ORIGO

L2 Switch Series

OS1326/OS1326P

User Manual

Introduction

OS1326/OS1326P Web User Manual provides features such as Administrator, Basic Configuration, VLAN Configuration, QoS Configuration, ACL Configuration, Security, Advanced Features and Monitoring. OS1326/OS1326P Switch support IE, Firefox, and Chrome.

Login OS1326/OS1326P Switch

Upon displaying Login Page, please input both default Username and Password.

Default IP address: 192.168.2.1

Default Username: admin

Default Password: admin

Note: Characters are case-sensitive. All Username and Password are in lower case.

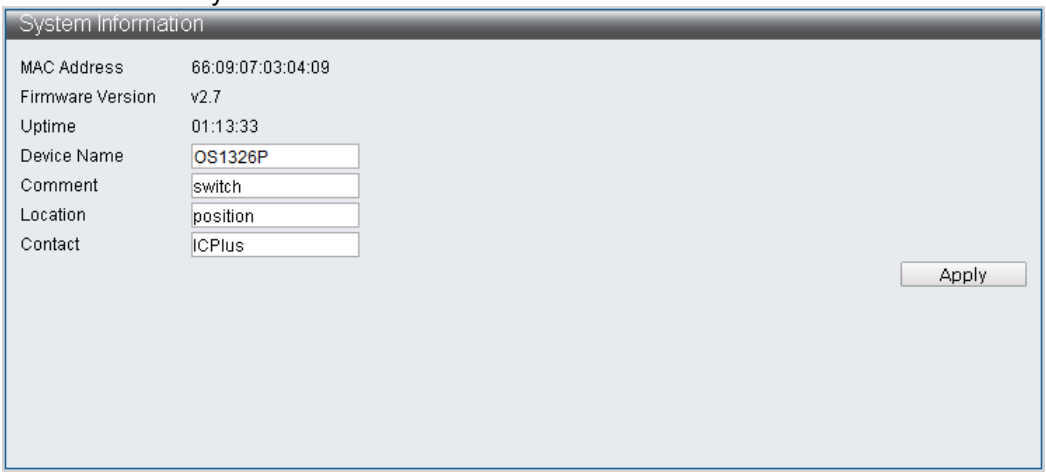
1 Administrator

1.1 System Information

System Information displays Ethernet Switch MAC Address, Firmware Version, Uptime, Device Name, Comment, Location and Contact Informcation.

System Information Configuration

Administrator -> System Information



Note：Space is limited to 15 letters.

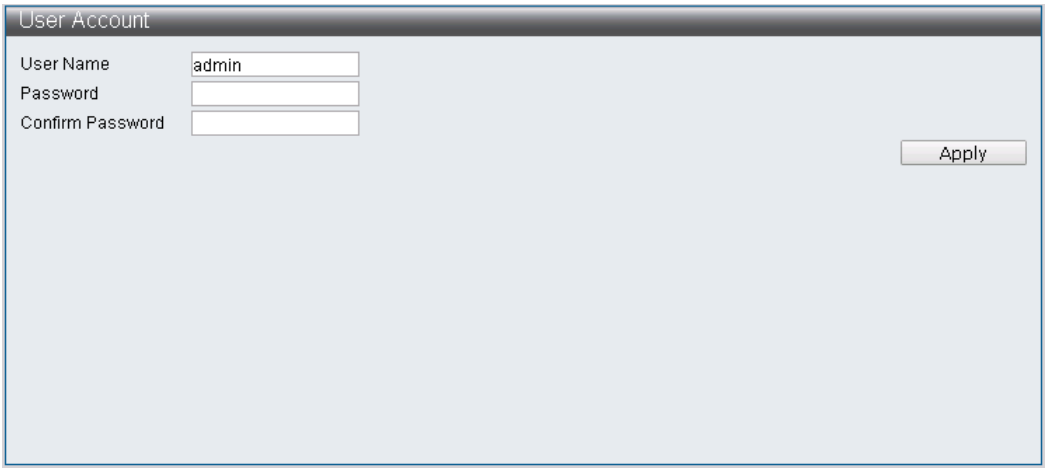
Parameter	Description
MAC Address	Display Ethernet MAC Address
Firmware Version	Software Version
Uptime	Machine-On Duration
Device Name	Name of the Device
Comment	Device Description
Location	Location Description
Contact	Receiver Description

1.2 Account/ Password

Users are required to input User Name and Passport.

Account/ Password Configuration

Administrator -> Account/ Password



Note：Space is limited to 15 letters.

Parameter	Description
User Name	Change Username
Password	Change Password
Confirm Password	Confirm Password

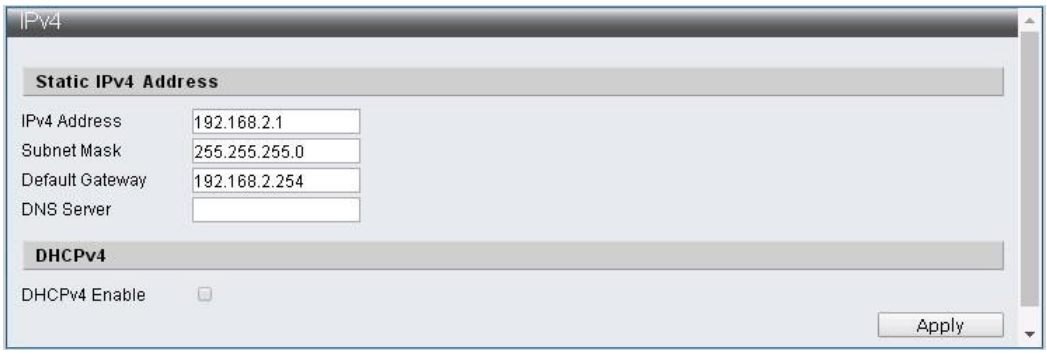
1.3 IP Configuration

IP Configuration allows users to configure IPv4 Address and IPv6 Address or allocated random value by DHCP Server.

1.3.1 IPv4

IPv4 Configuration

Administrator -> IP Configuration -> IPv4



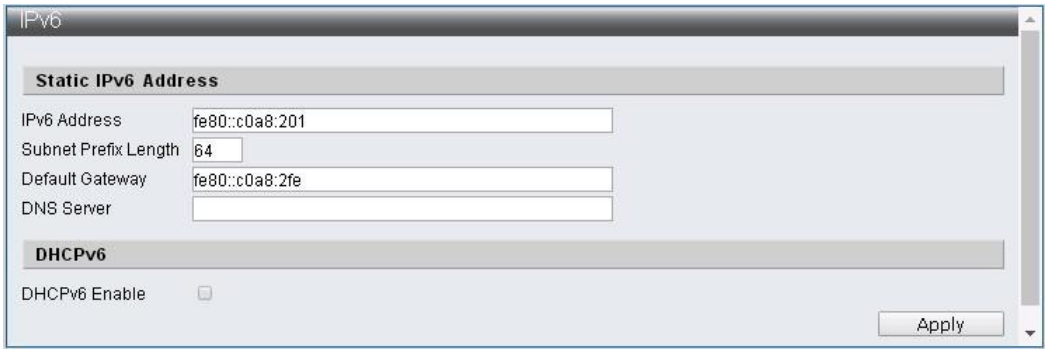
Note：Only numerical letters ranging from 0~9 are allowed.

Parameter	Description
IPv4 Address	Configure IPv4 Address
Subnet Mask	Configure IPv4 Subnet Mask
Default Gateway	Configure IPv4 Default Gateway
DNS Server	Configure IPv4 DNS Server
DHCPv4 Enable	Enable IPv4 DHCP Server

1.3.2 IPv6

IPv6 Configuration

Administrator -> IP Configuration -> IPv6



Note：Only numerical ranging from 0~9 and syllabus ranging from a~f are allowed.

Parameter	Description
IPv6 Address	Configure IPv6 Address
Subnet Prefix Length	Configure IPv6 Subnet Prefix Length
Default Gateway	Configure IPv6 Default Gateway
DNS Server	Configure IPv6 DNS Server
DHCPv6 Enable	Enable IPv6 DHCP Server

1.4 SNMP Settings

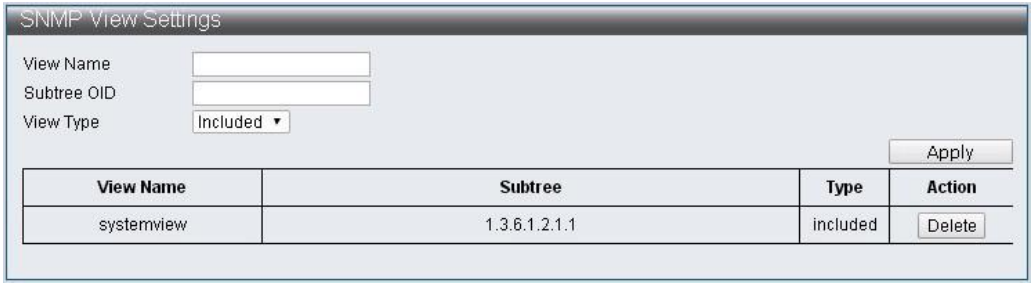
SNMP

Simple Network Management Protocol (SNMP) is an Internet Standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior. Devices that typically support SNMP include cable modems, routers, switches, servers, workstations, printers, and more. SNMP is widely used in network management for network monitoring. SNMP exposes management data in the form of variables on the managed systems organized in a management information base (MIB), which describe the system status and configuration. These variables can then be remotely queried (and, in some circumstances, manipulated) by managing applications. Three significant versions of SNMP have been developed and deployed. SNMPv1 is the original version of the protocol. More recent versions, SNMPv2c and SNMPv3, feature improvements in performance, flexibility and security. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force(IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

1.4.1 SNMP View Table

SNMP View Table Configuration

Administrator -> SNMP Settings -> SNMP View Table

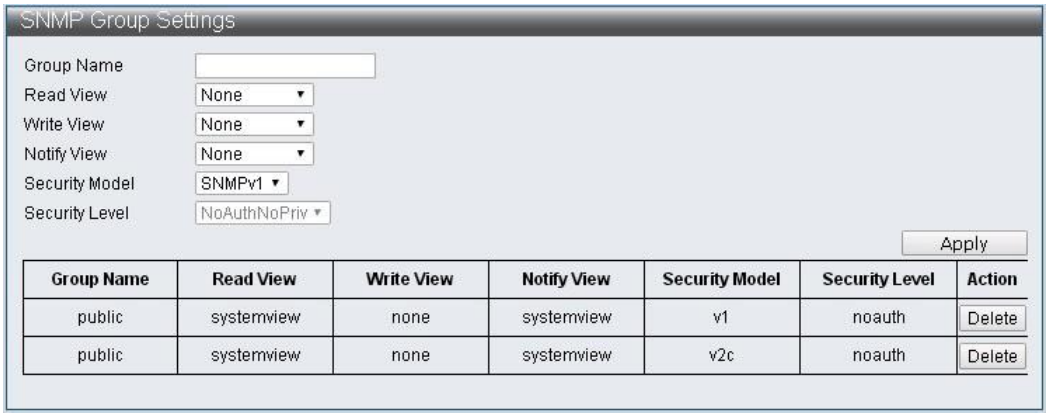


Parameter	Description
View Name	Create New View Name, limited to 20 letters
Subtree OID	Configure MIB Parameter
View Type	Define MIB Parameter of *included* and *excluded*
Delete	Delete existing View

1.4.2 SNMP Group Table

SNMP Group Table Configuration

Administrator -> SNMP Settings -> SNMP Group Table

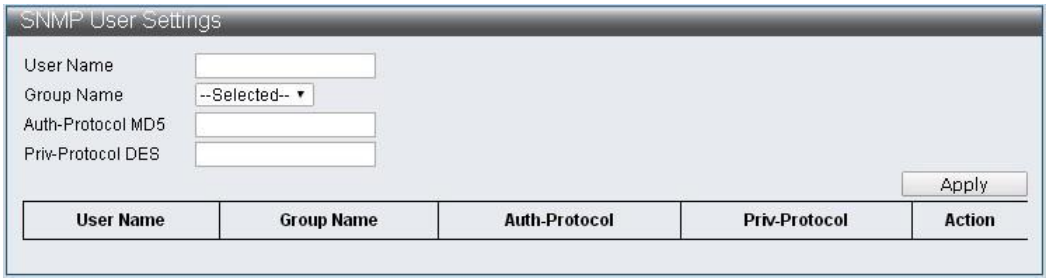


Parameter	Description
Group Name	Create New Group Name, limited to 20 letters
Read View	Configure Read View Authorization
Write View	Configure Write View Authorization
Notify View	Assign Trap View
Security Model	Assign SNMP
Security Level	Assign Security,support only SNMPv3 NoAuthNoPriv – Unlimited Access and No Encryption AuthNoPriv – Limited Access and No Encryption AuthPriv – Limited Access and Encrypted Packets
Delete	Delete existing Group

1.4.3 SNMP User Table

SNMP User Table Configuration

Administrator -> SNMP Settings -> SNMP User Table

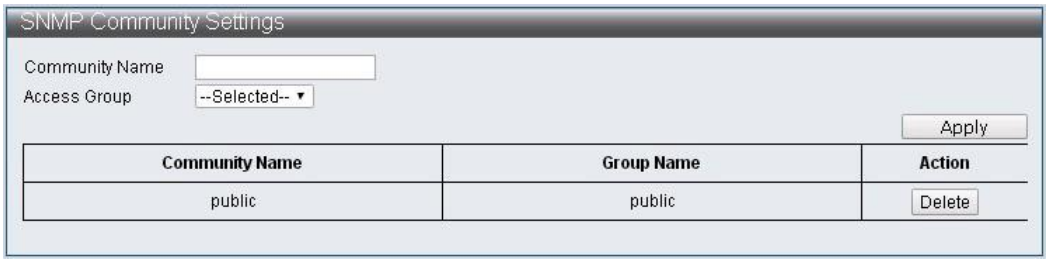


Parameter	Description
User Name	Configure New SNMPv3 Name, limited to 20 letters.
Group View	Configure New Group View
Auth-Protocol MD5	Configure Authentication using MD5 Protocol
Priv-Protocol DES	Configure Encryption using DES 56 Standard

1.4.4 SNMP Community Table

SNMP Community Table Configuration

Administrator -> SNMP Settings -> SNMP Community Table

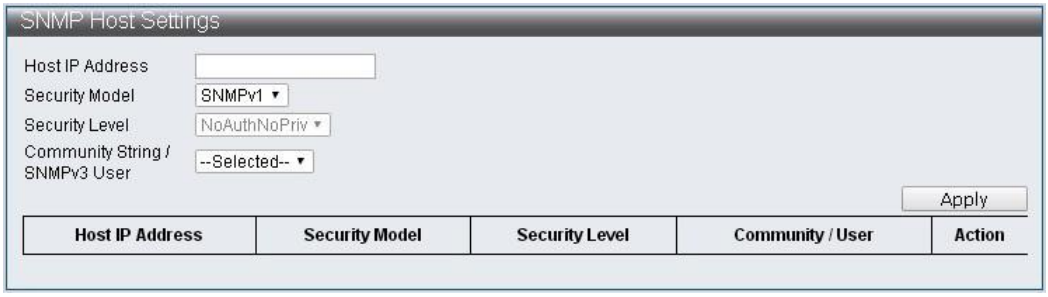


Parameter	Description
Community Name	Create New SNMPv1 / SNMPv2 Community Name, limited to 20 letters
Access Group	Configure New Access Group

1.4.5 SNMP Host Table

SNMP Host Table Configuration

Administrator -> SNMP Settings -> SNMP Host Table

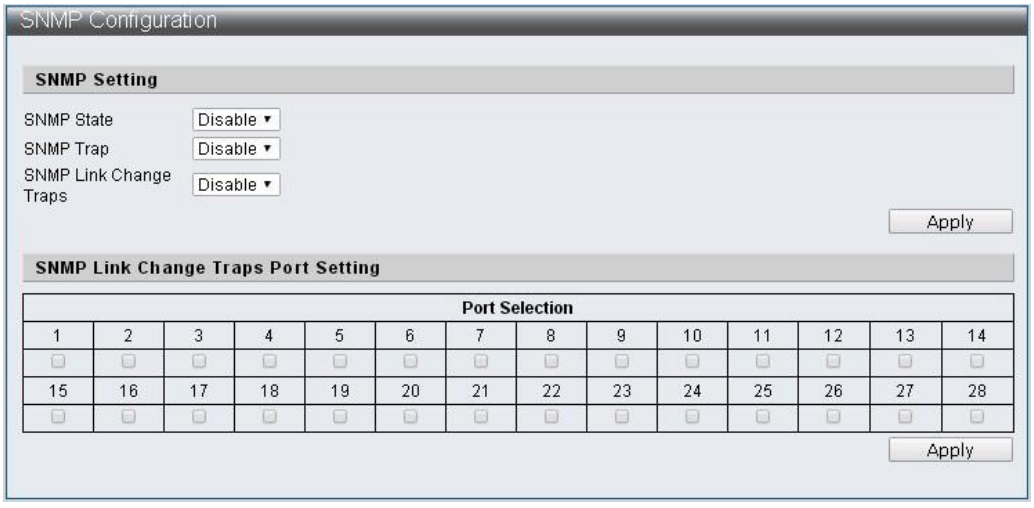


Parameter	Description
Host IP Address	Configure SNMP Trap Host IP Address
Security Model	Configure SNMP Version
Security Level	Assign Security, support only SNMPv3 NoAuthNoPriv – Unlimited Access and No Encryption AuthNoPriv – Limited Access and No Encryption AuthPriv – Limited Access and Encrypted Packets
Community String/SNMPv3 User	Input Community String or SNMPv3 Username Authentication

1.4.6 SNMP Configuration

SNMP Configuration

Administrator -> SNMP Settings -> SNMP Configuration



Parameter	Description
SNMP State	Enable / Disable SNMP Function
SNMP Trap	Enable / Disable SNMP Trap Function
SNMP Link Change Traps	Enable / Disable SNMP Link Change Traps
Port Selection	Configure Port Link Control

1.5 NTP Settings

NTP, Network Time Protocol, enables time calibration.

