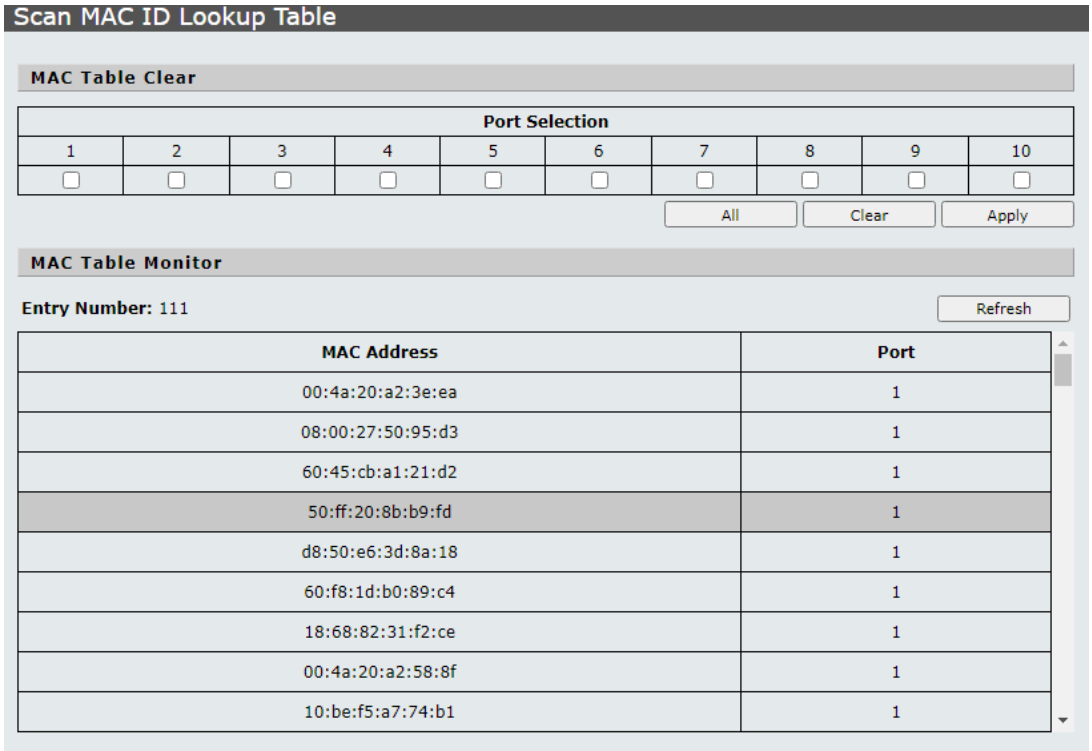


Figure 4-10-4: Scan MAC ID Lookup Table Page Screenshot

The page includes the following fields:

Object	Description
MAC Table Clear	
• **Port Selection**	This column provides selecting specific port for Scan MAC ID Lookup Table function.
MAC Table Monitor	
• **Enrty Number**	This column provides displaying entry number of MAC address table.
• **MAC Address**	This column provides displaying per port MAC address table information.
• **Port**	This column provides displaying port list.

Buttons

All : press this button to select all ports.

Clear : press this button to clear all selected ports.

Apply : press this button to confirm the changes.

Refresh : press this button to refresh current Scan MAC ID Lookup Table information.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.10.3 LLDP Remote MIB

This page allows you to configure the LLDP Remote MIB settings for Managed PoE+ Switch as the screen in Figure 4-10-5 appears.

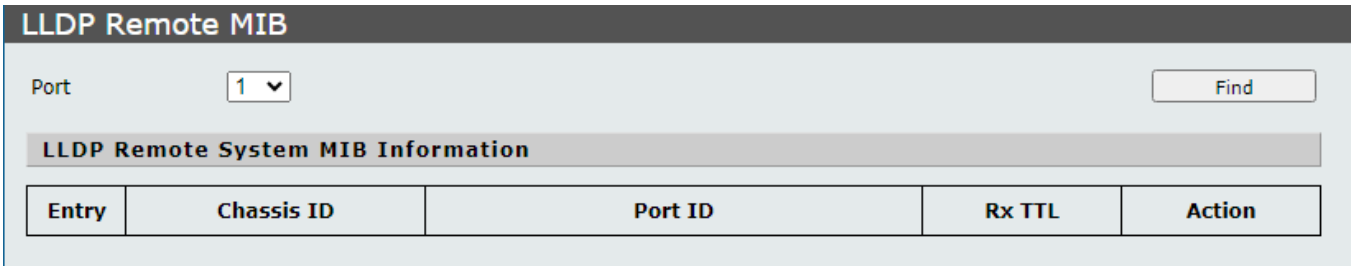


Figure 4-10-5: LLDP Remote MIB Page Screenshot

The page includes the following fields:

Object	Description
• **Port**	This column provides selecting specific port for LLDP Remote MIB function.
LLDP Remote System MIB Information	
• **Enrty**	This column provides displaying entry number of LLDP Remote MIB information.
• **Chassis ID**	This column provides displaying chassis ID of LLDP Remote MIB information.
• **Port ID**	This column provides displaying Port ID of LLDP Remote MIB information.
• **Rx TTL**	This column provides displaying Rx TTL of LLDP Remote MIB information.
• **Action**	Delete: press this button to delete specific LLDP Remote MIB information.

Button

Find: press this button to find LLDP Remote MIB information of specific port.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.10.4 Syslog

This page allows you to view the Syslog for Managed PoE+ Switch as the screen in Figure 4-10-6 appears.

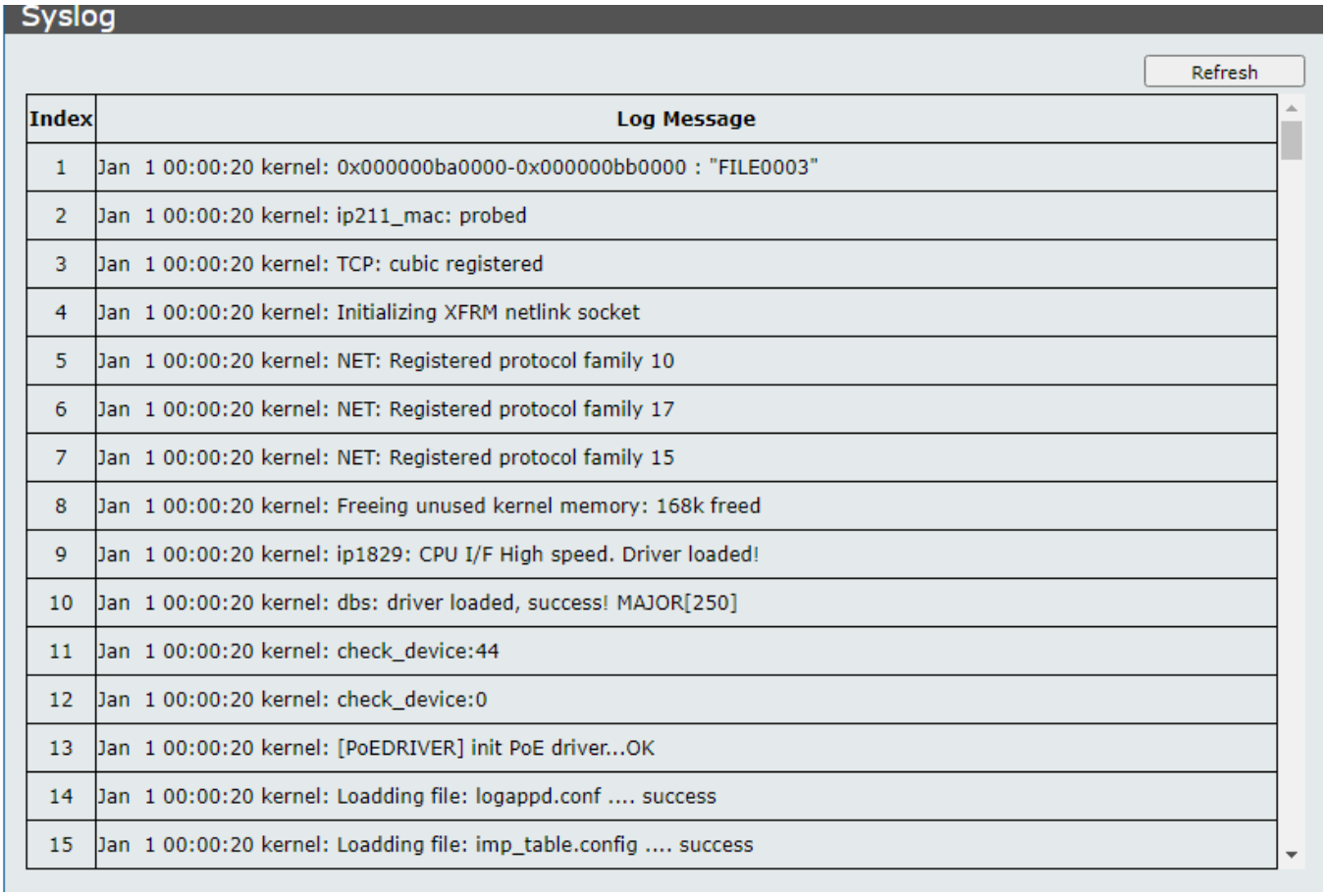


Figure 4-10-6: Syslog Page Screenshot

The page includes the following fields:

Object	Description
• **Index**	This column provides displaying per index list.
• **Log Message**	This column provides displaying log message information of per index.