NTP Configuration

Administrator -> NTP Settings

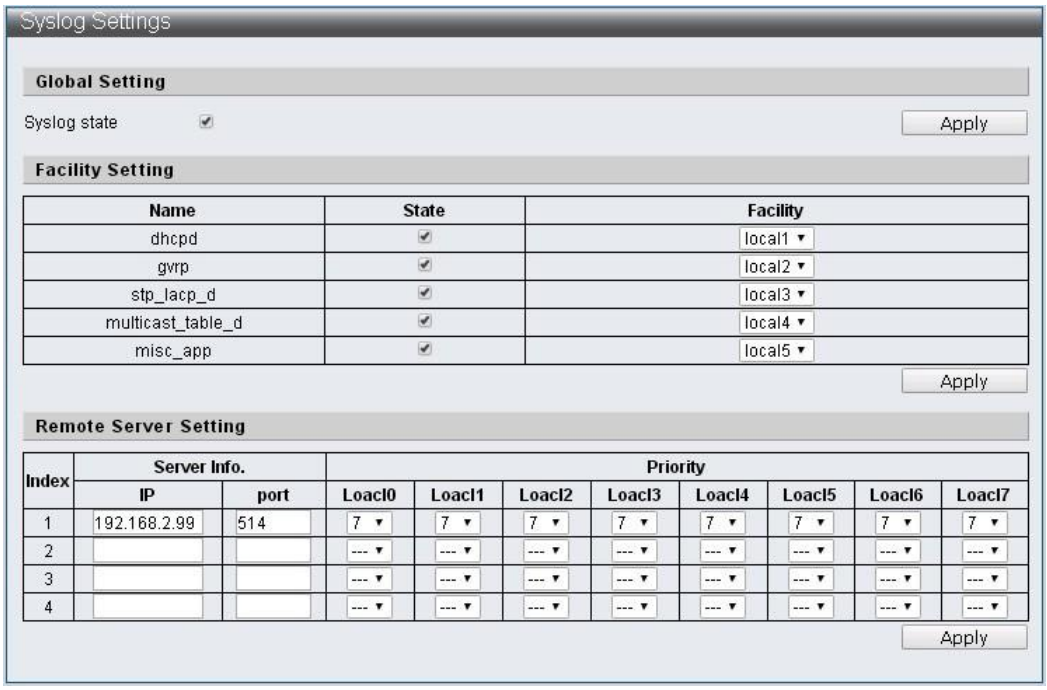
Parameter	Description
System Time	Display System Time
State	Enable / Disable NTP Function
Time Zone	Configure Time Zone
Primary Server IP	Configure Primary Server IP
Secondary Server IP	Configure Secondary Server IP

1.6 Syslog Settings

This page allows to Configure Syslog.

NTP Configuration

Administrator -> Syslog Settings



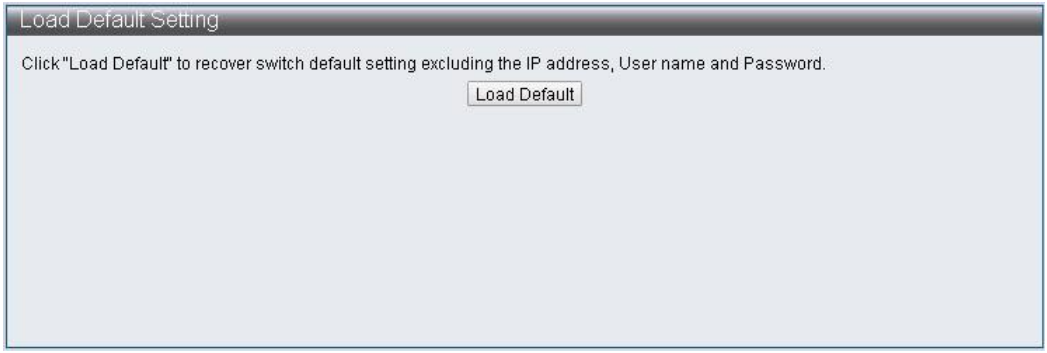
Parameter	Description
Syslog state	Enable Syslog
Name	Protocol
State	Enable / Disable Protocol
Facility	Configure Local Number
Server Info.	Configure IP Address and Port Number
Priority	Local Port Prioritize

1.7 Load Factory Default

This page allows the switch to return to original configuration.

Load Factory Default Configuration

Administrator -> Load Factory Default



Note: Loading Factory Default Setting will only reset OS1326/OS1326P Functions. It will not affect Username,Password, and IP Address.

Parameter	Description
Load Default	Return to Factory Default

1.8 Configuration

This page provides the administrator with a method to backup or recover the switch configuration. User may use Backup Feature to create a file call current.tar.gz. When user is in need of Restoring to previous setting, user may upload current.tar.gz in the Restore Feature.

1.8.1 Backup

Backup Configuration

Administrator -> Configuration -> Backup

Note: To proceed with Backup configuration, please apply and download file called current.tar.gz. This file is used when initiate Restore Configuration in the future.

1.8.2 Restore

Restore Configuration

Administrator -> Configuration -> Restore

Note: Applying current.tar.gz file will not effect IP Address.

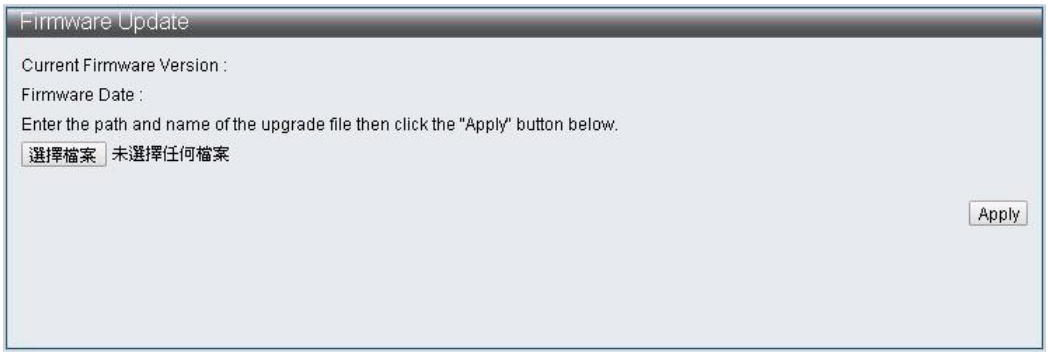
Parameter	Description
Select File	Apply current.tar.gz file

1.9 Firmware Update

This page allows user to update the latest version of OS1326/OS1326P Firmware. Locate the name of thefirmware file then click “Apply” to proceed with Firmware Update.

Firmware Update Configuration

Administrator -> Firmware Update



Parameter	Description
Select File	Apply Latest Version Firmware

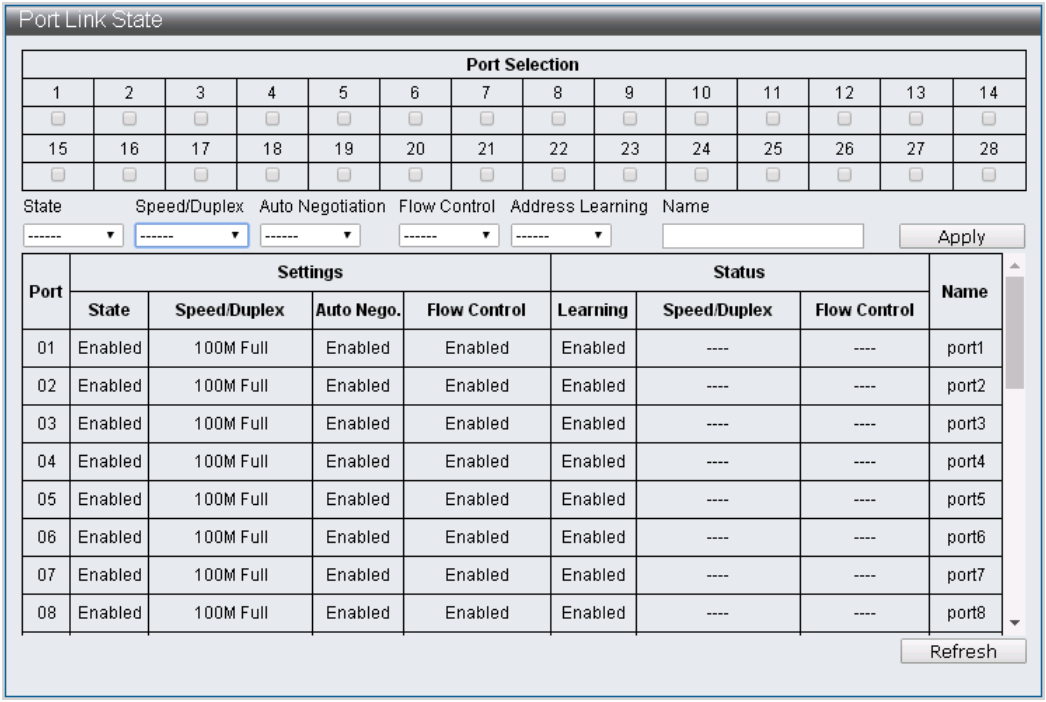
2 Port Management

2.1 Port Configuration

This page allows to configure individual port such as Power up / down, Speed, Duplex, Auto-Negotiation, Flow Control, Address Learning, and Port Name.

Port Configuration

Basic Configuration -> Port Configuration



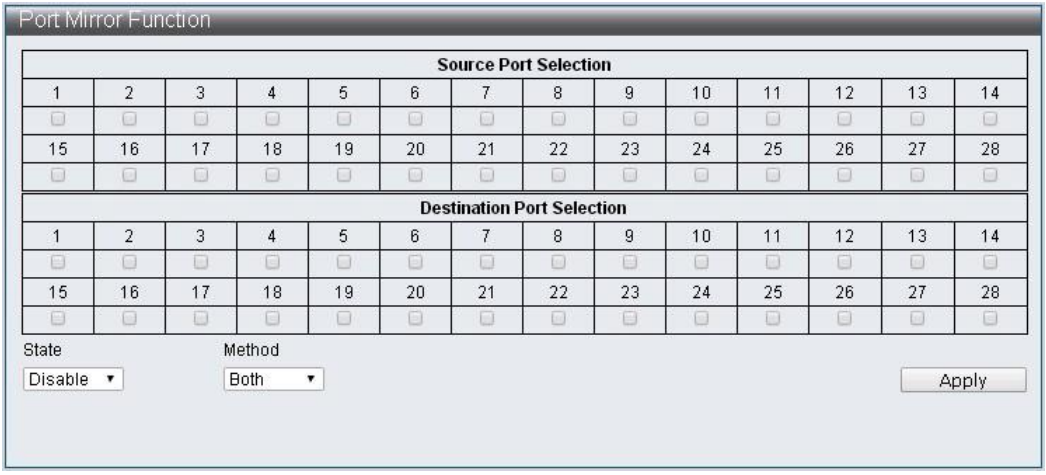
Parameter	Description
Port Selection	Selecting Corresponding Port
Settings	Display Port Selection
Status	Display Link Status
State	Power up/down
Speed/Duplex	Select Port Speed and Duplex
Auto Negotiation	Enable / Disable Auto-Negotiation
Flow Control	Enable / Disable Flow Control
Address Learning	Enable / Disable Address Learning
Name	Port Desciption
Refresh	Update Name

2.2 Port Mirror Function

Port Mirror Function is operated utilizing features such as Source Ports and Destination Ports to monitor and manage streaming bandwidth.

Port Mirror Function Configuration

Basic Configuration -> Port Mirror Function



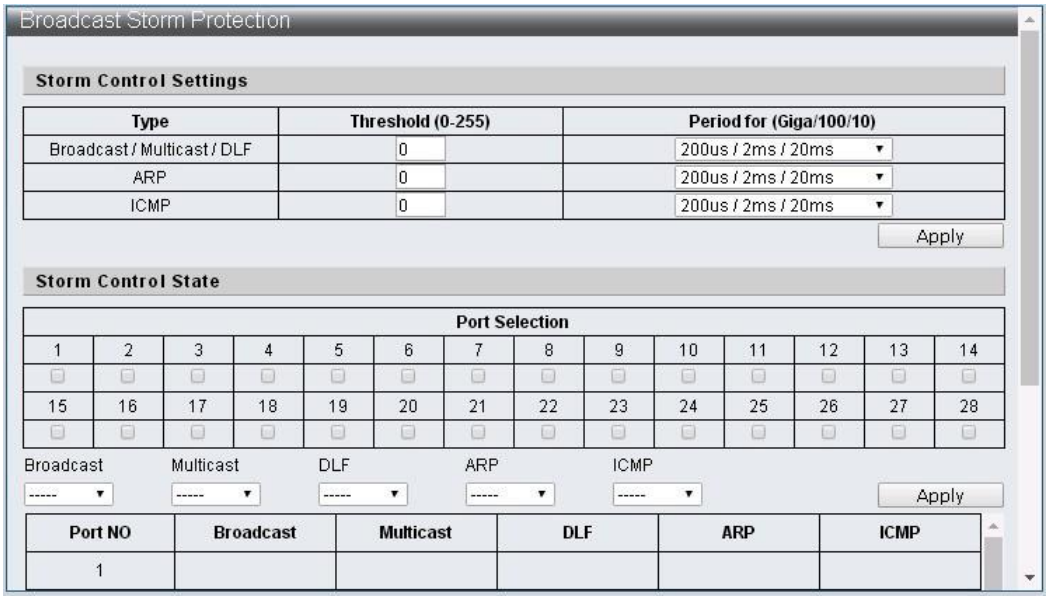
Parameter	Description
Source Port Selection	Selecting Corresponding Port
Destination Port Selection	Select Corresponding Destination Port
State	Enable / Disable Port Mirror Function
Method	Configure Full / Half Duplex Port Mirror Function

2.3 Broadcast Storm Protection

This page allows user to manage individual port by configuring Broadcast, Multicast, ARP, ICMP. The threshold is valid up to 255.

Broadcast Storm Protection Configuration

Basic Configuration -> Broadcast Storm Protection



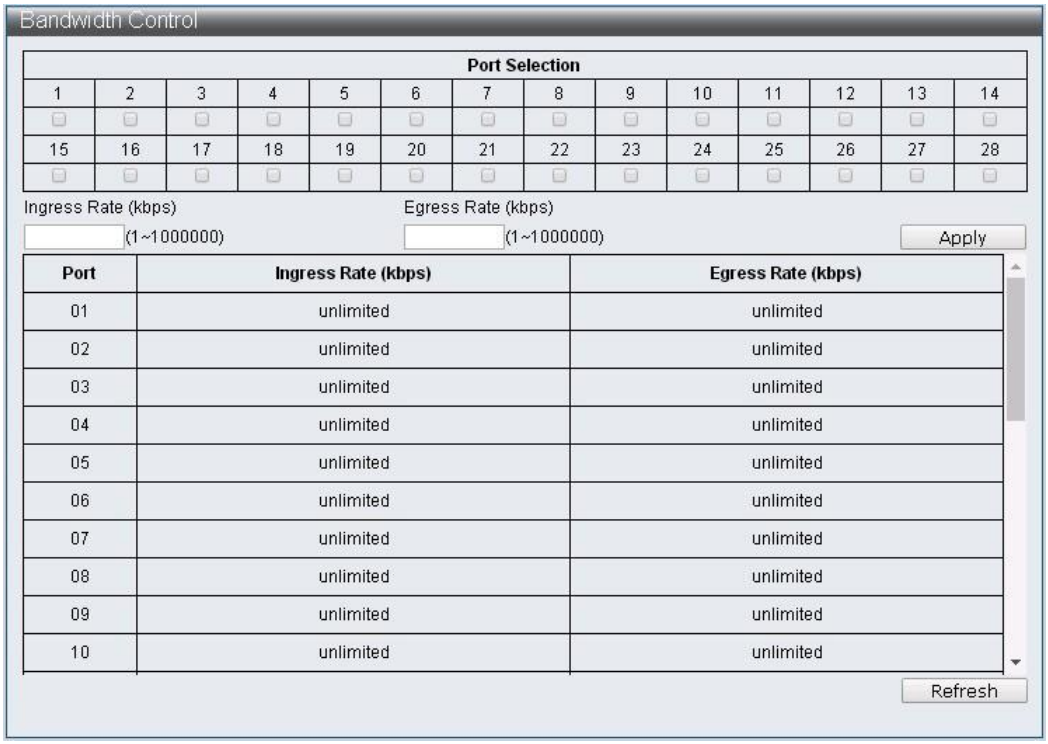
Parameter	Description
Type	The type of storm control Broadcast Multicast DLF ARP ICMP
Threshold	Configure the threshold of transmitting packet
Period for (Giga/100/10)	Configure the period
Port Selection	Selecting Corresponding Port
Broadcast	Enable / Disable Broadcast control
Multicast	Enable / Disable Multicast control
DLF	Enable / Disable DLF control
ARP	Enable / Disable ARP control
ICMP	Enable / Disable ICMP control

2.4 Bandwidth Control

This page allows user to configure the bandwidth for each port. Factory Default is configured to Highest Bandwidth.

Bandwidth Control Configuration

Basic Configuration -> Bandwidth Control



Parameter	Description
Port Selection	Selecting Corresponding Port
Ingress Rate	Configure Ingress Rate
Egress Rate	Configure Egress Rate
Refresh	Update Bandwidth Control Status

3 VLAN Configuration

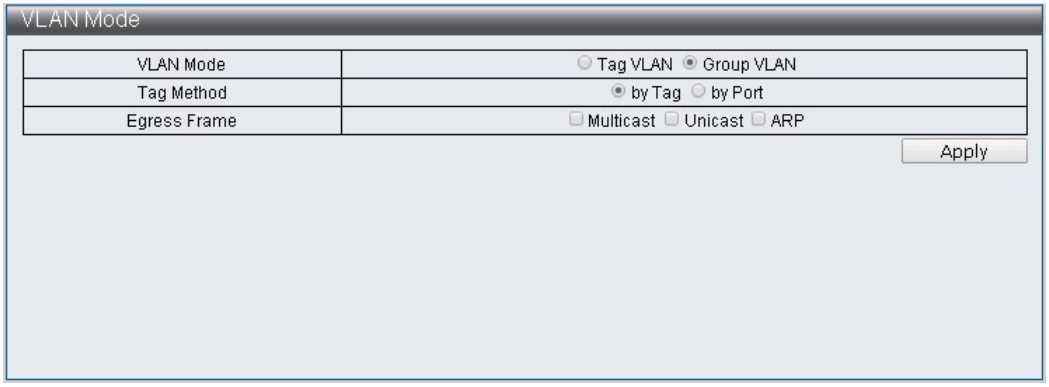
3.1 VLAN Mode

Virtual LAN allows user to configure the ports as a group to save switch bandwidth and increase network performance.

OS1326/OS1326P support both IEEE 802.1Q and Port-Based VLAN, untag function can remove 802.1Q tag from the packet to make sure the compatibility with devices which not support 802.1Q.

VLAN Mode Configuration

VLAN Configuration -> VLAN Mode

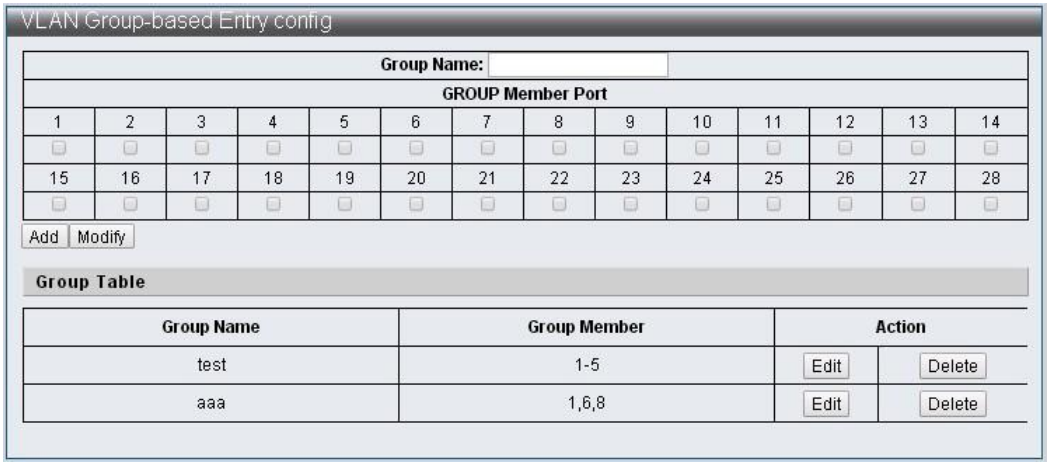


Parameter	Description
VLAN Mode	Tag VLAN: base on Tag-based Entry to define the VID and members of each entry. Group Vlan：base on Group-based Entry to define VLAN members.
Tag Method	Active only in Tag VLAN mode By Tag： add/remove tag base on Tag-based Entry setting By Port： add/remove tag base on port tagging setting in VLAN port config page.
Egress Frame	Selected packet（Muticast, Unicast and ARP) will be forwarded base on egress rule.

3.2 VLAN Group-based Entry Configuration

VLAN Group-based Entry Configuration

VLAN Configuration -> VLAN Group-based Entry Configuration



參數	說明
Group Name	Configure Group VLAN Name
Group Member Port	Configure Group VLAN Member
Add	Create New Group VLAN
Edit	Editing Group VLAN
Modify	Modify Group VLAN information
Delete	Delete selected Group VLAN

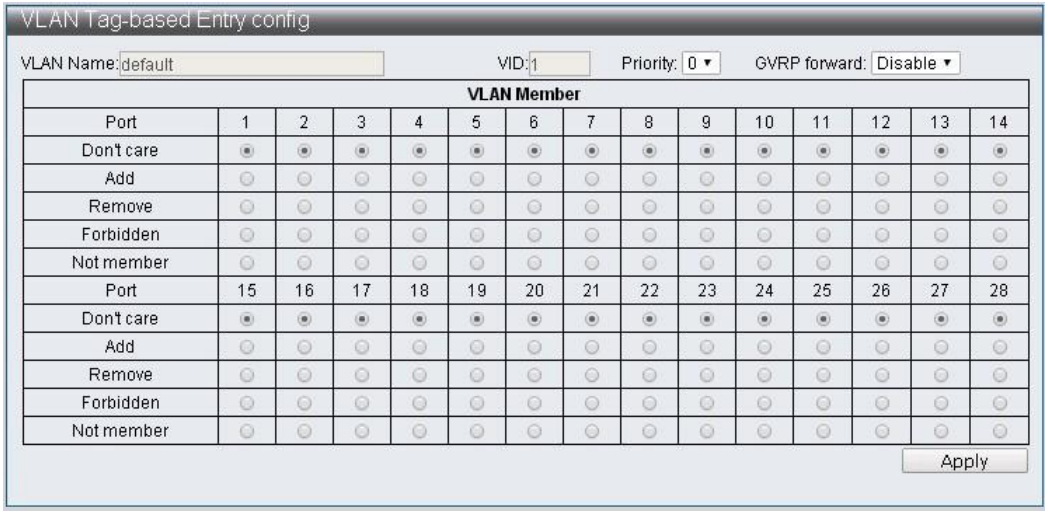
3.3 VLAN Tag-based Entry Configuration

VLAN Tag-based Entry Configuration

VLAN Configuration -> VLAN Tag-based Entry Configuration

Parameter	Description
Add	Add Tag VLAN entry and follow instruction to set Tag VLAN name and VID.
Edit	Edit selected Tag VLAN
Delete	Delete selected Tag VLAN

Tag VLAN webpage

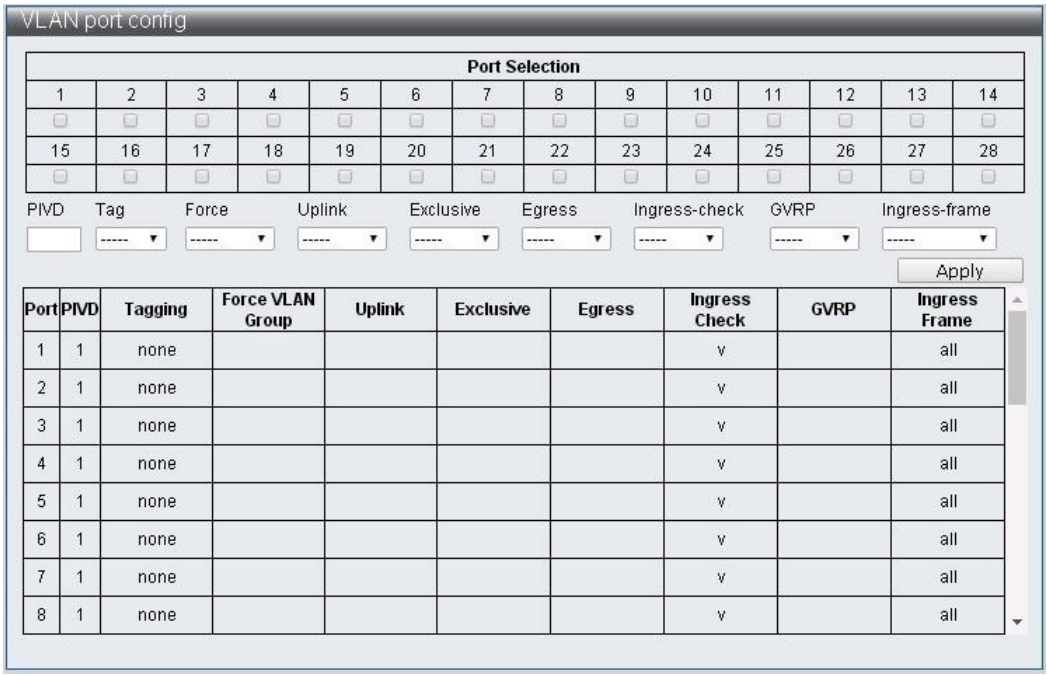


Parameter	Description
VLAN Name	Name of Tag VLAN
VID	Tag VLAN VID
Priority	Configure Tag VLAN Priority
GVRP forward	GVRP enable, define if Tag VLAN transmit through GVRP
VLAN Member	Configure Tag VLAN member
Don’t care	Not change tag information for date transmit from this port
Add	Add tag for date transmit from this port
Remove	Remove tag for date transmit from this port
Forbidden	Forbid individual port from configuring Tag VLAN through GVRP.
Not member	Not VLAN member

3.4 VLAN Port Configuration

VLAN Port Configuration

VLAN Configuration -> VLAN Port Configuration

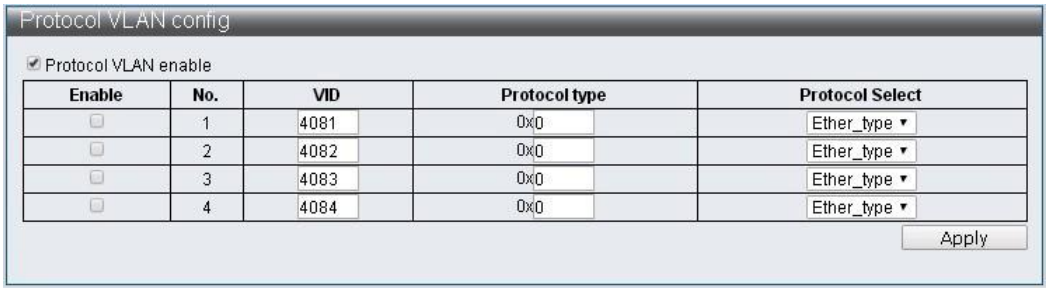


Parameter	Description
Port Selection	Select corresponding port
PVID	Configure Port VID
Tagging	Configure the selected Port to add or remove VLAN Tag for transmit packet
Force VLAN Group	Define if follow Group VLAN setting first.
Uplink	Define uplink port; when destination port is not in the same group, the packet will be forwarded from uplink port.
Exclusive	Define exclusive port: there is no data communication between selected exclusive ports.
Egress	define egress port；when destination port is not in the same group, the packet will be forwarded base on egress rule
Ingress Check	Enable ingress check；Check if the port is VLAN member through VID.
GVRP	Enable / Disable Port GVRP Feature
Ingress Frame	Allow to forward specific frame.

3.5 Protocol VLAN Configuration

Protocol VLAN Configuration

VLAN Configuration -> Protocol VLAN Configuration

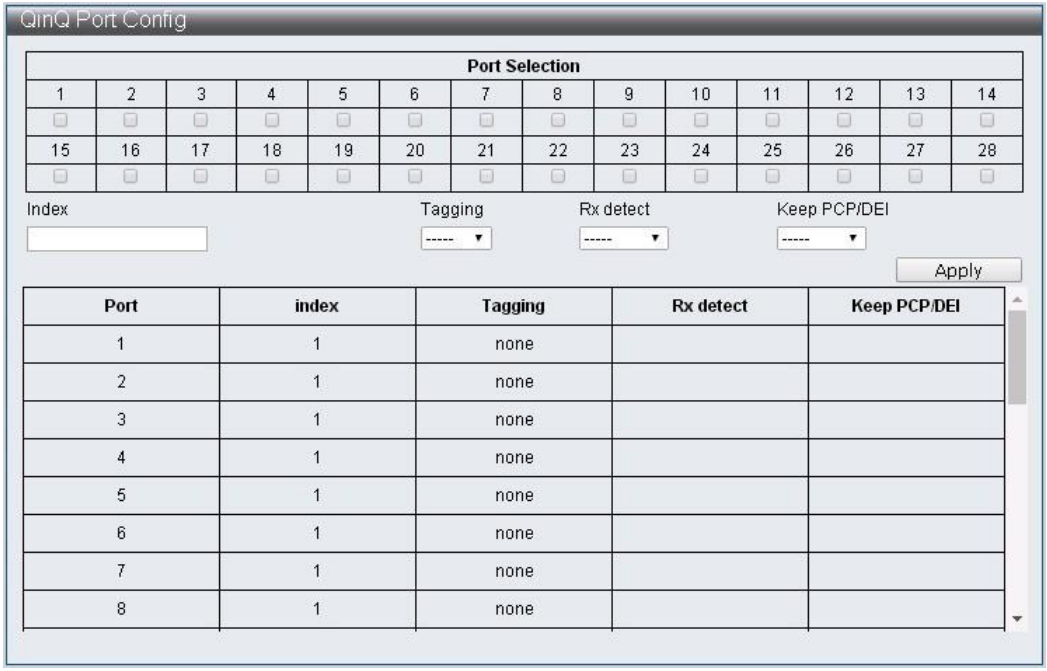


Parameter	Description
Protocol VLAN enable	Protocol VLAN On / Off
Enable check box	Select entry
VID	Configure VID, when the packet meet selected Protocol, will base on this VID to check VLAN Member
Protocol type	Configure Protocol type
Protocol Select	Ether Type：When configuring Ether Type, Protocol type settings must be greater than 0x0600, refer to the following format DA + SA + Protocol type LLC：Refer to the following format DA + SA + Length + Protocol type RFC 1042：Refer to the following format DA + SA + Length + AAAA03 + 000000 + Protocol type

3.6 QinQ Port Configuration

QinQ Port Configuration

VLAN Configuration -> QinQ Port Configuration

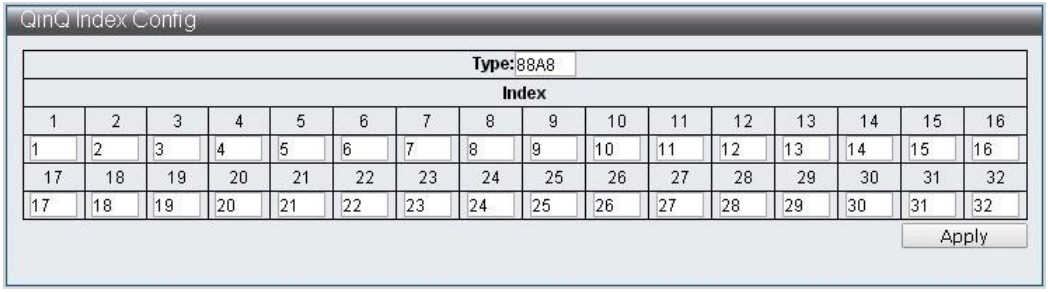


Parameter	Description
Port Selection	Select corresponding port
Index	Select Index, the Service tag of this Index can be set in QinQ Index Config webpage.
Tagging	Add：Add Service Tag on the packet, if the Service Tag already exist on packet, will base on Rx detect status to modify or replace Service tag. RMV： Remove Service tag when Rx detect enable.
Rx detect	Enable/Disable Service tag checking.
Keep PCP/DEI	Define if keep original PCP and DEI when modifying Service tag.

3.7 QinQ Index Configuration

QinQ Index Configuration

VLAN Configuration -> QinQ Index Configuration



Parameter	Description
Type	Configure Service Tag Type
Index	Configure Service Tag that is correlated to Index

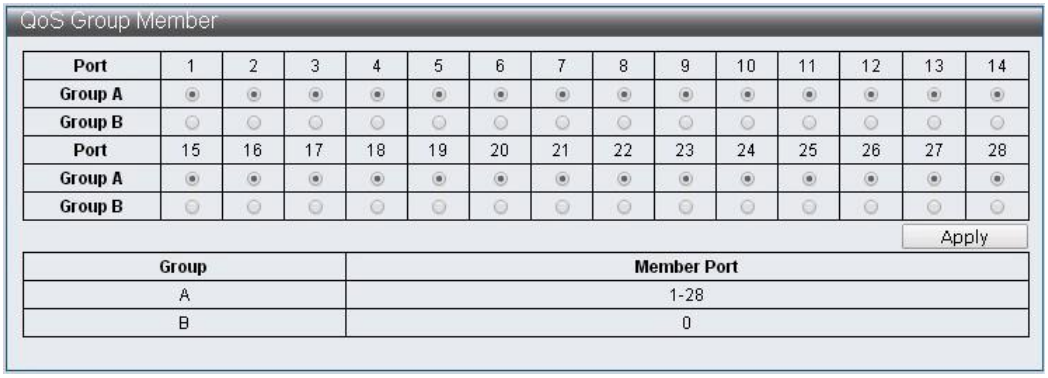
4 QoS(Quality of Service) Configuration

QoS is IEEE 802.1p, it allows user to define priority of specific packet to ensure the performance and bandwidth.

4.1 QoS Group Member

QoS Group Member Configuration

QoS Configuration -> QoS Group Member

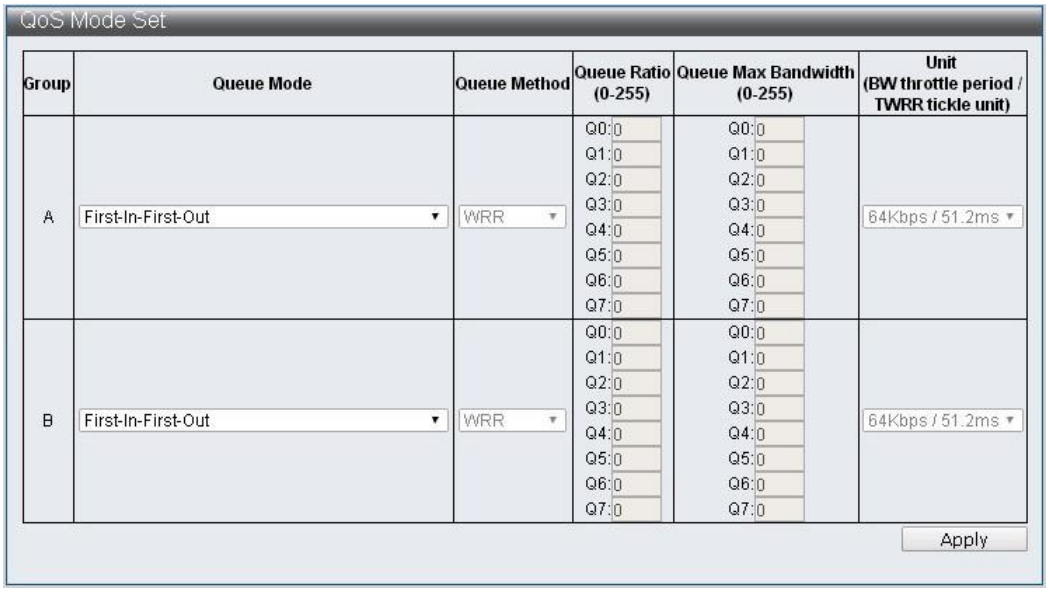


Parameter	Description
Group A	Select Group A Ports
Group B	Select Group B Ports

4.2 QoS Mode Set

QoS Mode Set Configuration

QoS Configuration -> QoS Mode Set

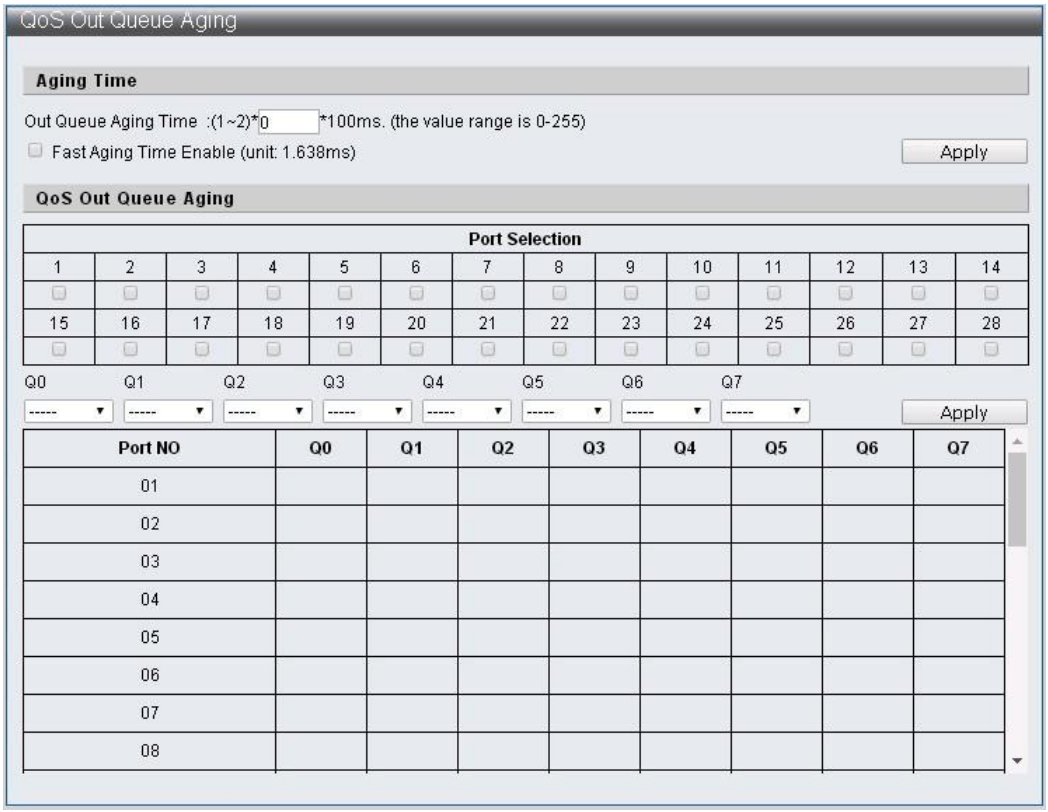


Parameter	Description
Queue Mode	Select QoS mode of each group 1. First-In-First-Out 2. SPx1+WRR/WFQ/BW/TWRRx7 3. SPx2+WRR/WFQ/BW/TWRRx6 4. SPx4+WRR/WFQ/BW/TWRRx4 5. SPx8
Queue Method	Select Queue method： 1. WRR: Weighted Round Robin 2. WFQ: Weighted Fair Queue 3. Bwassure Dynamic Bandwidth Management 4. Bwlimit Static Bandwidth Management 5. TWRR: Time Weighted Rate Return
Queue Ratio	Configure the weights of each mode.
Queue Max Bandwidth	Configure the max. bandwidth in Bwassure.
Unit (BW throttle period / TWRR tickle unit)	Configure the unit of weights in each mode.