Button

Refresh: press this button to refresh current Syslog log message information.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

4.10.5 CPU Resource Utilization

This page allows you to view the CPU resource utilization of Managed PoE+ Switch as the screen in Figure 4-10-7 appears.

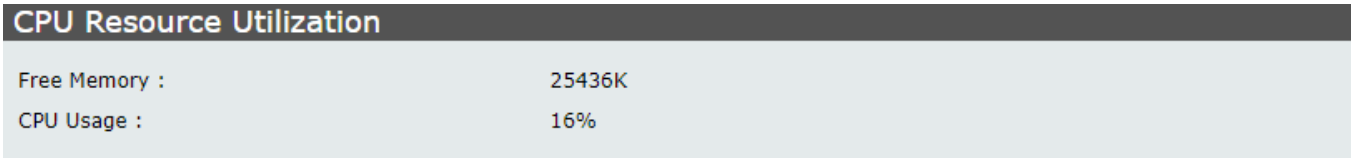


Figure 4-10-7: CPU Resource Utilization Page Screenshot

The page includes the following fields:

Object	Description
• **Free Memory**	This column provides displaying the free memory status.
• **CPU Usage**	This column provides displaying the CPU Usgae status.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5. COMMAND LINE INTERFACE

5.1 Accessing the CLI

When accessing the management interface for the Managed PoE+ Switch over a direct connection to the server's console port, or via a Telnet connection, the Managed PoE+ Switch can be managed by entering command keywords and parameters at the prompt. Using the Managed PoE+ Switch 's command-line interface (CLI) is very similar to entering commands on a UNIX system.

This chapter describes how to use the Command Line Interface (CLI).

Logging on to the Console

Once the terminal has connected to the device, power on the Managed PoE+ Switch, and the terminal will display running testing procedures.

Then, the following message asks the login username and password. The factory default password is as follows as the login screen in Figure 5-1 appears.

Username: **admin**

Password: **admin**

Welcome to STW-2422HP it is Thu Jan 00:01:47 UTC 1970

Figure 5-1: STW-2422HP Console Login Screen

Note

1. For security reason, please change and memorize the new password after this first setup.
2. Only accept command in lowercase letter under console interface.

Configure IP Address

The Managed PoE+ Switch is shipped with the default IP address shown below.

IP Address: **192.168.0.100**

Subnet Mask: **255.255.255.0**

To check the current IP address or modify a new IP address for the Managed PoE+ Switch, please use the procedures as follows:

■ **Show the current IP Address**

1. At the **">"** prompt, enter **"show ip".**
2. The screen displays the current IP address as shown in Figure 5-2.

> show ip

IP Address: **192.168.0.100**

Subnet Mask: **255.255.255.0**

Default Gateway: **192.168.0.254**

DNS Server:

DHCP Client: **Disabled**

Figure 5-2: IP Information Screen

SEC.RU | Короткий путь к информации
Скачано с sec.ru

■ **Configuring IP Address**

3. At the **">"** prompt, enter the following command and press **<Enter>** as shown in Figure 5-3.

```
> config ip address 192.168.1.100
> config ip submask 255.255.255.0
```

Figure 5-3: Configuring IP Address Screen

The previous command would apply the following settings for the Managed PoE+ Switch.

IP Address: **192.168.1.100**
Subnet Mask: **255.255.255.0**

4. Repeat step 1 to check if the IP address has changed.

If the IP is successfully configured, the Managed PoE+ Switch will apply the new IP address setting immediately. You can access the Web interface of Managed PoE+ Switch through the new IP address.

Note

If you are not familiar with console command or the related parameter, enter "**help**" anytime in console to get the help description.

You can change these settings, if desired, after you log on. This management method is often preferred because you can remain connected and monitor the system during system reboots. Also, certain error messages are sent to the serial port, regardless of the interface through which the associated action was initiated. A Macintosh or PC attachment can use any terminal-emulation program for connecting to the terminal serial port. A workstation attachment under UNIX can use an emulator such as TIP.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5.2 Telnet Login

The Managed PoE+ Switch also supports telnet for remote management. The Managed PoE+ Switch asks for user name and password for remote login when using telnet. Use **"admin"** for username and password as the login screen in Figure 5-4 appears.

```
Username:admin
Password:
Welcome to STW-822HP it is Mon Jan  5 07:55:22 UTC 1970
>
```

Figure 5-4: Remote Telnet Screen

SEC.RU | Короткий путь к информации
Скачано с sec.ru

6. Command Line Mode

The CLI groups all the commands in appropriate modes according to the nature of the command. A sample of the CLI command modes are described below. Each of the command modes supports specific software commands.

Command Groups:

clear	clear command, key in '?' to show the list
config	config command, key in '?' to show the list
create	create command, key in '?' to show the list
default	default command, key in '?' to show the list
delete	delete command, key in '?' to show the list
disable	disable command, key in '?' to show the list
enable	enable command, key in '?' to show the list
exit	Exit this CLI session
reboot	reboot
restart	re-start command, key in '?' to show the list
save	save setting.
show	Show command, key in '?' to show the list

SEC.RU | Короткий путь к информации
Скачано с sec.ru

6.1 Clear Command

Command Lists:

clear	clear command, key in '?' to show the list.
acl	Used to clear ACL table.
igmp_snooping	Used to clear entries of IGMP snooping.
ip	Used to clear IPv4 settings.
ipv6	Used to clear IPv6 settings.
mac_table	Used to clear dynamic entries of MAC-table function by port.
mib_counter	Used to clear MIB counters.
mld_snooping	Used to clear entries of MLD snooping.
poe	Used to clear poe informations.
syslog	Used to clear server information of syslog.
system	Used to clear system information.
vlan	Used to clear entry of protocol VLAN.

6.2 Config Command

Command Lists:

config	config command, key in '?' to show the list
account	Used to config account information.
acl	Used to config ACL.
bandwidth_ctrl	Used to set the bandwidth parameters of ports.
cos	Used to config cos function.
dhcprelay	Used to config dhcprelay.
double-vlan	Used to config double VLAN.
gvrp	Used to config gvrp information.
igmp_snooping	Used to config IGMP snooping.
imp_table	Used to config IMP-table.
ip	Used to config IP information.
ipv6	Used to config IPv6 information.
link_aggregation	Used to config link aggregation.
lldp	Used to config LLDP.
loop-detect	Used to config loop detect information.
mac_table	Used to config MAC-table.
mirror	Used to set mirror port function and method.
mld_snooping	Used to config MLD snooping.
neighbor	Used to config neighbor MACID information.
ntp	Used to config the attributes of ntp.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

poe	Used to config poe.
ports	Used to config the attributes of ports.
qosaging	Used to config Qos aging.
qosmode	Used to config Qos function.
qosremap	Used to config Qos remap function.
snmp	Used to config snmp information.
storm_ctrl	Used to config storm control.
stp	Used to config STP.
stp-loop-detect	Used to config STP loop detect information.
syslog	Used to config syslog.
system	Used to config system information.
vlan	Used to config VLAN.
voice-vlan	Used to config voice VLAN.