4.3 QoS Out Queue Aging

QoS Out Queue Aging Configuration

QoS Configuration -> QoS Out Queue Aging

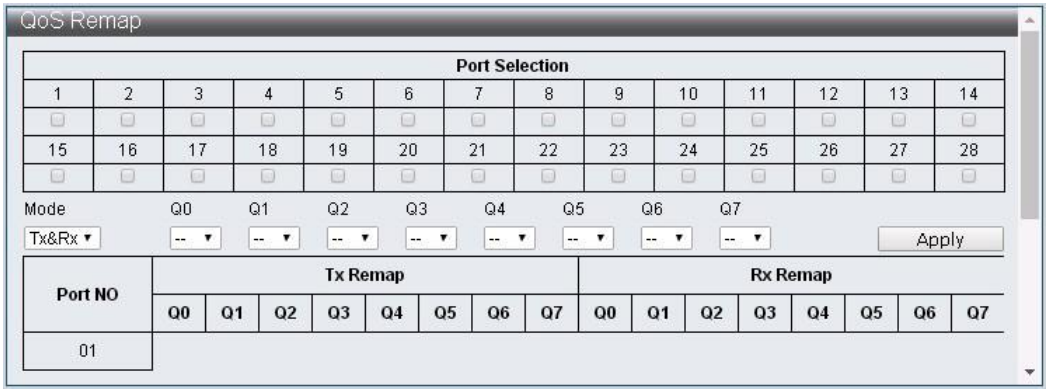


Parameter	Description
Out Queue Aging Time	Configure Queue Aging Time
Fast Aging Time Enable	Aging Time Unit Conversion,from 100ms to 1.638ms
Port Select	Select corresponding Ports
Q0 ~ Q7	Select the queue to enable Out Queue Aging Time

4.4 QoS Remap

QoS Remap Configuration

QoS Configuration -> QoS Remap

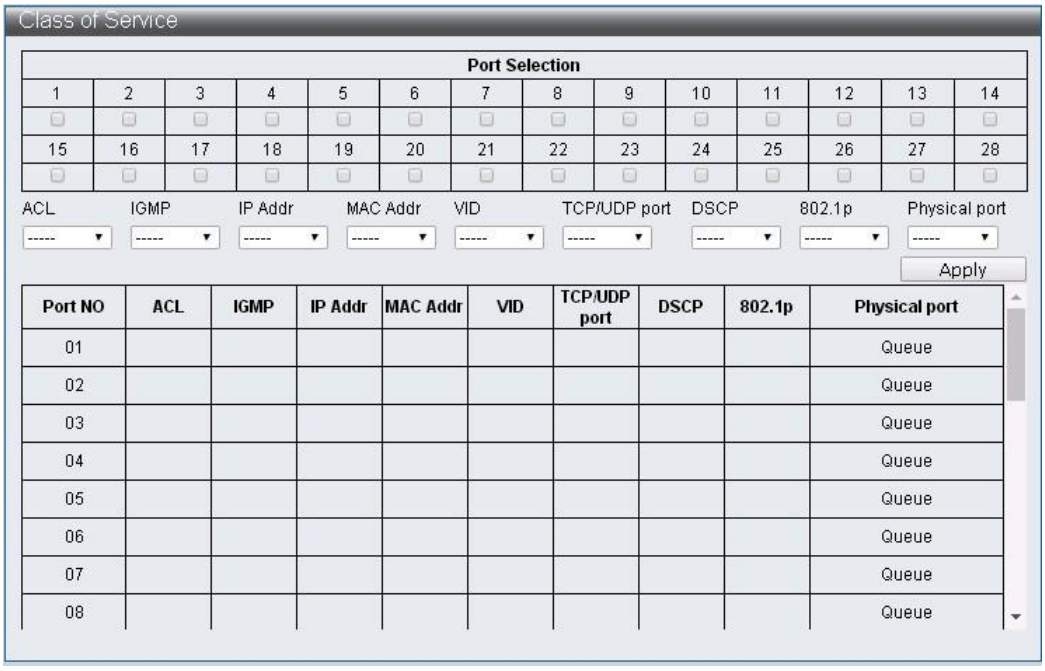


Parameter	Description
Port Selection	Select corresponding Ports
Mode	Mode select, Tx Rx or Tx&Rx
Q0 ~ Q7	Select the queue to remap Queue Number

4.5 Class of Service

Class of Service Configuration

QoS Configuration -> Class of Service



Class of Service Priority Level:

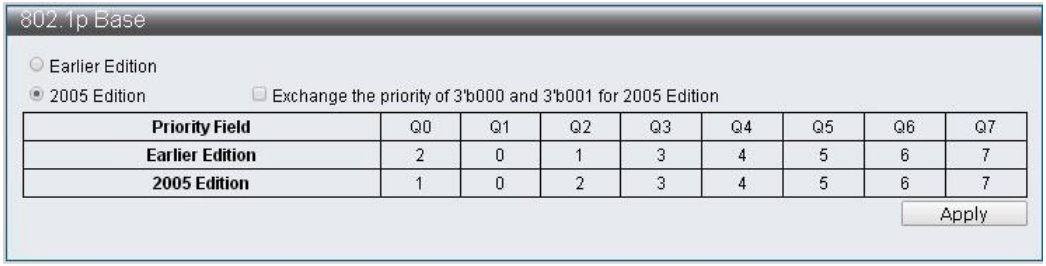
ACL > IGMP > IP Addr > MAC Addr > VID > TCP/UDP Port > DSCP > 802.1p > Physical Port

Parameter	Description
Port Selection	Select the ports which enable weights of specific packet.
ACL	Enable / Disable ACL
IGMP	Enable / Disable IGMP
IP Addr	Enable / Disable IP Adrr(Port-MAC-IP Entry)
MAC Addr	Enable / Disable MAC Addr (LUT Priority)
VID	Enable / Disable VLAN Tag
TCP/UDP Port	Enable / Disable TCP/UDP Port number
DSCP	Enable / Disable IPv4 TOS /IPv6 DSCP
802.1q	Enable / Disable 802.1p
Physical Port	Select weight of each Ports, Q0 ~ 7

4.6 802.1q Base

802.1q Base Configuration

QoS Configuration -> 802.1q Base

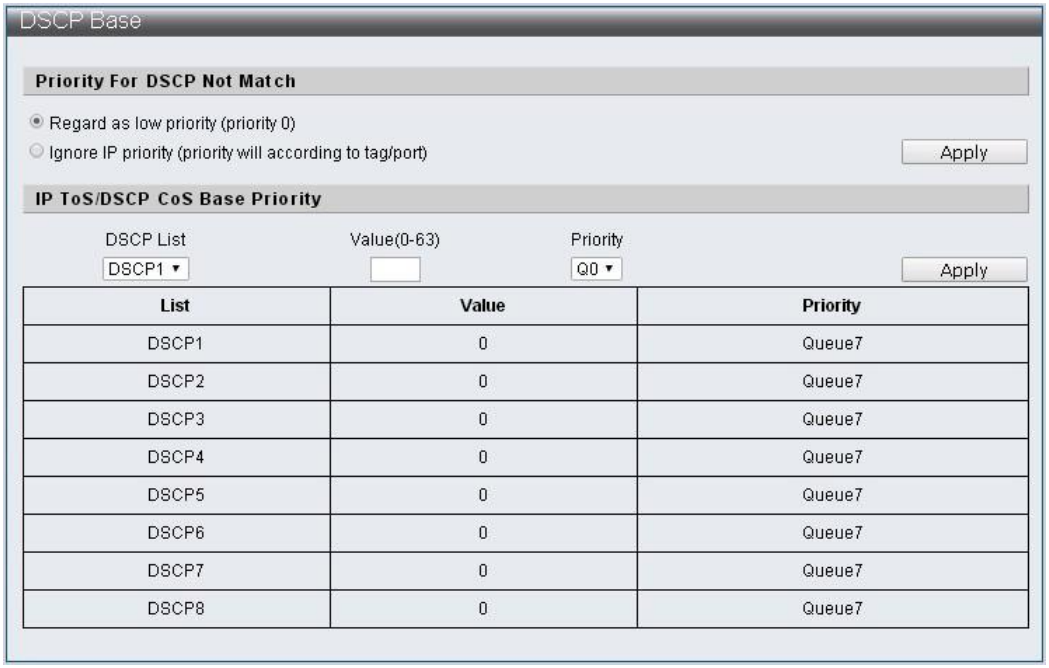


Parameter	Description
Earlier Edition	Select earlier version
2005 Edition	Select 2005 version
Exchange the priority	Exchange the weights

4.7 DSCP Base

DSCP Base Configuration

QoS Configuration -> DSCP Base

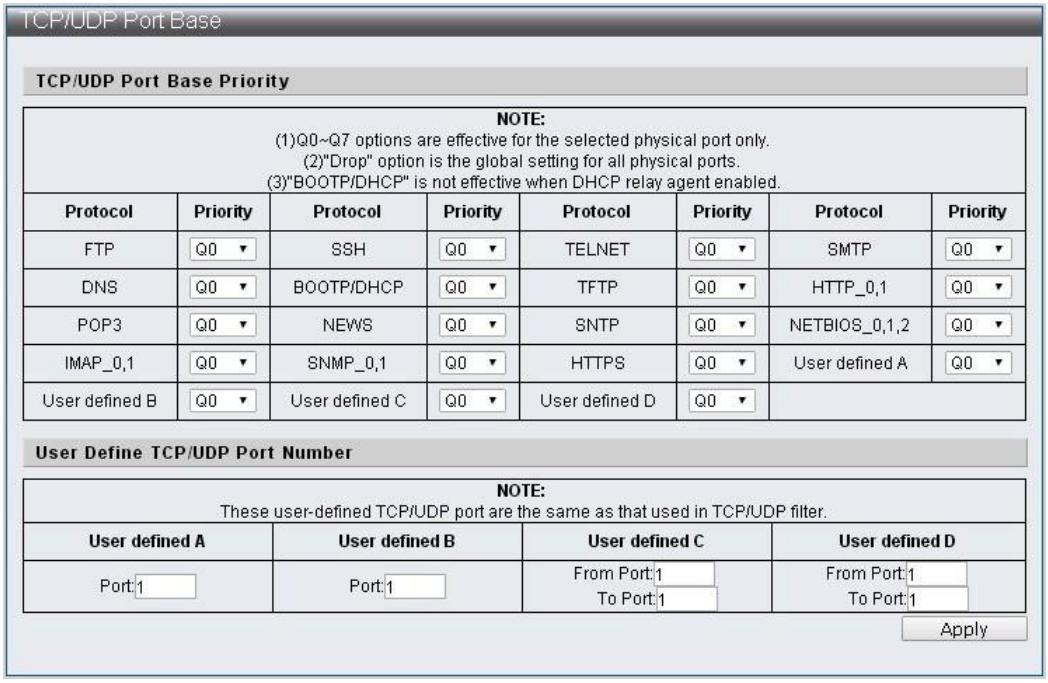


Parameter	Description
Priority For DSCP Not Match	Select the action when DSCP not match
DSCP List	Select DSCP List
Value	Configure DSCP
Priority	Configure the queue of DSCP.

4.8 TCP/UDP Port Base

TCP/UDP Port Base Configuration

QoS Configuration -> TCP/UDP Port Base



Parameter	Description
Protocol	TCP/UDP protocol
Priority	Select the queue of each TCP/UDP protocol
User defined A	Configure TCP/UDP Port number
User defined B	Configure TCP/UDP Port number
User defined C	Configure TCP/UDP Port Range
User defined D	Configure TCP/UDP Port Range

5 ACL Configuration

OS1326/OS1326P has 128 ACL Entry, which allows users to configure base of preference.

ACL Profile *List*

ACL Ctag *Settings*

ACL Stag *Settings*

ACL VLAN *Settings*

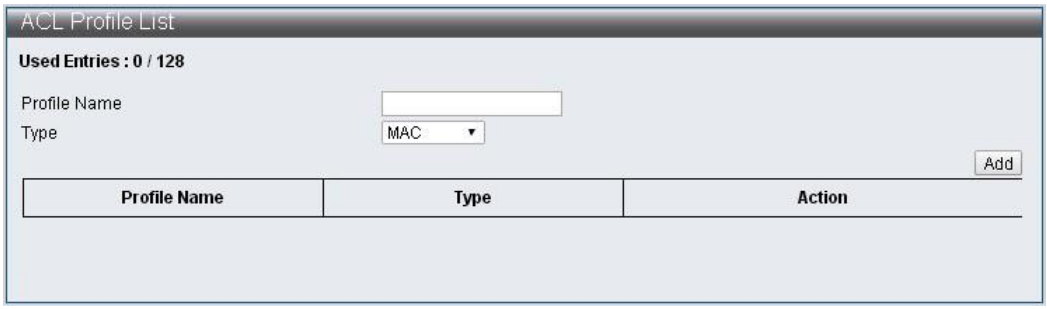
ACL Bandwidth *Settings*

ACL DSCP Settings

5.1 ACL Profile List

ACL Profile List Configuration

ACL Configuration -> ACL Profile List

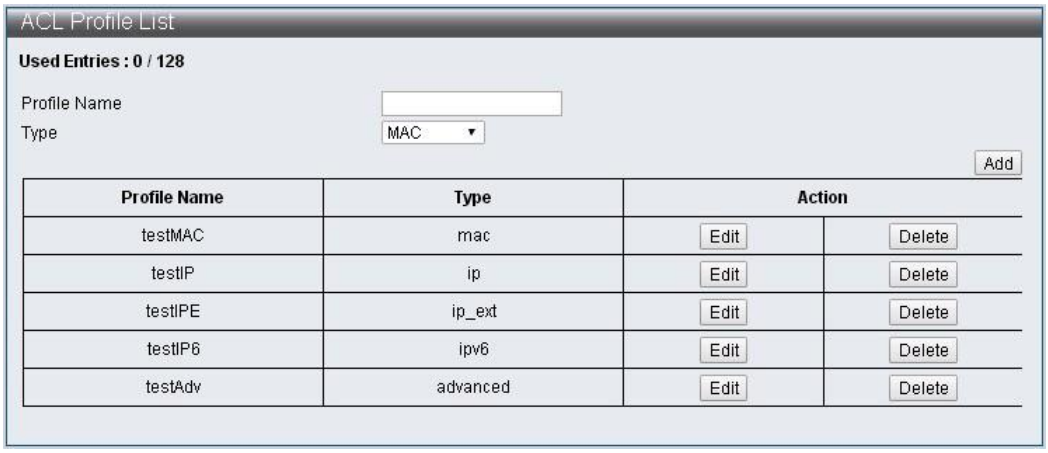


Parameter	Default	Description
Used Entries	0/128	Display used entry number. Please note the rule or setting may used more than one entry.
Profile Name		Profile name
Type		Type: MAC, IP, IP_Ext, IPv6, Advanced

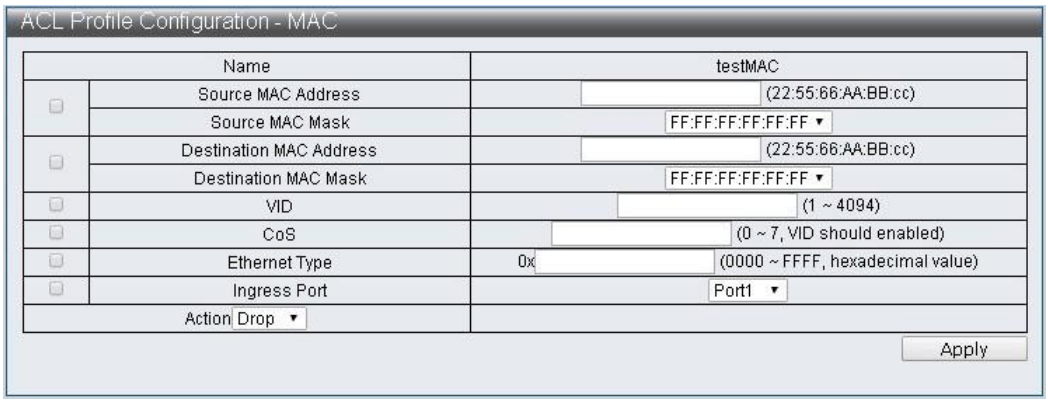
Please follow procedure below to set rule.

Step1: Input Profile Name, select Type, click “Add”

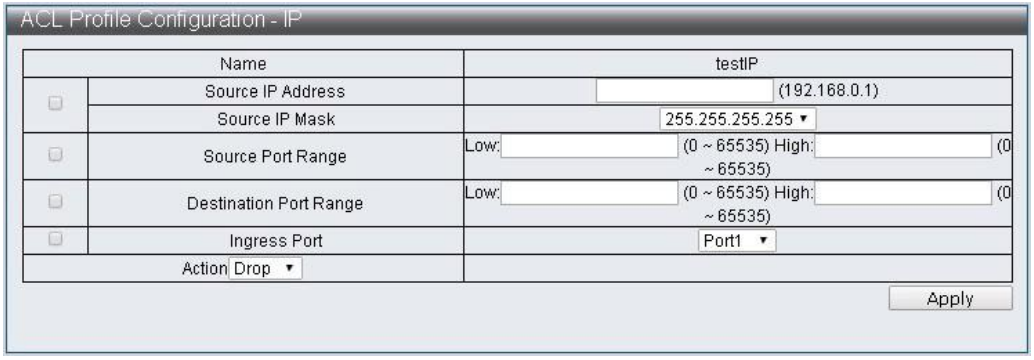
Step2: Click “edit” which user wants to modify.



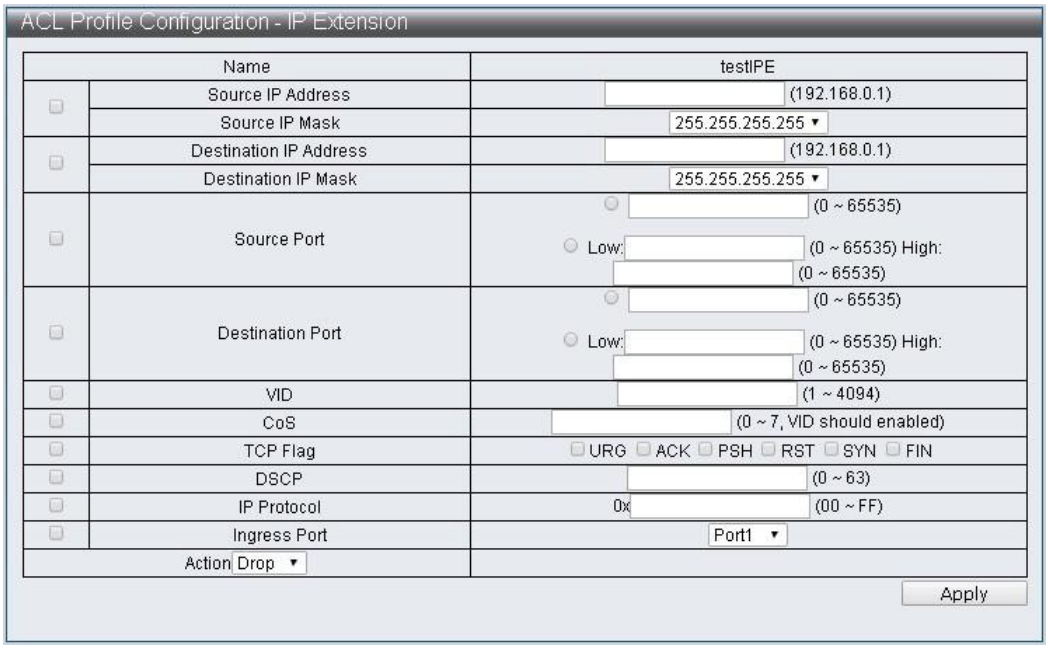
ACL Profile Configuration - MAC



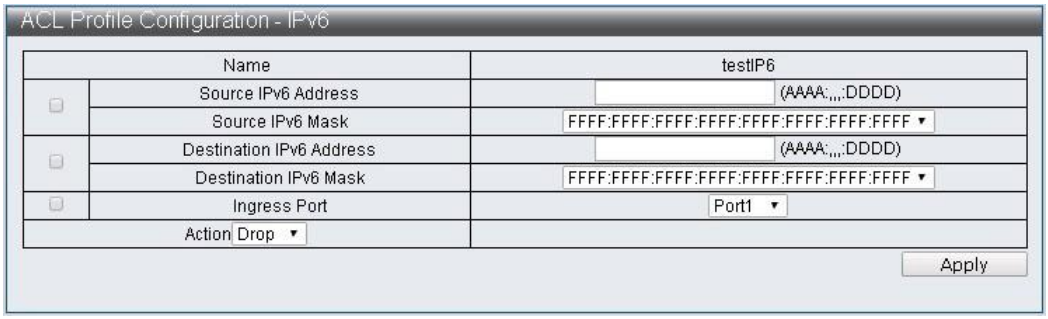
ACL Profile Configuration - IP



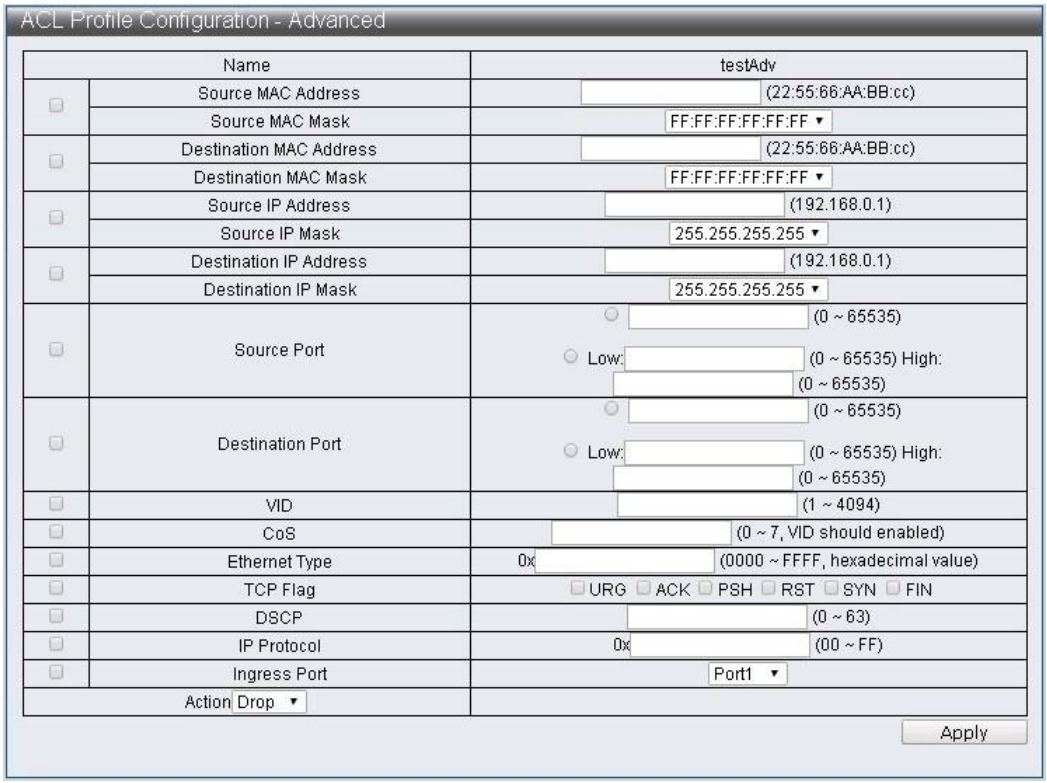
ACL Profile Configuration - IP Extension



ACL Profile Configuration - IPv6



ACL Profile Configuration - Advanced

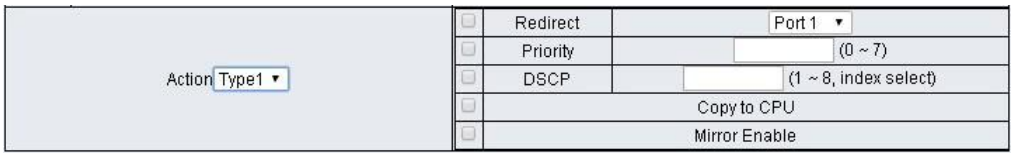


Parameter	Descprition
Source MAC Address	Input Source MAC Address
Source MAC Mask	Select Source MAC Mask,Select FF:FF:FF:FF:FF:FF、FF:FF:FF:00:00:00 and FF:FF:00:00:00:00
Destination MAC Address	Input Destination MAC Address
Destination MAC Mask	Select Destination MAC Mask , Select FF:FF:FF:FF:FF:FF 、 FF:FF:FF:00:00:00and FF:FF:00:00:00:00
Source IP Address	Select Source IP Address
Source IP Mask	Select Source IP Mask, Select 255.255.255.255 、 255.255.255.240 、 255.255.255.0 、 255.255.240.0 、 255.255.0.0、255.0.0.0 and 240.0.0.0
Destination IP Adress	Input Destination IP Address
Destination IP Mask	Select Destination IP Mask,Select 255.255.255.255 、 255.255.255.240 、 255.255.255.0 、 255.255.240.0 、 255.255.0.0、255.0.0.0 and 240.0.0.0
Source Port	Input Source Port, can be specific number or a range
Destination Port	Input Destination Port, can be specific number or a range

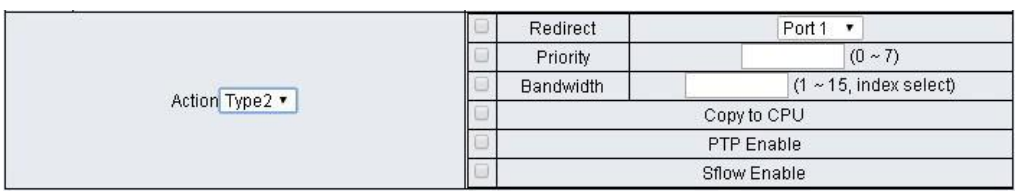
VID	Input VID, from 1~4094
CoS	Configure CoS, must be set with VID to take effect Range: 0~7
Ethernet Type	Input Ethernet Type, Parameter limited to 0000~FFFF
TCP Flag	Select TCP Flag
DSCP	Input DSCP, Parameter limited to 0~63
IP Protocol	Input IP Protocol, Parameter limited to 00~FF
Source IPv6 Address	Input Source IPv6 Address
Source IPv6 Mask	Select Source IPv6 Mask FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 、FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:0000:0000 、 FFFF:FFFF:FFFF:0000:0000:0000:0000:0000 and FFFF:0000:0000:0000:0000:0000:0000:0000
Destination IPv6 Adress	Input Destination IPv6 Address
Destination IPv6 Mask	Select Destination IPv6 Mask FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF 、 FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:0000:0000 、 FFFF:FFFF:FFFF:0000:0000:0000:0000:0000 and FFFF:0000:0000:0000:0000:0000:0000:0000
Ingress Port	Select source Port

Action Drop

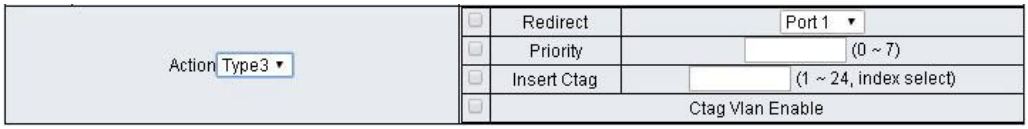
Action Type1



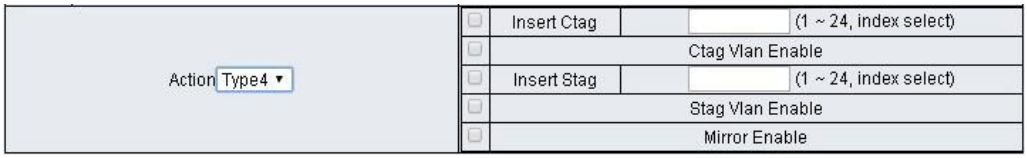
Action Type2



Action Type3



Action Type4

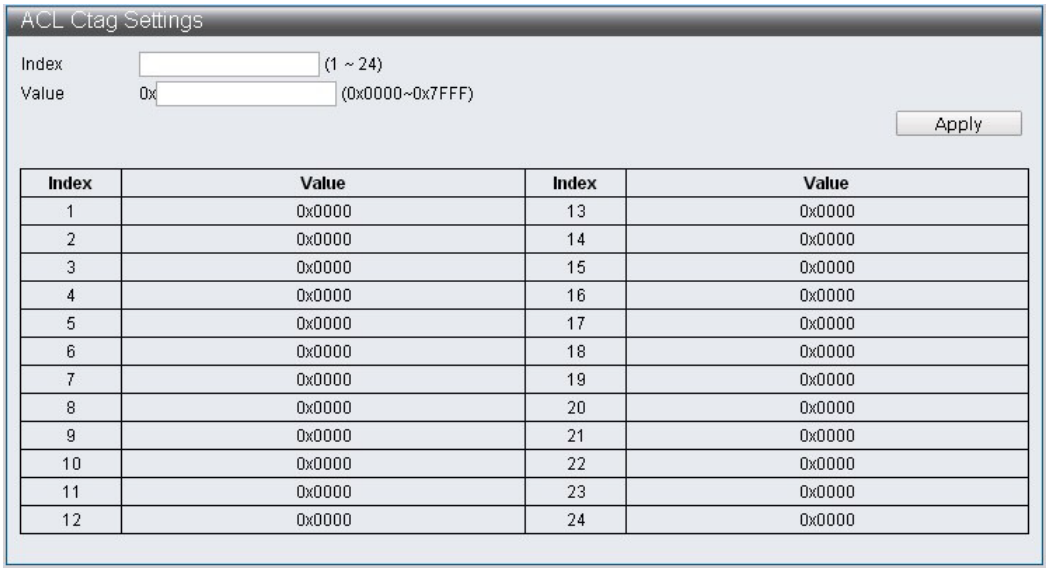


Parameter	Description
Redirect	Configure redirecting to another Port
Priority	Configure Priority, Parameter limited to 0~7
DSCP	Configure DSCP Index, Transmit DSCP value base on ACL DSCP Settings Configuration.
Bandwidth	Configure Bandwidth Index, Limit packet bandwidth base on the configuration of ACL Bandwidth Settings.
Copy to CPU	Copy to CPU
PTP Enable	Enable PTP function
Mirror Enable	Enable Mirror Feature, Transmit packet to Destination Port base on the Basic Configuration -> Port Mirror Function Configuration.
Sflow Enable	Enable Sflow function.
Insert Ctag	Configure Insert Ctag Index, base on ACL Ctag Settings to insert Ctag
Ctag Vlan Enable	Enable Insert Ctag Index to select ACL VLAN Settings to forward packet.
Insert Stag	Configure Insert Stag Index,base on ACL Stag Settings to insert Ctag
Stag Vlan Enable	Enable Insert Stag Index to select ACL VLAN Settings to forward packet.