6.3 Create Command

Command Lists:

create	create command, key in '?' to show the list
acl	Used to create a new profile of ACL.
igmp_snooping	Used to create a new entry of IGMP snooping.
imp_table	Used to create a new entry of IMP-table.
mac_table	Used to create a new entry of MAC-table.
mld_snooping	Used to create a new entry of MLD snooping.
snmp	Used to create snmp information.
stp	Used to create a new entry of STP.
vlan	Used to create a new entry of VLAN.

6.4 Default Command

Command Lists:

default	default command, key in '?' to show the list
all	Load factory default .

SEC.RU | Короткий путь к информации
Скачано с sec.ru

6.5 Delete Command

Command Lists:

delete	delete command, key in '?' to show the list
acl	Used to delete ACL profile .
igmp_snooping	Used to delete an entry of IGMP snooping .
imp_table	Used to delete an entry of IMP-table.
mac_table	Used to delete an entry of MAC-table.
mld_snooping	Used to delete an entry of MLD snooping .
snmp	Used to delete snmp informaiton.
stp	Used to delete an entry of STP .
vlan	Used to delete an entry of VLAN.
voice-vlan	Remove OUI setting.

6.6 Disable Command

Command Lists:

disable	disable command, key in '?' to show the list
DHCP_arp_inspection	Used to disable DHCP Dynamic ARP Inspection function.
DHCP_mac_verification	Used to disable DHCP MAC verification function.
DHCP_snooping	Used to disable DHCP Snooping function.
dhcprelay	Used to disable dhcprelay function.
gvrp	Used to disable gvrp function.
igmp_snooping	Used to disable IGMP snooping function.
imp_table	Used to disable IMP-table function.
lldp	Used to disable LLDP function.
loop-detect	Used to disable loop detect protocol.
mac_table	Used to disable MAC-table function.
mirror	Used to disable mirror in standard mode.
mld_snooping	Used to disable MLD snooping.
neighbor	Used to disable neighbor MACID function.
ntp	Used to disable network time protocol function.
poe	Used to dsable poe ports.
snmp	Used to disable SNMP protocol.
storm_ctrl	Used to disable storm control function.
stp	Used to disable STP function.
stp-loop-detect	Used to disable STP loop detect protocol.
syslog	Used to disable syslog function.
vlan	Used to disable VLAN function.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

6.7 Enable Command

Command Lists:

enable	enable command, key in '?' to show the list
DHCP_arp_inspection	Used to enable DHCP Dynamic ARP Inspection function.
DHCP_mac_verification	Used to enable DHCP MAC verification function.
DHCP_snooping	Used to enable DHCP Snooping function.
dhcprelay	Used to enable dhcprelay function.
gvrp	Used to enable gvrp function.
igmp_snooping	Used to enable IGMP snooping function.
imp_table	Used to enable IMP-table function.
lldp	Used to enable LLDP function.
loop-detect	Used to enable loop detect protocol.
mac_table	Used to enable MAC-table function.
mirror	Used to enable mirror in standard mode.
mld_snooping	Used to enable MLD snooping.
neighbor	Used to enable neighbor MACID function.
ntp	Used to enable network time protocol function.
poe	Used to enable poe ports.
snmp	Used to enable SNMP protocol.
storm_ctrl	Used to enable storm control function.
stp	Used to enable STP function.
stp-loop-detect	Used to enable STP loop detect protocol.
syslog	Used to enable syslog function.
vlan	Used to enable VLAN function.

6.8 Exit Command

Command List:

exit	Exit this CLI session.

6.9 Reboot Command

Command List:

reboot	Reboot the Managed PoE+ Switch.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

6.10 Restart Command

Command List:

restart	re-start command, key in '?' to show the list
igmp_snooping	Used to restart IGMP process.
link_aggregation	Used to restart link aggregation process.
mcp	Used to restart MCP process.
mld_snooping	Used to restart MLD process.
stp	Used to restart STP process .
syslog	Used to restart syslog function.

6.11 Save Command

Command List:

save	save setting of Managed PoE+ Switch.

6.12 Show Command

Command List:

show	Show command, key in '?' to show the list
account	Used to show account information.
acl	Used to show information of ACL.
bandwidth_ctrl	Used to show the information of bandwidth control.
cos	Used to show cos function information.
DHCP Snooping	Used to show information of DHCP Snooping.
dhcprelay	Used to show information of dhcprelay.
double-vlan	Used to show information of double VLAN.
gvrp	Used to show gvrp status information.
igmp_snooping	Used to show information of IGMP snooping.
imp_table	Used to show information of IMP-table.
ip	Used to show the information of IP.
ipv6	Used to show the information of IPv6.
link_aggregation	Used to show information of link aggregation.
lldp	Used to show information of LLDP.
loop-detect	Used to show loop detect status information .
mac_table	Used to show information of MAC-table.
mib_counter	Used to show information of MIB counter.
mirror	Used to show the information of mirror.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

mld_snooping	Used to show information of MLD snooping.
neighbor	Used to show the neighbor MACID Information.
ntp	Used to show the attributes of ntp.
poe	Used to show the attributes of poe.
ports	Used to show the attributes of ports.
qosaging	Used to show Qos aging function information.
qosmode	Used to show Qos mode information.
qosremap	Used to show Qos remap information.
snmp	Used to show SNMP Status information.
storm_ctrl	Used to show information of storm control.
stp	Used to show information of STP.
stp-loop-detect	Used to show STP Loop Detect Status information .
syslog	Used to show information of syslog.
system	Used to show system information.
vlan	Used to show information of VLAN.
voice-vlan	Used to show voice vlan informatio.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

7. SWITCH OPERATION

7.1 Address Table

The **Managed PoE+ Switch** is implemented with an address table. This address table is composed of many entries. Each entry is used to store the address information of some node in network, including MAC address, port no., etc. This information comes from the learning process of **Managed PoE+ Switch**.

7.2 Learning

When one packet comes in from any port, the **Managed PoE+ Switch** will record the source address, port no., and the other related information in the address table. This information will be used to decide either forwarding or filtering for future packets.

7.3 Forwarding & Filtering

When one packet comes from some port of the **Managed PoE+ Switch**, it will also check the destination address besides the source address learning. The **Managed PoE+ Switch** will lookup the address-table for the destination address. If not found, this packet will be forwarded to all the other ports except the port, which this packet comes in. And these ports will transmit this packet to the network it connected. If found, and the destination address is located at different port from this packet comes in, the **Managed PoE+ Switch** will forward this packet to the port where this destination address is located according to the information from address table. But, if the destination address is located at the same port with this packet comes in, then this packet will be filtered. Thereby increasing the network throughput and availability.

7.4 Store-and-Forward

Store-and-Forward is one type of packet-forwarding techniques. A Store-and-Forward **Managed PoE+ Switch** stores the incoming frame in an internal buffer, and does the complete error checking before transmission. Therefore, no error will occur. Choosing a network that needs efficiency and stability is the best choice.
The **Managed PoE+ Switch** scans the destination address from the packet-header, searches the routing table provided for the incoming port and forwards the packet, only if required. The fast forwarding makes the switch attractive for connecting servers directly to the network, thereby increasing throughput and availability. However, the switch is most commonly used to segment the existing hubs, which nearly always improves the overall performance. An Ethernet Switching can be easily configured in any Ethernet network environment to significantly boost bandwidth using conventional cabling and adapters.
Due to the learning function of the **Managed PoE+ Switch**, the source address and corresponding port number of each incoming and outgoing packet are stored in a routing table. This information is subsequently used to filter packets whose destination address is on the same segment as the source address. This confines network traffic to its respective domain and reduce the overall load on the network.
The **Managed PoE+ Switch** performs **"Store and Fforward";** therefore, no error packets occur. More reliably, it reduces the re-transmission rate. No packet loss will occur.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

7.5 Auto-Negotiation

The STP ports on the Switch have built-in **"Auto-negotiation"**. This technology automatically sets the best possible bandwidth when a connection is established with another network device (usually at Power On or Reset). This is done by detecting the modes and speeds at the second of both devices is connected and capable of. Both 10BASE-T and 100BASE-TX devices can connect with the port in either Half- or Full-Duplex mode. 1000BASE-T can be only connected in Full-duplex mode.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

8. Power over Ethernet Overview

What is PoE?