5.2 ACL Ctag Settings

ACL Ctag Settings Configuration

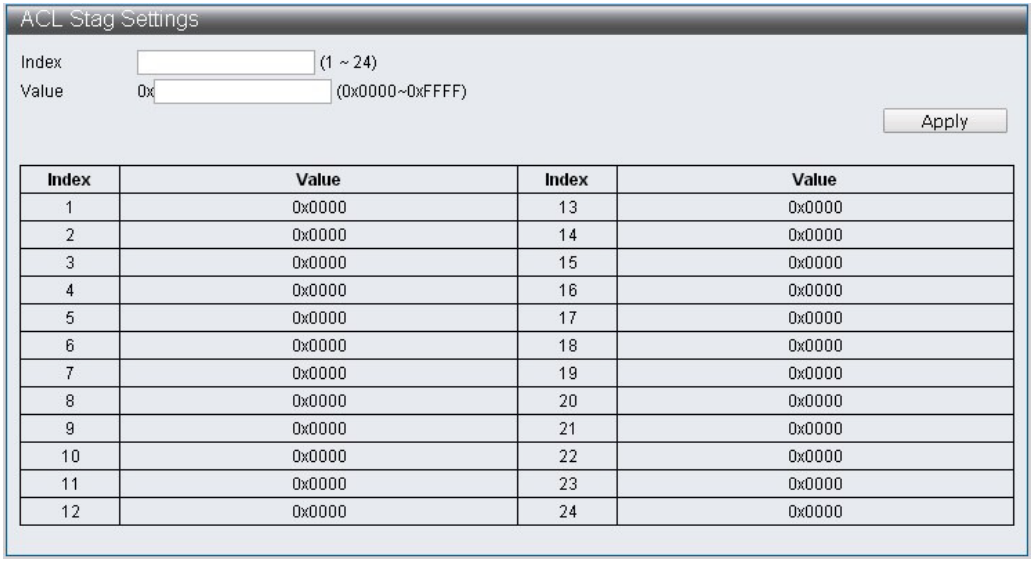
ACL Configuration -> ACL Ctag Settings



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

ACL Stag Settings

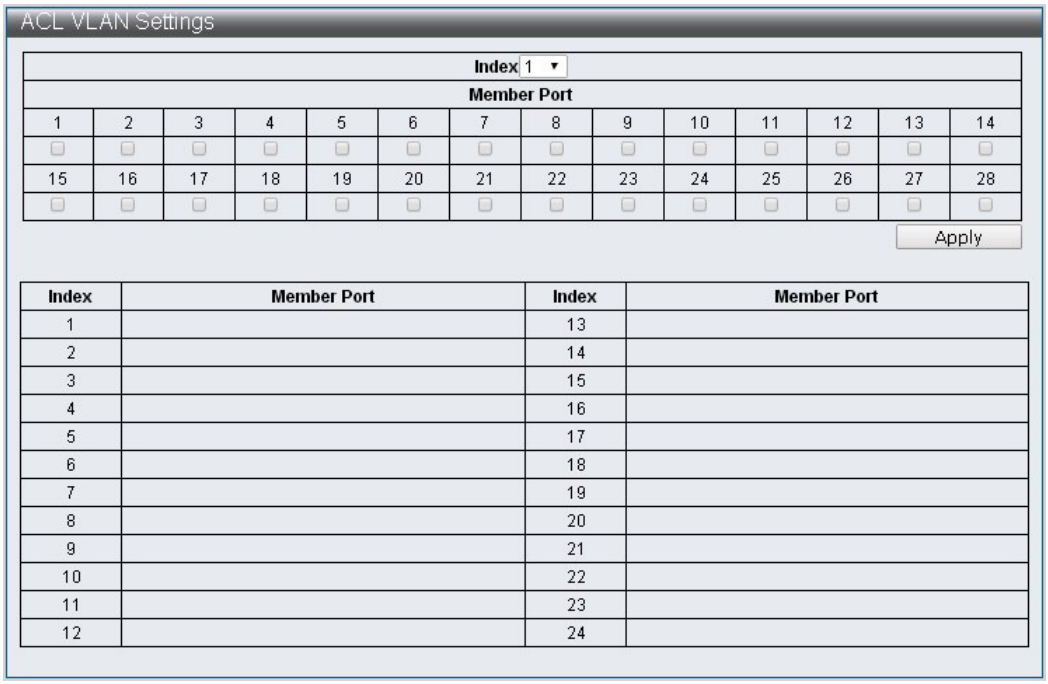
ACL Configuration -> ACL Stag Settings



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

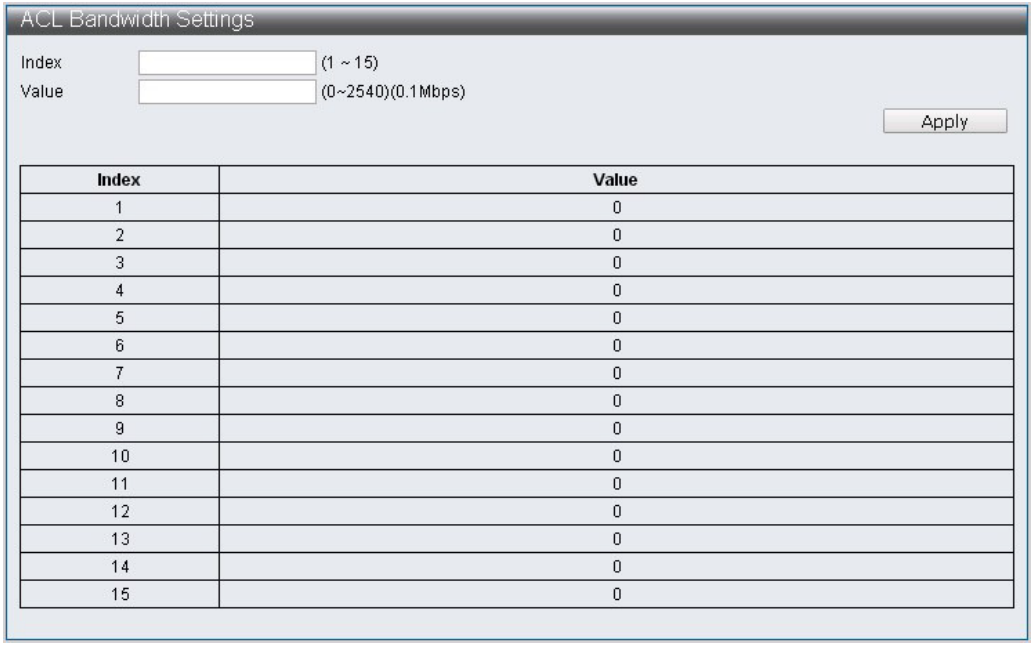
ACL VLAN Settings

ACL Configuration -> ACL VLAN Settings



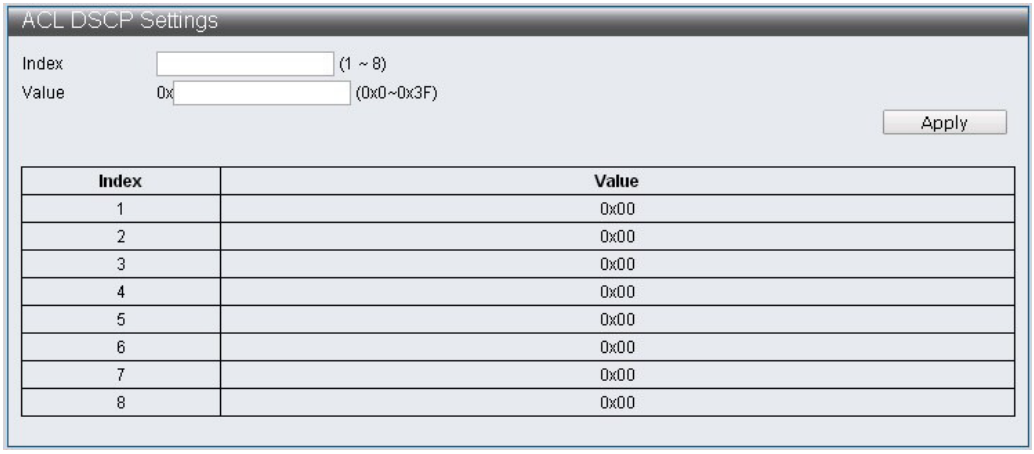
ACL Bandwidth Settings

ACL Configuration -> ACL Bandwidth Settings



ACL DSCP Settings

ACL Configuration -> ACL DSCP Settings



6 Security

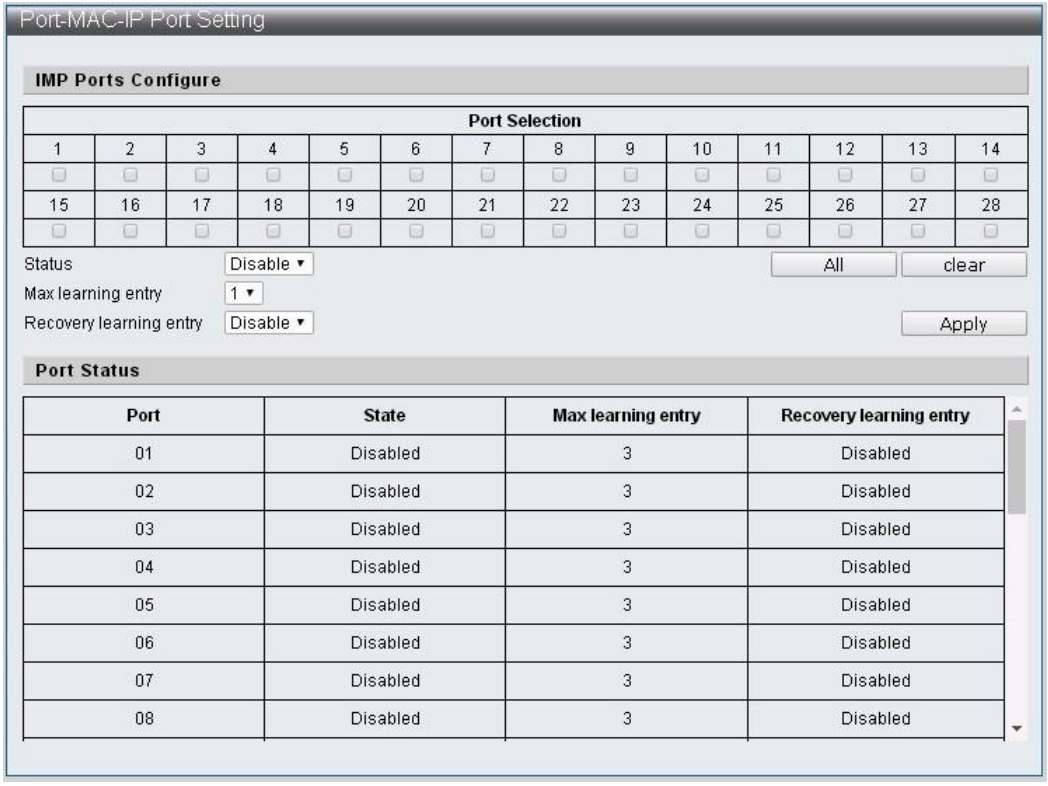
6.1 Port-MAC-IP Binding

Support IPv4/IPv6, through source IP/MAC check to improve security and filtering.

6.1.1 Port-MAC-IP Port Setting

Port-MAC-IP Port Setting Configuration

Security -> Port-MAC-IP Binding -> Port-MAC-IP Port Setting

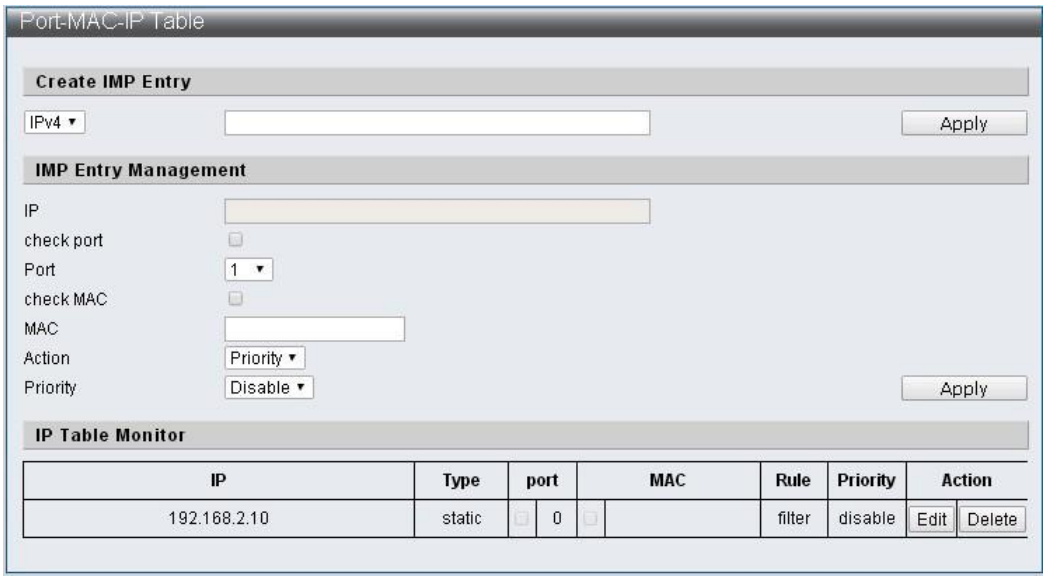


Parameter	Description
Port Selection	Select corresponding Ports
All	Select all Ports
Clear	Delete all selected Ports
Status	Enable / Disable Port-MAC-IP Binding Feature
Max learning entry	Configure each Port's maximum learning entry
Recover learning entry	When learning entry reach max. number, automatically recover first entry.

6.1.2 Port-MAC-IP Entry Setting

Port-MAC-IP Entry Setting Configuration

Security -> Port-MAC-IP Binding -> Port-MAC-IP Entry Setting

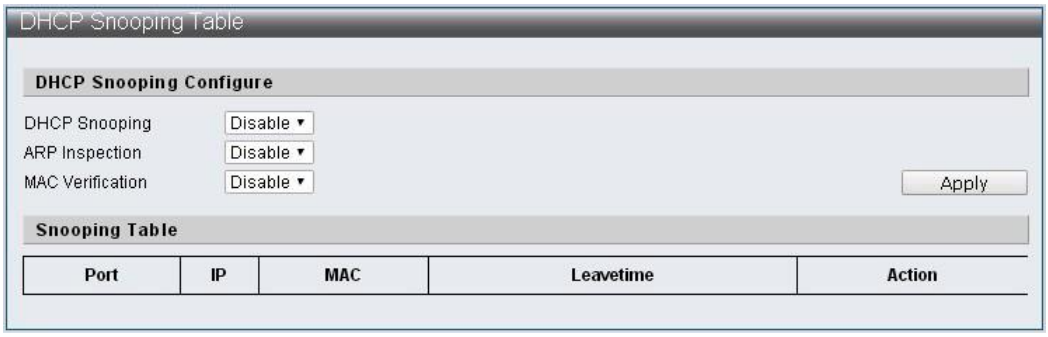


Parameter	Description
IPv4/IPv6	Select IPv4 or IPv6 and in put IP Address
IMP Entry Management	Click “edit” icon to modify IMP entry in IP Table Monitor
IP	IMP Entry IP Address
Check port	Enable/Disable source port checking
Port	Configure IP Address corresponding Port
Check MAC	Enable/Disable source MAC checking.
MAC	Configure source MAC of IP Address.
Action	Configure action when matching, Filter/Priority
Priority	Configure IMP Entry Queue when selected action is priority

6.1.3 DHCP Snooping Entry Setting

DHCP Snooping Entry Setting Configuration

Security -> Port-MAC-IP Binding -> DHCP Snooping Entry Setting



Parameter	Description
DHCP Snooping	Enable / Disable DHCP Snooping Feature
ARP Inspection	Enable / Disable ARP Inspection Feature
MAC Verification	Enable / Disable MAC Verification Feature

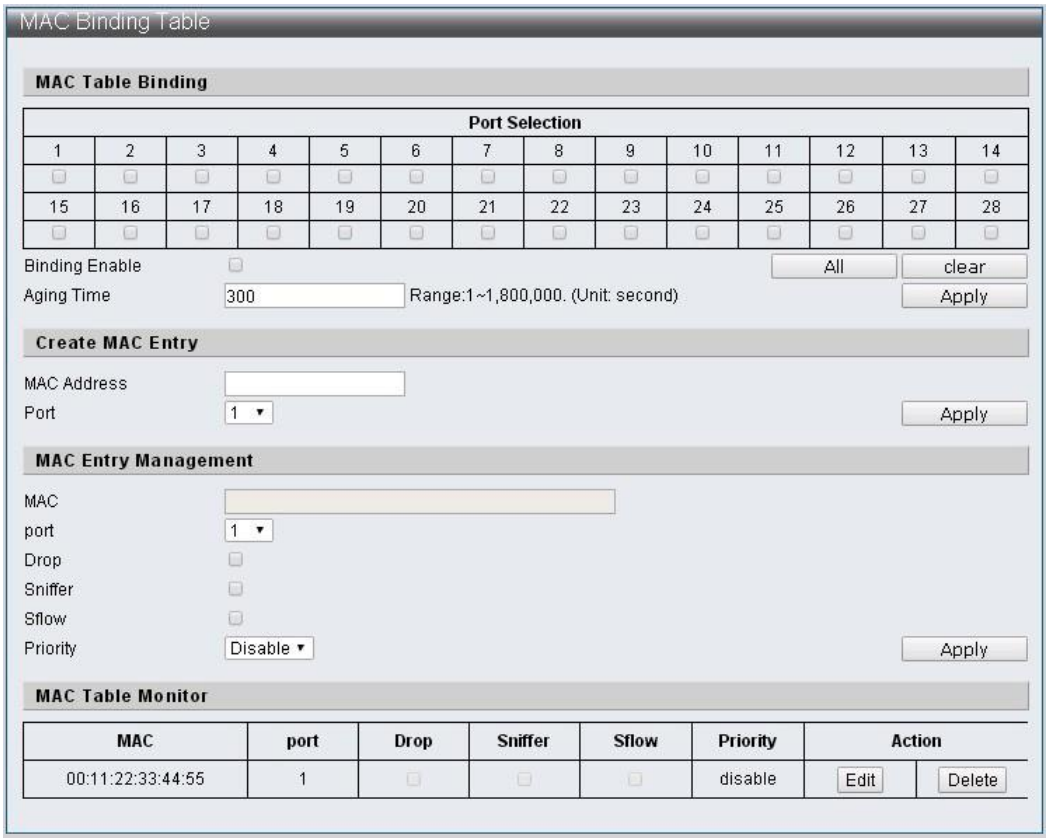
6.2 MAC Address Binding

This feature allows to drop, Mirror and forward packets to CPU port when source MAC is not match MAC binding list.

Please note MAC address learning disable is requested to stop unknown MAC(the MAC not exist in MAC table) or this function just can stop the packet with the MAC which learned in MAC table.

MAC Address Binding Configuration

Security -> MAC Address Binding



Parameter	Description
Port Selection	Select corresponding port and disable address learning
Binding Enable	Enable / Disable MAC Binding Feature
Aging Time	Configure MAC Binding Aging Time from 1~1800000sec
MAC Address	Create Binding MAC Address
Port	Select MAC Address Binding Port
MAC Entry Management	Click “edit” icon in MAC table to modify or delete setting.
MAC	Display MAC Address Information
Port	Configure Binding MAC Address Port
Drop	When source MAC of received packet match Mac entry. The packet will be dropped.
Sniffer1	When source MAC of received packet match Mac entry. The packet will be forwarded to Destination Port which defined in Port Mirror.
Sflow	When source MAC of received packet match Mac entry. The packet will be forwarded to CPU Port.

Priority	When source MAC of received packet match Mac entry. The packet will be assign to corresponding queue.

7 Advanced Features

7.1 Spanning Tree Protocol

STP

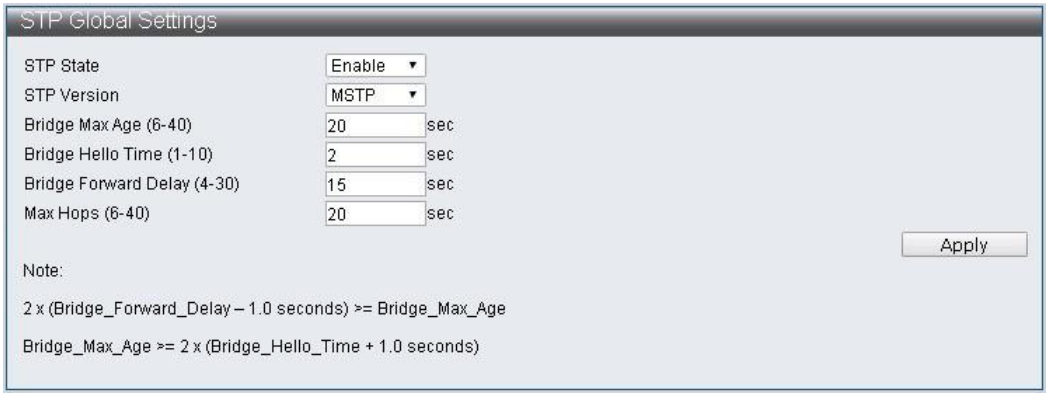
STP (Spanning Tree Protocol) is a layer 2 protocol base on OSI model, this feature ensure loop free Ethernet Network to avoid broadcast storm, prevent repeated packet and MAC address table trashing. Spanning tree also allows a network design to include backup links to provide fault tolerance if an active link fails.

BPDU

BPDU (Bridge Protocol Data Unit) is a special packet which used to exchange information about bridge IDs and root path costs between each bridge.

7.1.1 STP Global Settings Configuration

Advanced Features -> Spanning Tree Protocol -> STP Global Settings

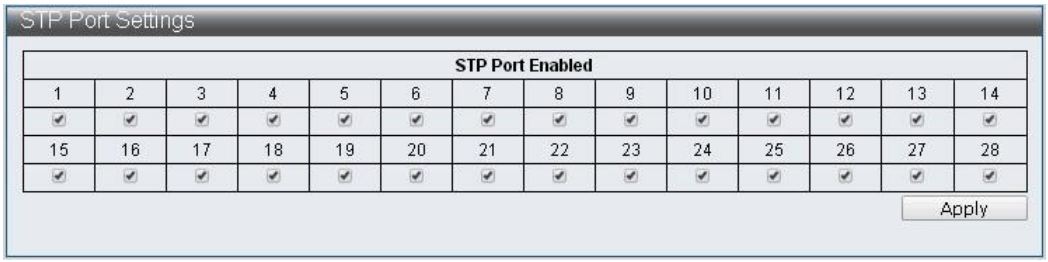


Parameter	Default	Description
STP State	Enable	Enable / Disable STP Feature
STP Version	MSTP	Configure STP version, support STP、RSTP、MSTP
Bridge Max Age (6-40)	20	Configure the max bridge age when this switch is defined as root bridge. When any of Bridge Port in this tree (except Designated Port) did not receive BPDU within this period, that Bridge Port will start to send BPDU to re-create spanning tree
Bridge Hello Time (1-10)	2	Configure the BPDU sending time interval when this switch is defined as root bridge.
Bridge Forward Delay (4-30)	15	Configure time interval which switch port state turns to Forwarding when this switch is defined as root bridge.
Max Hops (6-40)	20	When operating in MSTP mode, configure the Max hops when this switch is defined as root bridge. This setting defining the Max. node of BPDU, when switch receive BPDU, it will minus 1 of Remaining Hops, the it becomes 0, will not send BPDU.