The PoE is an abbreviation of Power over Ethernet; the PoE technology means a system to pass electrical power safely, along with data on Ethernet UTP cable. The IEEE standard for PoE technology requires Category 5 cable or higher for high power PoE levels, but can operate with category 3 cable for low power levels. Power is supplied in common mode over two or more of the differential pairs of wires found in the Ethernet cables and comes from a power supply within a PoE-enabled networking device such as an Ethernet switch or can be injected into a cable run with a mid-span power supply.
The original IEEE 802.3af-2003 PoE standard provides up to 15.4 W of DC power (minimum 44 V DC and 350mA) to each device. Only 12.95 W is assured to be available at the powered device as some power is dissipated in the cable.
The updated IEEE 802.3at-2009 PoE standard also known as PoE+ or PoE plus, provides up to 25.5 W of power. The 2009 standard prohibits a powered device from using all four pairs for power
The 802.3af / 802.3at define two types of source equipment: Mid-Span and End-Span.

Mid-Span
Mid-Span device is placed between legacy switch and the powered device. Mid-Span is tap the unused wire pairs 4/5 and 7/8 to carry power, the other four is for data transmit.

End-Span
End-Span device is direct connecting with power device. End-Span could also tap the wire 1/2 and 3/6.

PoE System Architecture
The specification of PoE typically requires two devices: the **Powered Source Equipment (PSE)** and the **Powered Device (PD)**. The PSE is either an End-Span or a Mid-Span, while the PD is a PoE-enabled terminal, such as IP Phones, Wireless LAN, etc. Power can be delivered over data pairs or spare pairs of standard CAT-5 cabling.

Powered Source Equipment (PSE)

Power sourcing equipment (PSE) is a device such as a switch that provides (sources) power on the Ethernet cable. The maximum allowed continuous output power per cable in IEEE 802.3af is 15.40 W. A later specification, IEEE 802.3at, offers 25.50 W. When the device is a switch, it is commonly called an End-span (although IEEE 802.3af refers to it as endpoint). Otherwise, if it's an intermediary device between a non PoE capable switch and a PoE device, it's called a Mid-span. An external PoE injector is a Mid-span device.

Powered device

A powered device (PD) is a device powered by a PSE and thus consumes energy. Examples include wireless access points, IP Phones, and IP cameras. Many powered devices have an auxiliary power connector for an optional, external, power supply. Depending on the PD design, some, none, or all power can be supplied from the auxiliary port, with the auxiliary port sometimes acting as backup power in case of PoE supplied power failure.

How Power is Transferred Through the Cable
A standard CAT5 Ethernet cable has four twisted pairs, but only two of these are used for 10BASE-T and 100BASE-TX. The specification allows two options for using these cables for power, shown in Figure 1 and Figure 2:
The spare pairs are used. Figure 1 shows the pair on pins 4 and 5 connected together and forming the positive supply, and the pair on pins 7 and 8 connected and forming the negative supply. (In fact, a late change to the spec allows either polarity to be used).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

9. TROUBLESHOOTING

This chapter contains information to help you solve issues. If the Managed PoE+ Switch is not functioning properly, make sure the Managed PoE+ Switch was set up according to instructions in this manual.

■ The Link LED is not lit

Solution:
Check the cable connection and remove duplex mode of the Managed PoE+ Switch

■ Some stations cannot talk to other stations located on the other port

Solution:
Please check the VLAN settings, trunk settings, or port enabled / disabled status.

■ Performance is bad

Solution:
Check the full duplex status of the Managed PoE+ Switch. If the Managed PoE+ Switch is set to full duplex and the partner is set to half duplex, then the performance will be poor. Please also check the in/out rate of the port.

■ Why the Switch doesn't connect to the network

Solution:

1. Check the LNK/ACT LED on the switch
2. Try another port on the Switch
3. Make sure the cable is installed properly
4. Make sure the cable is the right type
5. Turn off the power. After a while, turn on power again

■ 1000BASE-T port link LED is lit, but the traffic is irregular

Solution:
Check that the attached device is not set to dedicate full duplex. Some devices use a physical or software switch to change duplex modes. Auto-negotiation may not recognize this type of full-duplex setting.

■ Switch does not power up

Solution:

1. AC power cord not inserted or faulty
2. Check that the AC power cord is inserted correctly
3. Replace the power cord If the cord is inserted correctly, check that the AC power source is working by connecting a different device in place of the switch.
4. If that device works, refer to the next step.
5. If that device does not work, check the AC power

SEC.RU | Короткий путь к информации
Скачано с sec.ru

■ **IP address has been changed or admin password has been forgotten –**

Solution:

To reset the IP address to the default IP address **"192.168.0.100"** or reset the login password to default value, press the hardware-based **reset button** on the front panel for about **5 seconds.** After the device is rebooted, you can log in to the management Web interface within the same subnet of 192.168.0.xx.

Figure 9-1: STW-822HP Reset Button

Figure 9-2: STW-1622HP Reset Button

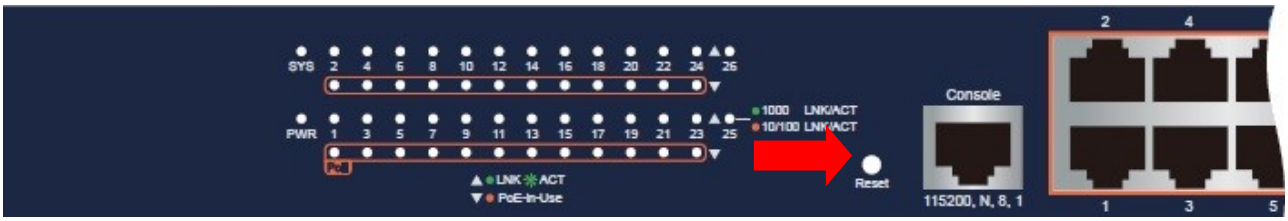
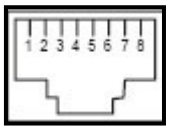


Figure 9-3: STW-2422HP Reset Button

SEC.RU | Короткий путь к информации
Скачано с sec.ru

APPENDIX A: Networking Connection

A.1 PoE RJ45 Port Pin Assignments



PIN NO	RJ45 POWER ASSIGNMENT
1	• Power +
2	• Power +
3	• Power -
6	• Power -

A.2 Switch's Data RJ45 Pin Assignments -- 1000Mbps, 1000BASE-T

PIN NO	MDI	MDI-X
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-

Implicit implementation of the crossover function within a twisted-pair cable, or at a wiring panel, while not expressly forbidden, is beyond the scope of this standard.

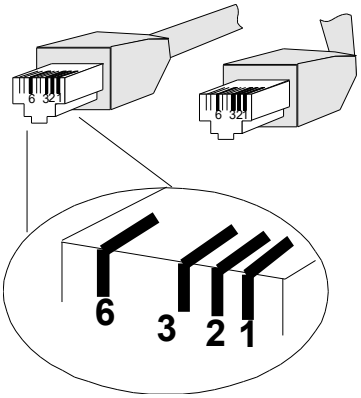
A.3 10/100Mbps, 10/100BASE-TX

When connecting your Switch to another Fast Ethernet switch, a bridge or a hub, a straight or crossover cable is necessary. Each port of the Switch supports auto-MDI/MDI-X detection. That means you can directly connect the Switch to any Ethernet devices without making a crossover cable. The following table and diagram show the standard RJ45 receptacle/ connector and their pin assignments:

RJ45 Connector pin assignment		
PIN NO	MDI Media Dependent Interface	MDI-X Media Dependent Interface -- Cross
1	Tx + (transmit)	Rx + (receive)
2	Tx - (transmit)	Rx - (receive)
3	Rx + (receive)	Tx + (transmit)
4, 5	Not used	
6	Rx - (receive)	Tx - (transmit)
7, 8	Not used	

SEC.RU | Короткий путь к информации
Скачано с sec.ru

The standard cable, RJ45 pin assignment



The standard RJ45 receptacle/connector

There are 8 wires on a standard UTP/STP cable and each wire is color-coded. The following shows the pin allocation and color of straight cable and crossover cable connection:

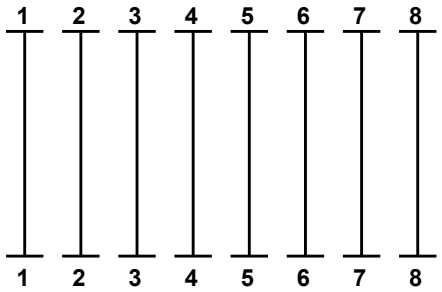
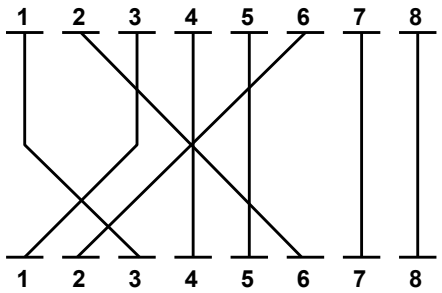
Straight Cable		SIDE 1	SIDE2
	SIDE 1 SIDE 2	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown
Crossover Cable		**SIDE 1**	**SIDE2**
	SIDE 1 SIDE 2	1 = White / Orange 2 = Orange 3 = White / Green 4 = Blue 5 = White / Blue 6 = Green 7 = White / Brown 8 = Brown	1 = White / Green 2 = Green 3 = White / Orange 4 = Blue 5 = White / Blue 6 = Orange 7 = White / Brown 8 = Brown

Figure A-1: Straight-through and Crossover Cable

Please make sure your connected cables are with same pin assignment and color as the above table before deploying the cables into your network.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

APPENDIX B: GLOSSARY

A

ACE

ACE is an acronym for **A**ccess **C**ontrol **E**ntry. It describes access permission associated with a particular ACE ID.

There are three ACE frame types (Ethernet Type, ARP, and IPv4) and two ACE actions (permit and deny). The ACE also contains many detailed, different parameter options that are available for individual application.

ACL

ACL is an acronym for **A**ccess **C**ontrol **L**ist. It is the list table of ACEs, containing access control entries that specify individual users or groups permitted or denied to specific traffic objects, such as a process or a program.

Each accessible traffic object contains an identifier to its ACL. The privileges determine whether there are specific traffic object access rights.

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

There are 3 web-Pages associated with the manual ACL configuration:

ACL|Access Control List: The web Page shows the ACEs in a prioritized way, highest (top) to lowest (bottom). Default the table is empty. An ingress frame will only get a hit on one ACE even though there are more matching ACEs. The first matching ACE will take action (permit/deny) on that frame and a counter associated with that ACE is incremented. An ACE can be associated with a Policy, 1 ingress port, or any ingress port (the whole switch). If an ACE Policy is created then that Policy can be associated with a group of ports under the "Ports" web-Page. There are number of parameters that can be configured with an ACE. Read the Web Page help text to get further information for each of them. The maximum number of ACEs is 64.

ACL|Ports: The ACL Ports configuration is used to assign a Policy ID to an ingress port. This is useful to group ports to obey the same traffic rules. Traffic Policy is created under the "Access Control List" - Page. You can you also set up specific traffic properties (Action / Rate Limiter / Port copy, etc) for each ingress port. They will though only apply if the frame gets past the ACE matching without getting matched. In that case a counter associated with that port is incremented. See the Web Page help text for each specific port property.

ACL|Rate Limiters: Under this Page you can configure the rate limiters. There can be 15 different rate limiters, each ranging from 1-1024K packets per seconds. Under "Ports" and "Access Control List" web-Pages you can assign a Rate Limiter ID to the ACE(s) or ingress port(s).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

AES

AES is an acronym for **A**dvanced **E**ncryption **S**tandard. The encryption key protocol is applied in 802.1i standard to improve WLAN security. It is an encryption standard by the U.S. government, which will replace DES and 3DES. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits.

AMS

AMS is an acronym for **A**uto **M**edia **S**elect. AMS is used for dual media ports (ports supporting both copper (cu) and fiber (SFP) cables. AMS automatically determines if a SFP or a CU cable is inserted and switches to the corresponding media. If both SFP and cu cables are inserted, the port will select the prefered media.

APS

APS is an acronym for **A**utomatic **P**rotection **S**witching. This protocol is used to secure that switching is done bidirectional in the two ends of a protection group, as defined in G.8031.

Aggregation

Using multiple ports in parallel to increase the link speed beyond the limits of a port and to increase the redundancy for higher availability.

(Also *Port Aggregation, Link Aggregation*).

ARP

ARP is an acronym for **A**ddress **R**esolution **P**rotocol. It is a protocol that used to convert an IP address into a physical address, such as an Ethernet address. ARP allows a host to communicate with other hosts when only the Internet address of its neighbors is known. Before using IP, the host sends a broadcast ARP request containing the Internet address of the desired destination system.

ARP Inspection

ARP Inspection is a secure feature. Several types of attacks can be launched against a host or devices connected to Layer 2 networks by "poisoning" the ARP caches. This feature is used to block such attacks. Only valid ARP requests and responses can go through the switch device.

Auto-Negotiation

Auto-negotiation is the process where two different devices establish the mode of operation and the speed settings that can be shared by those devices for a link.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

CC

CC is an acronym for **C**ontinuity **C**heck. It is a MEP functionality that is able to detect loss of continuity in a network by transmitting CCM frames to a peer MEP.

CCM

CCM is an acronym for **C**ontinuity **C**heck **M**essage. It is a OAM frame transmitted from a MEP to it's peer MEP and used to implement CC functionality.

CDP

CDP is an acronym for **C**isco **D**iscovery **P**rotocol.

D

DEI

DEI is an acronym for **D**rop **E**ligible **I**ndicator. It is a 1-bit field in the VLAN tag.

DES

DES is an acronym for **D**ata **E**ncryption **S**tandard. It provides a complete description of a mathematical algorithm for encrypting (enciphering) and decrypting (deciphering) binary coded information.

Encrypting data converts it to an unintelligible form called cipher. Decrypting cipher converts the data back to its original form called plaintext. The algorithm described in this standard specifies both enciphering and deciphering operations which are based on a binary number called a key.

DHCP

DHCP is an acronym for **D**ynamic **H**ost **C**onfiguration **P**rotocol. It is a protocol used for assigning dynamic IP addresses to devices on a network.

DHCP used by networked computers (clients) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server.

The DHCP server ensures that all IP addresses are unique, for example, no IP address is assigned to a second client while the first client's assignment is valid (its lease has not expired). Therefore, IP address pool management is done by the server and not by a human network administrator.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means that a new computer can be added to a network without the hassle of manually assigning it a unique IP address.

DHCP Relay

DHCP Relay is used to forward and to transfer DHCP messages between the clients and the server when they are not on the same subnet domain.

The DHCP option 82 enables a DHCP relay agent to insert specific information into a DHCP request packets when forwarding client DHCP packets to a DHCP server and remove the specific information from a DHCP reply packets when forwarding server DHCP packets to a DHCP client. The DHCP server can use this information to implement IP address or other assignment policies. Specifically the option works by setting two sub-options: Circuit ID (option 1) and Remote ID (option2). The Circuit ID sub-option is supposed to include information specific to which circuit the request came in on. The Remote ID sub-option was designed to carry information relating to the remote host end of the circuit.

The definition of Circuit ID in the switch is 4 bytes in length and the format is "vlan_id" "module_id" "port_no". The parameter of "vlan_id" is the first two bytes represent the VLAN ID. The parameter of "module_id" is the third byte for the module ID (in standalone switch it always equal 0, in stackable switch it means switch ID). The parameter of "port_no" is the fourth byte and it means the port number.
The Remote ID is 6 bytes in length, and the value is equal the DHCP relay agents MAC address.

DHCP Snooping

DHCP Snooping is used to block intruder on the untrusted ports of the switch device when it tries to intervene by injecting a bogus DHCP reply packet to a legitimate conversation between the DHCP client and server.

DNS

DNS is an acronym for **D**omain **N**ame **S**ystem. It stores and associates many types of information with domain names. Most importantly, DNS translates human-friendly domain names and computer hostnames into computer-friendly IP addresses. For example, the domain name www.example.com might translate to 192.168.0.1.

DoS

DoS is an acronym for **D**enial of **S**ervice. In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services. By targeting at network sites or network connection, an attacker may be able to prevent network users from accessing email, web sites, online accounts (banking, etc.), or other services that rely on the affected computer.

Dotted Decimal Notation

Dotted Decimal Notation refers to a method of writing IP addresses using decimal numbers and dots as separators between octets.
An IPv4 dotted decimal address has the form x.y.z.w, where x, y, z, and w are decimal numbers between 0 and 255.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

DSCP

DSCP is an acronym for **D**ifferentiated **S**ervices **C**ode **P**oint. It is a field in the header of IP packets for packet classification purposes.

E

EEE

EEE is an abbreviation for Energy Efficient Ethernet defined in IEEE 802.3az.

EPS

EPS is an abbreviation for Ethernet Protection Switching defined in ITU/T G.8031.

Ethernet Type

Ethernet Type, or EtherType, is a field in the Ethernet MAC header, defined by the Ethernet networking standard. It is used to indicate which protocol is being transported in an Ethernet frame.

F

FTP

FTP is an acronym for **F**ile **T**ransfer **P**rotocol. It is a transfer protocol that uses the Transmission Control Protocol (TCP) and provides file writing and reading. It also provides directory service and security features.

Fast Leave

IGMP snooping Fast Leave processing allows the switch to remove an interface from the forwarding-table entry without first sending out group specific queries to the interface. The VLAN interface is pruned from the multicast tree for the multicast group specified in the original leave message. Fast-leave processing ensures optimal bandwidth management for all hosts on a switched network, even when multiple multicast groups are in use simultaneously.

H

HTTP

HTTP is an acronym for **H**ypertext **T**ransfer **P**rotocol. It is a protocol that used to transfer or convey information on the World Wide Web (WWW).

HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web Page. The other main standard that controls how the World Wide Web works is HTML, which covers how Web Pages are formatted and displayed.

Any Web server machine contains, in addition to the Web Page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. The Web browser is an HTTP client, sending requests to server machines. An HTTP client initiates a request by establishing a Transmission Control Protocol (TCP)

SEC.RU | Короткий путь к информации
Скачано с sec.ru

connection to a particular port on a remote host (port 80 by default). An HTTP server listening on that port waits for the client to send a request message.

HTTPS

HTTPS is an acronym for **H**ypertext **T**ransfer **P**rotocol over **S**ecure Socket Layer. It is used to indicate a secure HTTP connection.

HTTPS provide authentication and encrypted communication and is widely used on the World Wide Web for security-sensitive communication such as payment transactions and corporate logons.

HTTPS is really just the use of Netscape's Secure Socket Layer (SSL) as a sublayer under its regular HTTP application layering. (HTTPS uses port 443 instead of HTTP port 80 in its interactions with the lower layer, TCP/IP.) SSL uses a 40-bit key size for the RC4 stream encryption algorithm, which is considered an adequate degree of encryption for commercial exchange.

I

ICMP

ICMP is an acronym for **I**nternet **C**ontrol **M**essage **P**rotocol. It is a protocol that generated the error response, diagnostic or routing purposes. ICMP messages generally contain information about routing difficulties or simple exchanges such as time-stamp or echo transactions. For example, the PING command uses ICMP to test an Internet connection.

IEEE 802.1X

IEEE 802.1X is an IEEE standard for port-based Network Access Control. It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails. With 802.1X, access to all switch ports can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

IGMP

IGMP is an acronym for **I**nternet **G**roup **M**anagement **P**rotocol. It is a communications protocol used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and adjacent multicast routers to establish multicast group memberships. It is an integral part of the IP multicast specification, like ICMP for unicast connections. IGMP can be used for online video and gaming, and allows more efficient use of resources when supporting these uses.

IGMP Querier

A router sends IGMP Query messages onto a particular link. This router is called the Querier.

IMAP

IMAP is an acronym for **I**nternet **M**essage **A**ccess **P**rotocol. It is a protocol for email clients to retrieve email messages

SEC.RU | Короткий путь к информации
Скачано с sec.ru

from a mail server.

IMAP is the protocol that IMAP clients use to communicate with the servers, and SMTP is the protocol used to transport mail to an IMAP server.

The current version of the Internet Message Access Protocol is IMAP4. It is similar to Post Office Protocol version 3 (POP3), but offers additional and more complex features. For example, the IMAP4 protocol leaves your email messages on the server rather than downloading them to your computer. If you wish to remove your messages from the server, you must use your mail client to generate local folders, copy messages to your local hard drive, and then delete and expunge the messages from the server.

IP

IP is an acronym for **I**nternet **P**rotocol. It is a protocol used for communicating data across a internet network.

IP is a "best effort" system, which means that no packet of information sent over it is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IPMC

IPMC is an acronym for **IP** **M**ulti**C**ast.

IP Source Guard

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

SEC.RU | Короткий путь к информации
Скачано с sec.ru

L

LACP

LACP is an IEEE 802.3ad standard protocol. The **L**ink **A**ggregation **C**ontrol **P**rotocol, allows bundling several physical ports together to form a single logical port.

LLDP

LLDP is an IEEE 802.1ab standard protocol.

The **L**ink **L**ayer **D**iscovery **P**rotocol(LLDP) specified in this standard allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN, the major capabilities provided by the system incorporating that station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the stations point of attachment to the IEEE 802 LAN required by those management entity or entities. The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) using a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP-MED

LLDP-MED is an extendsion of IEEE 802.1ab and is defined by the telecommunication industry association (TIA-1057).

LOC

LOC is an acronym for **L**oss **O**f **C**onnectivity and is detected by a MEP and is indicating lost connectivity in the network. Can be used as a switch criteria by EPS

M

MAC Table

Switching of frames is based upon the DMAC address contained in the frame. The switch builds up a table that maps MAC addresses to switch ports for knowing which ports the frames should go to (based upon the DMAC address in the frame). This table contains both static and dynamic entries. The static entries are configured by the network administrator if the administrator wants to do a fixed mapping between the DMAC address and switch ports.

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frame with the corresponding SMAC address have been seen after a configurable age time.

MEP

SEC.RU | Короткий путь к информации
Скачано с sec.ru

MEP is an acronym for **M**aintenance **E**ntity **E**ndpoint and is an endpoint in a Maintenance Entity Group (ITU-T Y.1731).

MD5

MD5 is an acronym for **M**essage-**D**igest algorithm **5**. MD5 is a message digest algorithm, used cryptographic hash function with a 128-bit hash value. It was designed by Ron Rivest in 1991. MD5 is officially defined in RFC 1321 - The MD5 Message-Digest Algorithm.

Mirroring

For debugging network problems or monitoring network traffic, the switch system can be configured to mirror frames from multiple ports to a mirror port. (In this context, mirroring a frame is the same as copying the frame.)

Both incoming (source) and outgoing (destination) frames can be mirrored to the mirror port.

MLD

MLD is an acronym for **M**ulticast **L**istener **D**iscovery for IPv6. MLD is used by IPv6 routers to discover multicast listeners on a directly attached link, much as IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

MVR

Multicast VLAN Registration (MVR) is a protocol for Layer 2 (IP)-networks that enables multicast-traffic from a source VLAN to be shared with subscriber-VLANs.
The main reason for using MVR is to save bandwidth by preventing duplicate multicast streams being sent in the core network, instead the stream(s) are received on the MVR-VLAN and forwarded to the VLANs where hosts have requested it/them(Wikipedia).

N

NAS

NAS is an acronym for Network Access Server. The NAS is meant to act as a gateway to guard access to a protected source. A client connects to the NAS, and the NAS connects to another resource asking whether the client's supplied credentials are valid. Based on the answer, the NAS then allows or disallows access to the protected resource. An example of a NAS implementation is IEEE 802.1X.

NetBIOS

NetBIOS is an acronym for **Net**work **B**asic **I**nput/**O**utput **S**ystem. It is a program that allows applications on separate computers to communicate within a Local Area Network (LAN), and it is not supported on a Wide Area Network (WAN).

The NetBIOS giving each computer in the network both a NetBIOS name and an IP address corresponding to a different host name, provides the session and transport services described in the Open Systems Interconnection (OSI) model.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

NFS

NFS is an acronym for **N**etwork **F**ile **S**ystem. It allows hosts to mount partitions on a remote system and use them as though they are local file systems.

NFS allows the system administrator to store resources in a central location on the network, providing authorized users continuous access to them, which means NFS supports sharing of files, printers, and other resources as persistent storage over a computer network.