7.1.2 STP Port Settings

STP Port Settings Configuration

Advanced Features -> Spanning Tree Protocol -> STP Port Settings

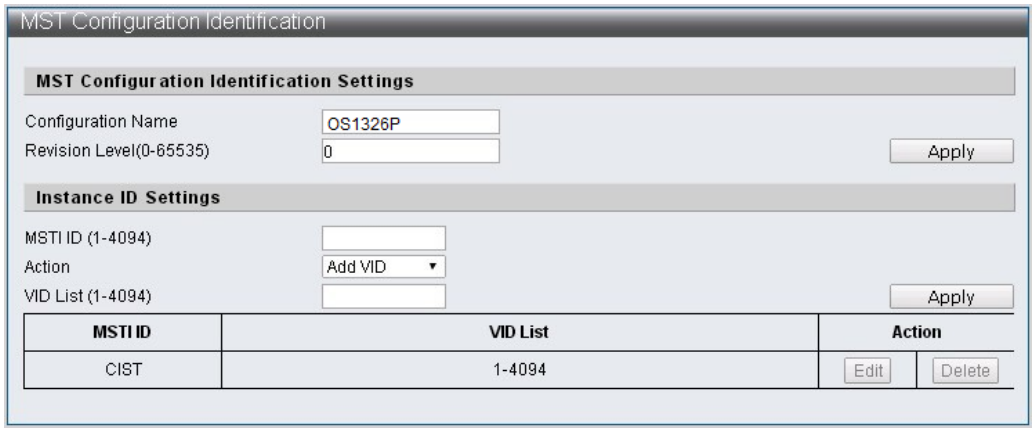


Parameter	Default	Description
STP Port Enabled	Enabled	Enable STP of corresponding Port

7.1.3 MST Configuration Identification

MST Configuration Identification Configuration

Advanced Features -> Spanning Tree Protocol -> MST Configuration Identification



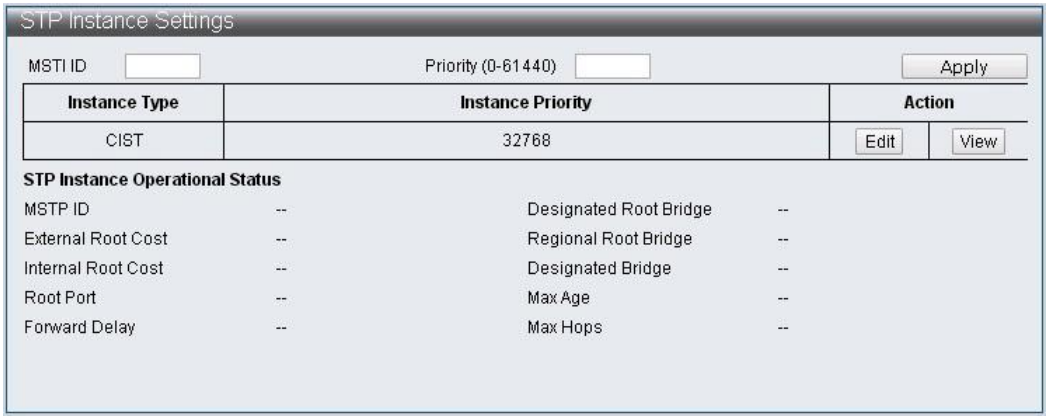
Parameter	Default	Description
Configuration Name	OS1326P	Configure name, it’ s MSTI (Multiple Spanning Tree Instance) only ID.
Revision Level(0-65535)	0	Configure revision level to identify if in the same MSTP region
MSTI ID (1-4094)		Configure MSTI entry ID
Action	Add VID	MSTI VID List method Add VID: add VID List to MSTI Remove VID: remove VID List from MSTI.

VID List (1-4094)		Edit MSTI VID List

7.1.4 STP Instance Settings

STP Instance Settings Configuration

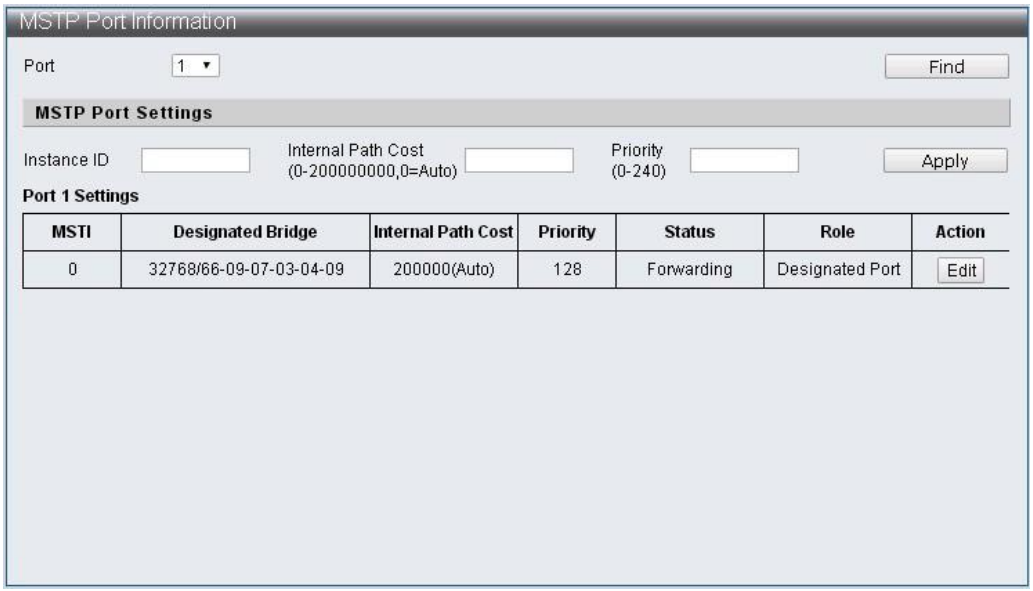
Advanced Features -> Spanning Tree Protocol -> STP Instance Settings



7.1.5 MSTP Port Information

MSTP Port Information Configuration

Advanced Features -> Spanning Tree Protocol -> MSTP Port Information



Parameter	Default	Description
Port	1	Configure displayed Port no.
Instance ID		Configure MSTI entry ID no.
Internal Path Cost (0-200000000,0=Auto)		Configure MSTI internal cost of the Port. When Region is a independent network, this cost means root cost of this bridge.
Priority (0-240)		Configure MSTI priority of the Port.

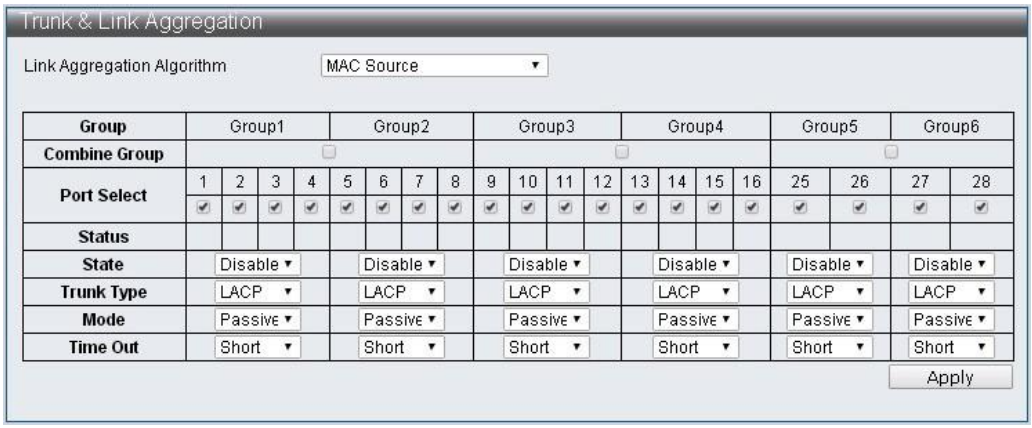
7.2 Trunk & Link Aggregation

Trunk Group combine several specific ports and use load balance design to achieve higher bandwidth and performance. OS1326/OS1326P supports four FE groups and two Gigabit Ethernet groups,

Each FE trunk group included max. four members, Gigabit group included 2 members.
Also can combine two FE group to one trunk group or four gigabit port as one group.

Trunk & Link Aggregation Configuration

Advanced Features -> Trunk & Link Aggregation



Parameter	Default	Description
Link Aggregation Algorithm	MAC Source	Link Aggregation Algorithm, support Port、MAC Source 、 MAC Destination 、 IP Source 、 IP Destination 、 TCP/UDP Destination Port 、 TCP/UDP Source Port
Group		Group index
Combine Group		Combine two Groups as one
Port Select		Select group member
Status		Display member statud, ”A” means setting accomplished.
State	Disable	Enable / Disable Status
Trunk Type	LACP	Select Trunk type, LACP or Static
Mode	Passive	Mode selection, Passive or Active
Time Out	Short	Time Outselection, support Short and Long, Short means one packet per second, Time Outis 3 sec., Long means one packet per 30 sec. and Time Out is 90 sec.

7.3 IGMP Snooping

Internet Group Management Protocol (IGMP) Snooping

IGMP Snooping Settings

IGMP Snooping Router Ports Settings

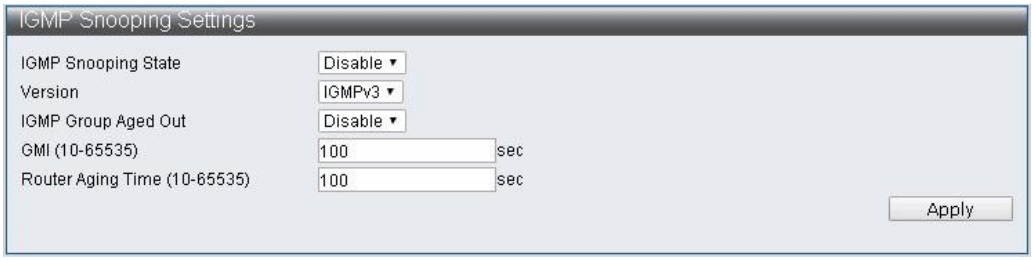
IGMP Snooping Groups

IGMP Snooping Ports

7.3.1 IGMP Snooping Settings

IGMP Snooping Settings Configuration

Advanced Features -> IGMP Snooping -> IGMP Snooping Settings

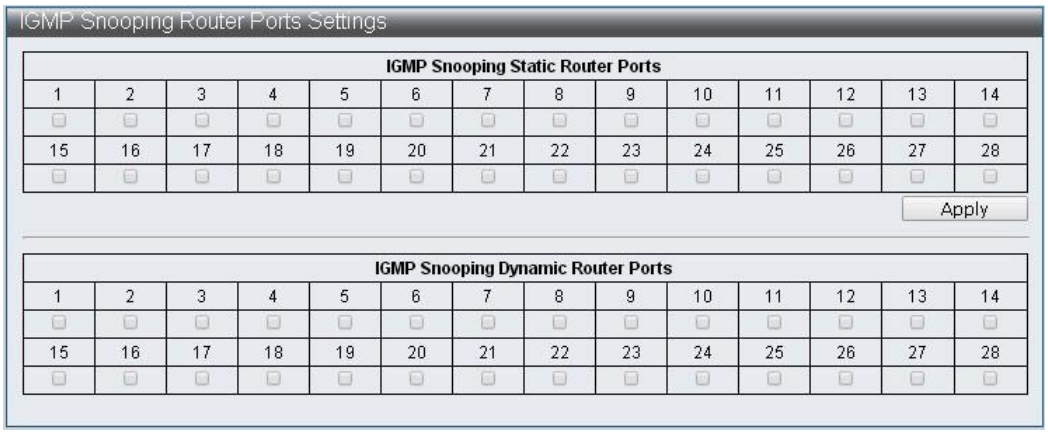


Parameter	Default	Description
IGMP Snooping State	Disable	IGMP Snooping Enable / Disable
Version	IGMPv3	Select version from IGMPv1、IGMPv2、IGMPv3
IGMP Group Aged Out	Disable	Enable/Disable dynamic group age out follow GMI Configuration.
GMI	100(sec)	Group Member Interval, dynamic Group will base on this setting to query if member still exist.
Router Aging Time	100(sec)	Dynamic Router Port aging time, if no Query received continuously, dynamic Router Port will be removed.

7.3.2 IGMP Snooping Router Ports Settings

IGMP Snooping Router Ports Settings Configuration

Advanced Features -> IGMP Snooping -> IGMP Snooping Router Ports Settings

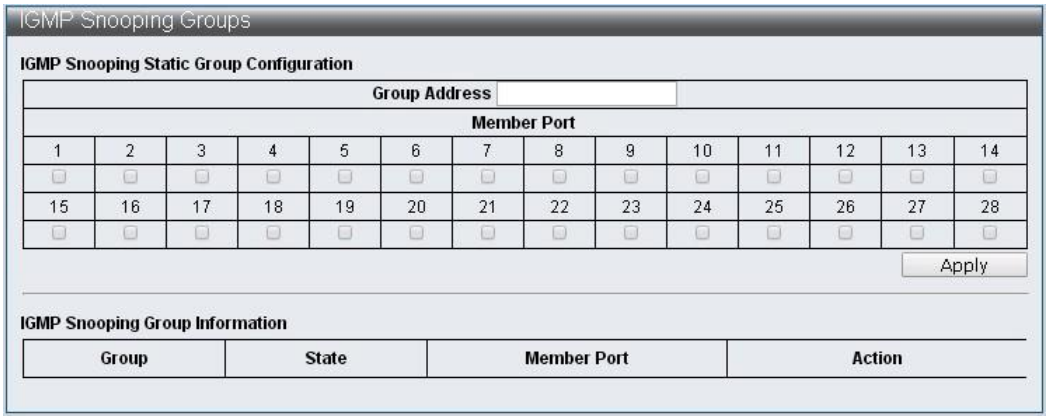


Parameter	Description
IGMP Snooping Static Router Ports	Configure static Router Ports
IGMP Snooping Dynamic Router Ports	Display static Router Ports

7.3.3 IGMP Snooping Groups

IGMP Snooping Groups Configuration

Advanced Features -> IGMP Snooping -> IGMP Snooping Groups

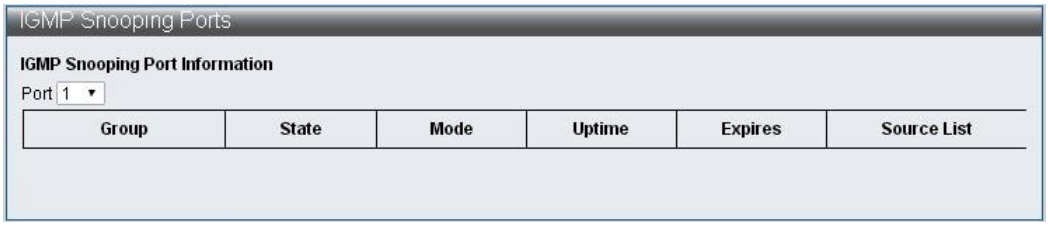


Parameter	Description
IGMP Snooping Static Group Configuration	Configure static group and members.
IGMP Snooping Group Information	Display current Group status

7.3.4 IGMP Snooping Ports

IGMP Snooping Ports Configuration

Advanced Features -> IGMP Snooping -> IGMP Snooping Ports



Parameter	Description
IGMP Snooping Port Information	Display Group information of selected port.

7.4 MLD Snooping

MLD Snooping

Multicast Listener Discovery (MLD) Snooping

MLD Snooping Settings

MLD Snooping Router Ports Settings

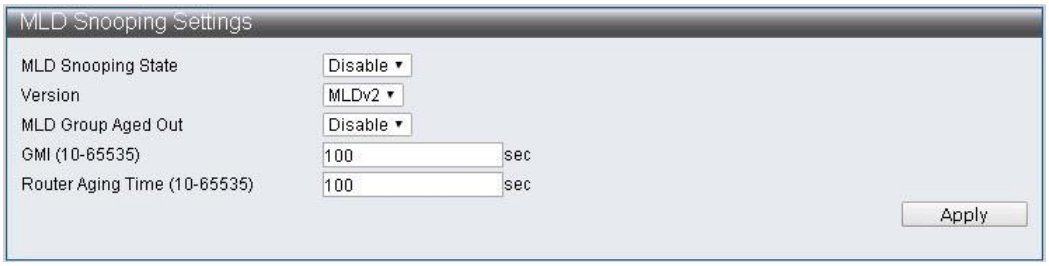
MLD Snooping Groups

MLD Snooping Ports

7.4.1 MLD Snooping Settings

MLD Snooping Settings Configuration

Advanced Features -> MLD Snooping -> MLD Snooping Settings

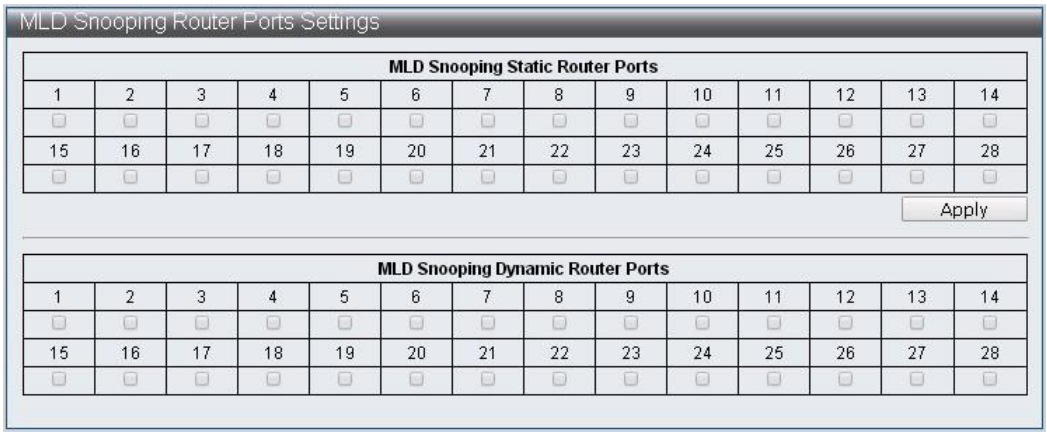


Parameter	Default	Description
MLD Snooping State	Disable	Enable / Disable MLD Snooping
Version	IGMPv3	Version selection, choose between MLDv1 & MLDv2
MLD Group Aged Out	Disable	Enable/Disable dynamic group age out follow GMI Configuration.
GMI	100(sec)	Group Member Interval, dynamic Group will base on this setting to query if member still exist
Router Aging Time	100(sec)	Dynamic Router Port aging time, if no Query received continuously, dynamic Router Port will be removed.