NTP

NTP is an acronym for **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. NTP uses UDP (datagrams) as transport layer.

O

OAM

OAM is an acronym for **O**peration **A**dministration and **M**aintenance.

It is a protocol described in ITU-T Y.1731 used to implement carrier ethernet functionality. MEP functionality like CC and RDI is based on this.

Optional TLVs.

A LLDP frame contains multiple TLVs

For some TLVs it is configurable if the switch shall include the TLV in the LLDP frame. These TLVs are known as optional TLVs. If an optional TLVs is disabled the corresponding information is not included in the LLDP frame.

OUI

OUI is the organizationally unique identifier. An OUI address is a globally unique identifier assigned to a vendor by IEEE. You can determine which vendor a device belongs to according to the OUI address which forms the first 24 bits of a MAC address.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

P

PCP

PCP is an acronym for Priority Code Point. It is a 3-bit field storing the priority level for the 802.1Q frame. It is also known as User Priority.

PD

PD is an acronym for **P**owered **D**evice. In a PoE> system the power is delivered from a PSE (power sourcing equipment) to a remote device. The remote device is called a PD.

PHY

PHY is an abbreviation for Physical Interface Transceiver and is the device that implement the Ethernet physical layer (IEEE-802.3).

PING

ping is a program that sends a series of packets over a network or the Internet to a specific computer in order to generate a response from that computer. The other computer responds with an acknowledgment that it received the packets. Ping was created to verify whether a specific computer on a network or the Internet exists and is connected.

ping uses Internet Control Message Protocol (ICMP) packets. The PING Request is the packet from the origin computer, and the PING Reply is the packet response from the target.

Policer

A policer can limit the bandwidth of received frames. It is located in front of the ingress queue.

POP3

POP3 is an acronym for **P**ost **O**ffice **P**rotocol version 3. It is a protocol for email clients to retrieve email messages from a mail server.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

An alternative protocol is Internet Message Access Protocol (IMAP). IMAP provides the user with more capabilities for retaining e-mail on the server and for organizing it in folders on the server. IMAP can be thought of as a remote file server.

POP and IMAP deal with the receiving of e-mail and are not to be confused with the Simple Mail Transfer Protocol (SMTP). You send e-mail with SMTP, and a mail handler receives it on your recipient's behalf. Then the mail is read

SEC.RU | Короткий путь к информации
Скачано с sec.ru

using POP or IMAP. IMAP4 and POP3 are the two most prevalent Internet standard protocols for e-mail retrieval. Virtually all modern e-mail clients and servers support both.

PPPoE

PPPoE is an acronym for Point-to-Point Protocol over Ethernet.
It is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. It is used mainly with ADSL services where individual users connect to the ADSL transceiver (modem) over Ethernet and in plain Metro Ethernet networks (Wikipedia).

Private VLAN

In a private VLAN, communication between ports in that private VLAN is not permitted. A VLAN can be configured as a private VLAN.

PTP

PTP is an acronym for Precision Time Protocol, a network protocol for synchronizing the clocks of computer systems.

Q

QCE

QCE is an acronym for **Q**oS **C**ontrol **E**ntry. It describes QoS class associated with a particular QCE ID.

There are six QCE frame types: Ethernet Type, VLAN, UDP/TCP Port, DSCP, TOS, and Tag Priority. Frames can be classified by one of 4 different QoS classes: "Low", "Normal", "Medium", and "High" for individual application.

QCL

QCL is an acronym for **Q**oS **C**ontrol **L**ist. It is the list table of QCEs, containing QoS control entries that classify to a specific QoS class on specific traffic objects.

Each accessible traffic object contains an identifier to its QCL. The privileges determine specific traffic object to specific QoS class.

QL

QL In SyncE this is the Quality Level of a given clock source. This is received on a port in a SSM indicating the quality of the clock received in the port.

QoS

QoS is an acronym for **Q**uality **o**f **S**ervice. It is a method to guarantee a bandwidth relationship between individual applications or protocols.

A communications network transports a multitude of applications and data, including high-quality video and delay-sensitive data such as real-time voice. Networks must provide secure, predictable, measurable, and sometimes guaranteed services.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Achieving the required QoS becomes the secret to a successful end-to-end business solution. Therefore, QoS is the set of techniques to manage network resources.

QoS class

Every incoming frame is classified to a QoS class, which is used throughout the device for providing queuing, scheduling and congestion control guarantees to the frame according to what was configured for that specific 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.

R

RARP

RARP is an acronym for **R**everse **A**ddress **R**esolution **P**rotocol. It is a protocol that is used to obtain an IP address for a given hardware address, such as an Ethernet address. RARP is the complement of ARP.

RADIUS

RADIUS is an acronym for **R**emote **A**uthentication **D**ial In **U**ser **S**ervice. It is a networking protocol that provides centralized access, authorization and accounting management for people or computers to connect and use a network service.

RDI

RDI is an acronym for **R**emote **D**efect **I**ndication. It is a OAM functionallity that is used by a MEP to indicate defect detected to the remote peer MEP

Router Port

A router port is a port on the Ethernet switch that leads switch towards the Layer 3 multicast device.

RSTP

In 1998, the IEEE with document 802.1w introduced an evolution of STP: the **R**apid **S**panning **T**ree **P**rotocol, which provides for faster spanning tree convergence after a topology change. Standard IEEE 802.1D-2004 now incorporates RSTP and obsoletes STP, while at the same time being backwards-compatible with STP.

S

SAMBA

Samba is a program running under UNIX-like operating systems that provides seamless integration between UNIX and Microsoft Windows machines. Samba acts as file and print servers for Microsoft Windows, IBM OS/2, and other SMB client machines. Samba uses the Server Message Block (SMB) protocol and Common Internet File System (CIFS), which is the underlying protocol used in Microsoft Windows networking.

Samba can be installed on a variety of operating system platforms, including Linux, most common Unix platforms, OpenVMS, and IBM OS/2.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Samba can also register itself with the master browser on the network so that it would appear in the listing of hosts in Microsoft Windows "Neighborhood Network".

SHA

SHA is an acronym for **S**ecure **H**ash **A**lgorithm. It designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. Hash algorithms compute a fixed-length digital representation (known as a message digest) of an input data sequence (the message) of any length.

Shaper

A shaper can limit the bandwidth of transmitted frames. It is located after the ingress queues.

SMTP

SMTP is an acronym for **S**imple **M**ail **T**ransfer **P**rotocol. It is a text-based protocol that uses the Transmission Control Protocol (TCP) and provides a mail service modeled on the FTP file transfer service. SMTP transfers mail messages between systems and notifications regarding incoming mail.

SNAP

The SubNetwork Access Protocol (SNAP) is a mechanism for multiplexing, on networks using IEEE 802.2 LLC, more protocols than can be distinguished by the 8-bit 802.2 Service Access Point (SAP) fields. SNAP supports identifying protocols by Ethernet type field values; it also supports vendor-private protocol identifier.

SNMP

SNMP is an acronym for **S**imple **N**etwork **M**anagement **P**rotocol. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for network management. SNMP allow diverse network objects to participate in a network management architecture. It enables network management systems to learn network problems by receiving traps or change notices from network devices implementing SNMP.

SNTP

SNTP is an acronym for **S**imple **N**etwork **T**ime **P**rotocol, a network protocol for synchronizing the clocks of computer systems. SNTP uses UDP (datagrams) as transport layer.

SPROUT

Stack **P**rotocol using **ROU**ting **T**echnology. An advanced protocol for almost instantaneous discovery of topology changes within a stack as well as election of a master switch. SPROUT also calculates parameters for setting up each switch to perform shortest path forwarding within the stack.

SSID

Service **S**et **Id**entifier is a name used to identify the particular 802.11 wireless LANs to which a user wants to attach. A client device will receive broadcast messages from all access points within range advertising their SSIDs, and can choose one to connect to based on pre-configuration, or by displaying a list of SSIDs in range and asking the user to select one (wikipedia).

SSH

SEC.RU | Короткий путь к информации
Скачано с sec.ru

SSH is an acronym for **S**ecure **SH**ell. It is a network protocol that allows data to be exchanged using a secure channel between two networked devices. The encryption used by SSH provides confidentiality and integrity of data over an insecure network. The goal of SSH was to replace the earlier rlogin, TELNET and rsh protocols, which did not provide strong authentication or guarantee confidentiality (Wikipedia).

SSM

SSM In SyncE this is an abbreviation for Synchronization Status Message and is containing a QL indication.

STP

Spanning **T**ree **P**rotocol is an OSI layer-2 protocol which ensures a loop free topology for any bridged LAN. The original STP protocol is now obsoleted by RSTP.

SyncE

SyncE Is an abbreviation for Synchronous Ethernet. This functionality is used to make a network 'clock frequency' synchronized. Not to be confused with real time clock synchronized (IEEE 1588).

T

TACACS+

TACACS+ is an acronym for **T**erminal **A**cess **C**ontroller **A**ccess **C**ontrol **S**ystem **P**lus. It is a networking protocol which provides access control for routers, network access servers and other networked computing devices via one or more centralized servers. TACACS+ provides separate authentication, authorization and accounting services.

Tag Priority

Tag Priority is a 3-bit field storing the priority level for the 802.1Q frame.

TCP

TCP is an acronym for **T**ransmission **C**ontrol **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

The TCP protocol guarantees reliable and in-order delivery of data from sender to receiver and distinguishes data for multiple connections by concurrent applications (for example, Web server and e-mail server) running on the same host.

The applications on networked hosts can use TCP to create connections to one another. It is known as a connection-oriented protocol, which means that a connection is established and maintained until such time as the message or messages to be exchanged by the application programs at each end have been exchanged. TCP is responsible for ensuring that a message is divided into the packets that IP manages and for reassembling the packets back into the complete message at the other end.

Common network applications that use TCP include the World Wide Web (WWW), e-mail, and File Transfer Protocol (FTP).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

TELNET

TELNET is an acronym for **TEL**etype **NET**work. It is a terminal emulation protocol that uses the Transmission Control Protocol (TCP) and provides a virtual connection between TELNET server and TELNET client.

TELNET enables the client to control the server and communicate with other servers on the network. To start a Telnet session, the client user must log in to a server by entering a valid username and password. Then, the client user can enter commands through the Telnet program just as if they were entering commands directly on the server console.

TFTP

TFTP is an acronym for **T**rivial **F**ile **T**ransfer **P**rotocol. It is transfer protocol that uses the User Datagram Protocol (UDP) and provides file writing and reading, but it does not provides directory service and security features.

ToS

ToS is an acronym for **T**ype **o**f **S**ervice. It is implemented as the IPv4 ToS priority control. It is fully decoded to determine the priority from the 6-bit ToS field in the IP header. The most significant 6 bits of the ToS field are fully decoded into 64 possibilities, and the singular code that results is compared against the corresponding bit in the IPv4 ToS priority control bit (0~63).

TLV

TLV is an acronym for **T**ype **L**ength **V**alue. A LLDP frame can contain multiple pieces of information. Each of these pieces of information is known as TLV.

TKIP

TKIP is an acronym for **T**emporal **K**ey **I**ntegrity **P**rotocol. It used in WPA to replace WEP with a new encryption algorithm. TKIP comprises the same encryption engine and RC4 algorithm defined for WEP. The key used for encryption in TKIP is 128 bits and changes the key used for each packet.

U

UDP

UDP is an acronym for **U**ser **D**atagram **P**rotocol. It is a communications protocol that uses the Internet Protocol (IP) to exchange the messages between computers.

UDP is an alternative to the Transmission Control Protocol (TCP) that uses the Internet Protocol (IP). Unlike TCP, UDP does not provide the service of dividing a message into packet datagrams, and UDP doesn't provide reassembling and sequencing of the packets. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange may prefer UDP to TCP.

UDP provides two services not provided by the IP layer. It provides port numbers to help distinguish different user requests and, optionally, a checksum capability to verify that the data arrived intact.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

Common network applications that use UDP include the Domain Name System (DNS), streaming media applications such as IPTV, Voice over IP (VoIP), and Trivial File Transfer Protocol (TFTP).

UPnP

UPnP is an acronym for **U**niversal **P**lug and **P**lay. The goals of UPnP are to allow devices to connect seamlessly and to simplify the implementation of networks in the home (data sharing, communications, and entertainment) and in corporate environments for simplified installation of computer components

User Priority

User Priority is a 3-bit field storing the priority level for the 802.1Q frame.

V

VLAN

Virtual LAN. A method to restrict communication between switch ports. VLANs can be used for the following applications:

VLAN unaware switching: This is the default configuration. All ports are VLAN unaware with Port VLAN ID 1 and members of VLAN 1. This means that MAC addresses are learned in VLAN 1, and the switch does not remove or insert VLAN tags.

VLAN aware switching: This is based on the IEEE 802.1Q standard. All ports are VLAN aware. Ports connected to VLAN aware switches are members of multiple VLANs and transmit tagged frames. Other ports are members of one VLAN, set up with this Port VLAN ID, and transmit untagged frames.

Provider switching: This is also known as Q-in-Q switching. Ports connected to subscribers are VLAN unaware, members of one VLAN, and set up with this unique Port VLAN ID. Ports connected to the service provider are VLAN aware, members of multiple VLANs, and set up to tag all frames. Untagged frames received on a subscriber port are forwarded to the provider port with a single VLAN tag. Tagged frames received on a subscriber port are forwarded to the provider port with a double VLAN tag.

VLAN ID

VLAN ID is a 12-bit field specifying the VLAN to which the frame belongs.

Voice VLAN

Voice VLAN is VLAN configured specially for voice traffic. By adding the ports with voice devices attached to voice VLAN, we can perform QoS-related configuration for voice data, ensuring the transmission priority of voice traffic and voice quality.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

W

WEP

WEP is an acronym for **W**ired **E**quivalent **P**rivacy. WEP is a deprecated algorithm to secure IEEE 802.11 wireless networks. Wireless networks broadcast messages using radio, so are more susceptible to eavesdropping than wired networks. When introduced in 1999, WEP was intended to provide confidentiality comparable to that of a traditional wired network (Wikipedia).

WiFi

WiFi is an acronym for **Wi**reless **Fi**delity. It is meant to be used generically when referring of any type of 802.11 network, whether 802.11b, 802.11a, dual-band, etc. The term is promulgated by the Wi-Fi Alliance.

WPA

WPA is an acronym for **W**i-Fi **P**rotected **A**ccess. It was created in response to several serious weaknesses researchers had found in the previous system , Wired Equivalent Privacy (WEP). WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. WPA is specifically designed to also work with pre-WPA wireless network interface cards (through firmware upgrades), but not necessarily with first generation wireless access points. WPA2 implements the full standard, but will not work with some older network cards (Wikipedia).

WPA-PSK

WPA-PSK is an acronym for **W**i-Fi **P**rotected **A**ccess - **P**re **S**hared **K**ey. WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPA-Radius

WPA-Radius is an acronym for **W**i-Fi **P**rotected **A**ccess - Radius (802.1X authentication server). WPA was designed to enhance the security of wireless networks. There are two flavors of WPA: enterprise and personal. Enterprise is meant for use with an IEEE 802.1X authentication server, which distributes different keys to each user. Personal WPA utilizes less scalable 'pre-shared key' (PSK) mode, where every allowed computer is given the same passphrase. In PSK mode, security depends on the strength and secrecy of the passphrase. The design of WPA is based on a Draft 3 of the IEEE 802.11i standard (Wikipedia)

WPS

WPS is an acronym for **W**i-Fi **P**rotected **S**etup. It is a standard for easy and secure establishment of a wireless home network. The goal of the WPS protocol is to simplify the process of connecting any home device to the wireless network (Wikipedia).

SEC.RU | Короткий путь к информации
Скачано с sec.ru

WRES

WRED is an acronym for **W**eighted **R**andom **E**arly **D**etection. It is an active queue management mechanism that provides preferential treatment of higher priority frames when traffic builds up within a queue. A frame's DP level is used as input to WRED. A higher DP level assigned to a frame results in a higher probability that the frame is dropped during times of congestion.

WTR

WTR is an acronym for **W**ait **T**o **R**estore. This is the time a fail on a resource has to be 'not active' before restoration back to this (previously failing) resource is done.

SEC.RU | Короткий путь к информации
Скачано с sec.ru