7.4.2 MLD Snooping Router Ports Settings

MLD Snooping Router Ports Settings Configuration

Advanced Features -> MLD Snooping -> MLD Snooping Router Ports Settings

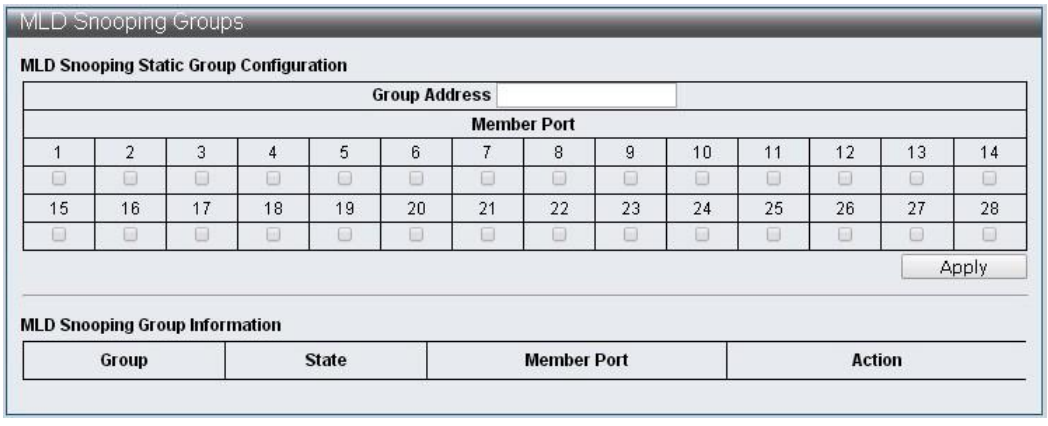


Parameter	Description
MLD Snooping Static Router Ports	Configure static Router Ports
MLD Snooping Dynamic Router Ports	Display learned dynamic Router Ports

7.4.3 MLD Snooping Groups

MLD Snooping Groups Configuration

Advanced Features -> MLD Snooping -> MLD Snooping Groups

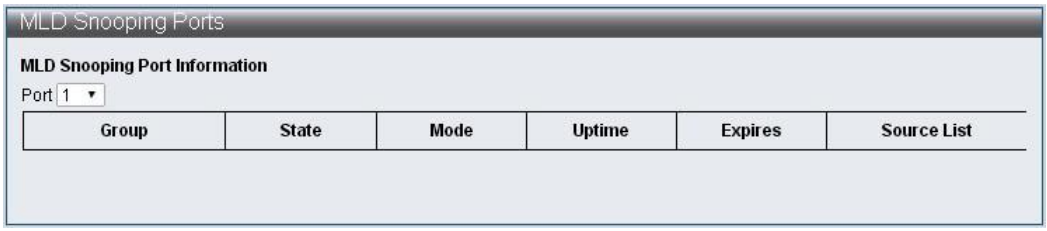


Parameter	Description
MLD Snooping Static Group Configuration	Configure static Group and members
MLD Snooping Group Information	Display current Group status

7.4.4 MLD Snooping Ports

MLD Snooping Ports Configuration

Advanced Features -> MLD Snooping -> MLD Snooping Ports

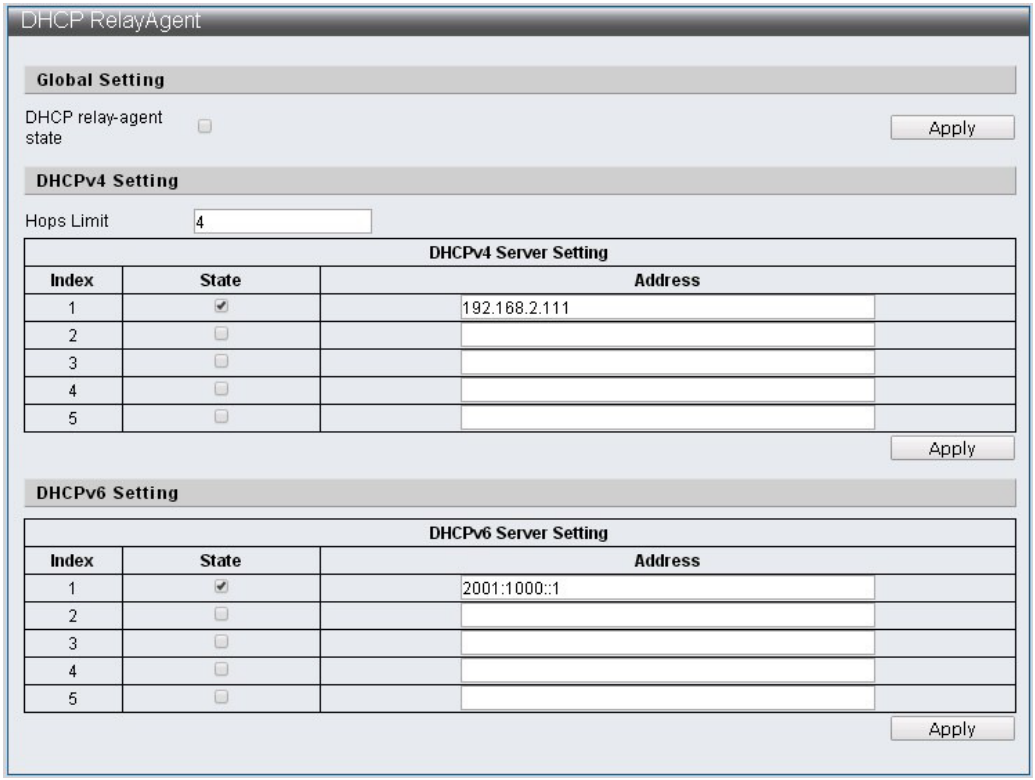


Parameter	Description
MLD Snooping Port Information	Display Group information of selected port.

7.5 DHCP Relay Agent

DHCP Relay Agent Configuration

Advanced Features -> DHCP Relay Agent



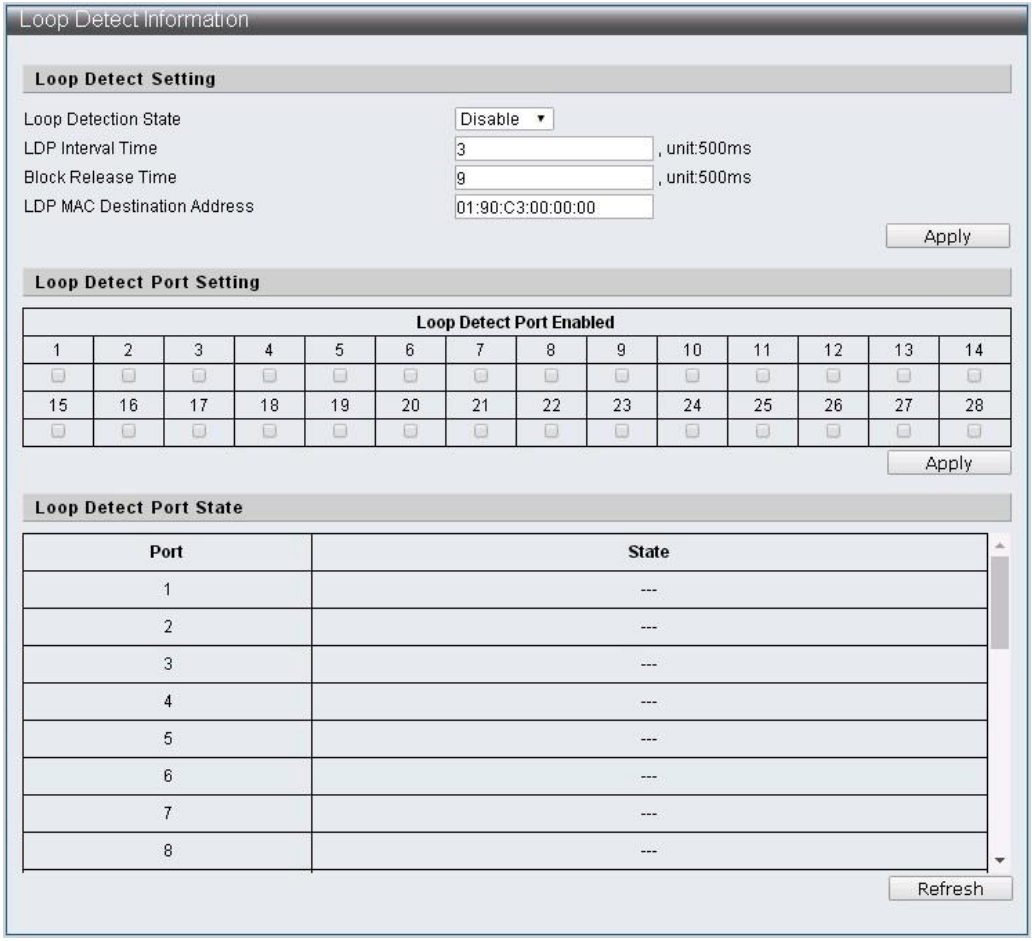
Parameter	Default	Description
DHCP relay-agent state		Enable/Disable DHCP Relay-Agent
Hops Limit	4	Hops limit of DHCP packet forwarding.
DHCPv4 Server Setting		DHCPv4 Server, configure up to 5 sets
DHCPv6 Server Setting		DHCPv6 Server, configure up to 5 sets

7.6 Loop Detect

Loop Detect is the ability to detect when a loop occurs within a switch. When loop detection is activated, the port that is causing loop will be blocked in order to prevent from crashing the network.

Loop Detection Configuration

Advanced Features -> Loop Detect



Parameter	Description
Loop Detect State	Enable / Disable Loop Detect
LDP Interval Time	Configure LDP time interval
Block Release Time	Configure release time for blocked Port
LDP MAC Destination Address	Configure DA of LDP
Loop Detect Port Enabled	Enable Loop Detect on corresponding Port
Refresh	Refresh Loop Detect Status

7.7 GVRP

GVRP (Generic VLAN Registration Protocol) is a protocol that facilitates control of VLANs, through several messages (Join, Leave and LeaveAll) exchanging, this allows network devices to dynamically exchange VLAN configuration information with other devices.

Join：When device received the Join message from other device or VLAN established in the device, it will send out Join message, Join message including JoinEmpty and JoinIn。

Leave：When device received the Join message from other device or VLAN removed from the device. It will send out Leave message, it including LeaveEmpty and LeaveIn。

LeaveAll：When Port enable GVRP function, it will activate LeaveAll timer in the mean time,once time Out occurred, it will send out LeaveAll message.

GVRP timer including Join timer, Leave timer and LeaveAll timer.

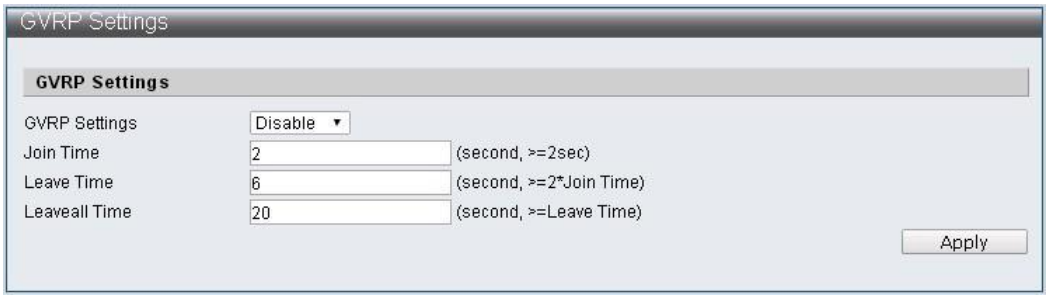
Join timer：Using to control transmission of Join message to ensure Join message well received by other device。

Leave timer：Using to control transmission of Leave message, when Leave or LeaveAll received, it will activate Leave timer.

LeaveAll timer： When Port enable GVRP function,it will activate LeaveAll timer, once time Out occurred, it will send out LeaveAll message. when LeaveAll received, LeaveAll timer will be reset to avoid unnecessary packet.

GVRP Configuration

Advanced Features -> GVRP Settings



Parameter	Description
GVRP Settings	Enable or Disable GVRP Feature
Join Time	Configure Join Time, Must be 2 seconds or greater
Leave Time	Configure Leave Time, Must be greater than 2*Join Time
Leaveall Time	Configure Leaveall Time, Must be greater than Leave Time

7.8 Neighbor MACID

Neighbor MACID is to find out Neighbor switch's MAC ID, base on select send period to transmit Neighbor Info packet, when switch receive Neighbor Info packet, will save and update MAC ID and Aging time, by using UDP NetCmd, can get Switch Neighbor MAC ID information.

Neighbor MACID Configuration

Advanced Features -> Neighbor MACID Settings

Parameter	Description
Status	Enable or Disable Neighbor MACID Feature
Send Period	Configure the duration in between every packet.
Aging Time	Configure aging time of each MAC.

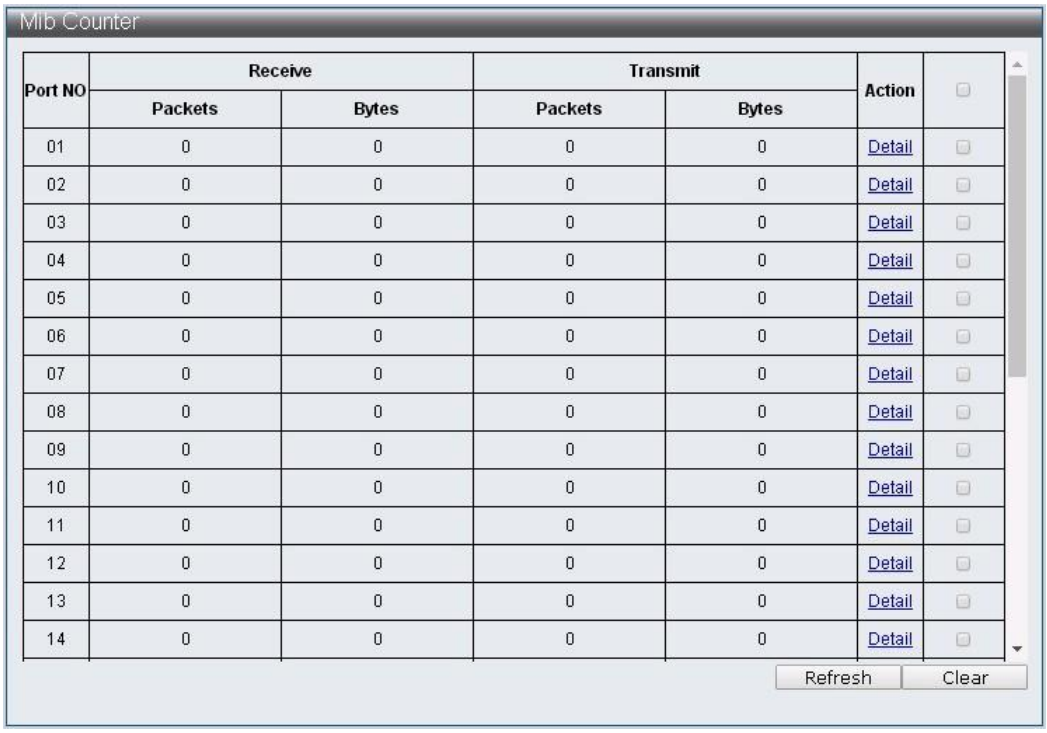
8 Monitoring

8.1 MIB Counter

MIB Counter provides the calculated data of packet number & bytes of each port, it can be narrow down to 28 of received packet type and 14 of transmitted packet type.

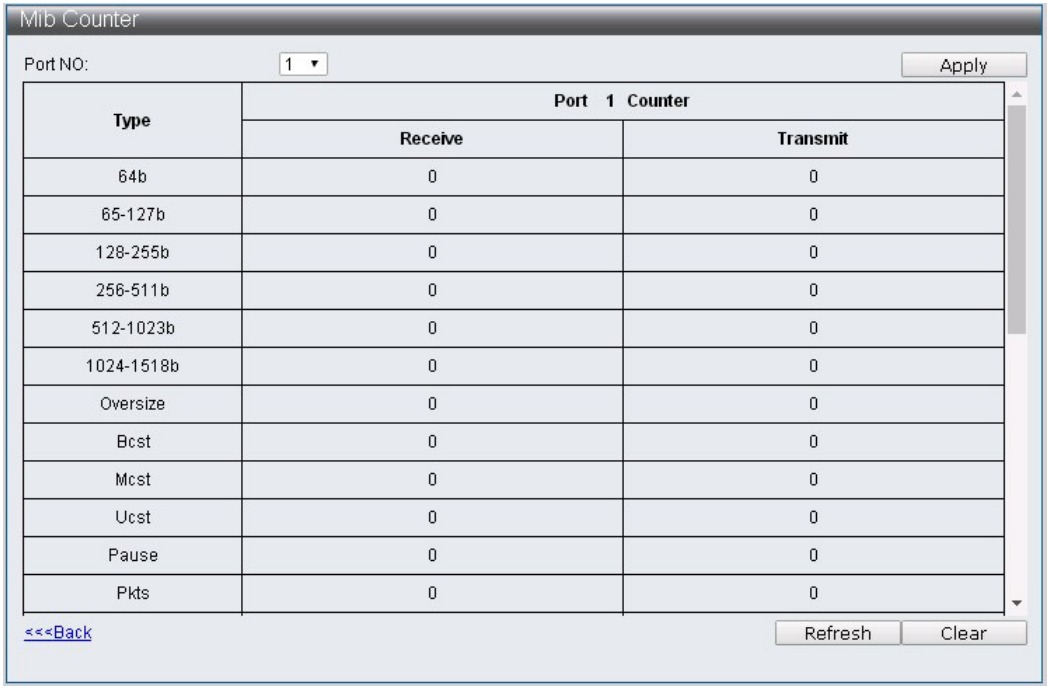
MIB Counter Configuration

Monitoring -> MIB Counter



Parameter	Description
Port No.	Port Number
Receive	The data of received Packets and Bytes
Transmit	The data of transmitted Packets and Bytes
Action	Port Detail Information
Refresh	Refresh packet counter
Clear	Clear packet counter

Monitoring -> MIB Counter -> Detail



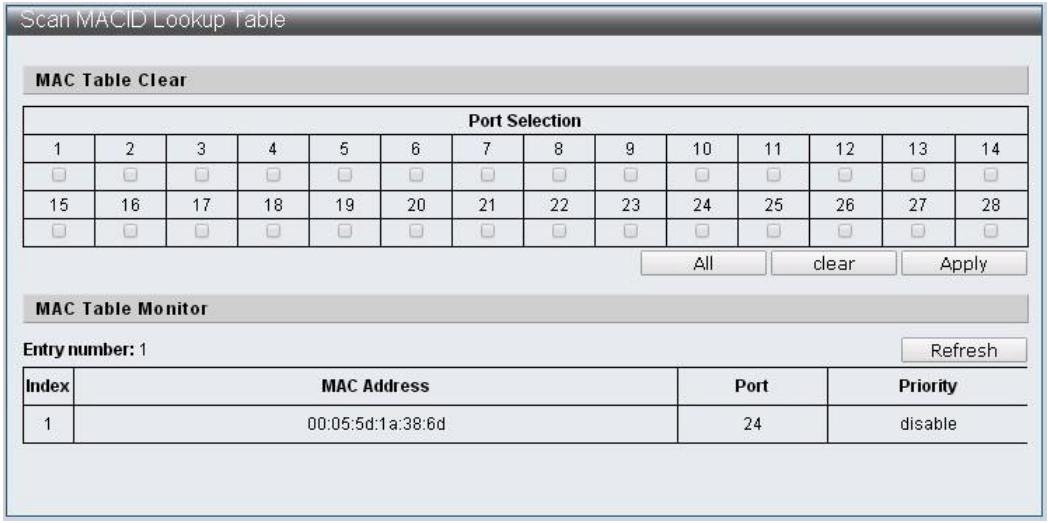
Parameter	Description
Type	Packet Type
Receive	The data of received Packets
Transmit	The data of transmitted Packets
Refresh	Refresh packet counter
Clear	Clear packet counter

8.2 Scan MACID Lookup Table

Scan MACID Lookup Table provides MAC Address for every port. Also, user is able to delete Lookup Table's MAC Address.

Scan MACID Lookup Table Configuration

Monitoring -> Scan MACID Lookup Table



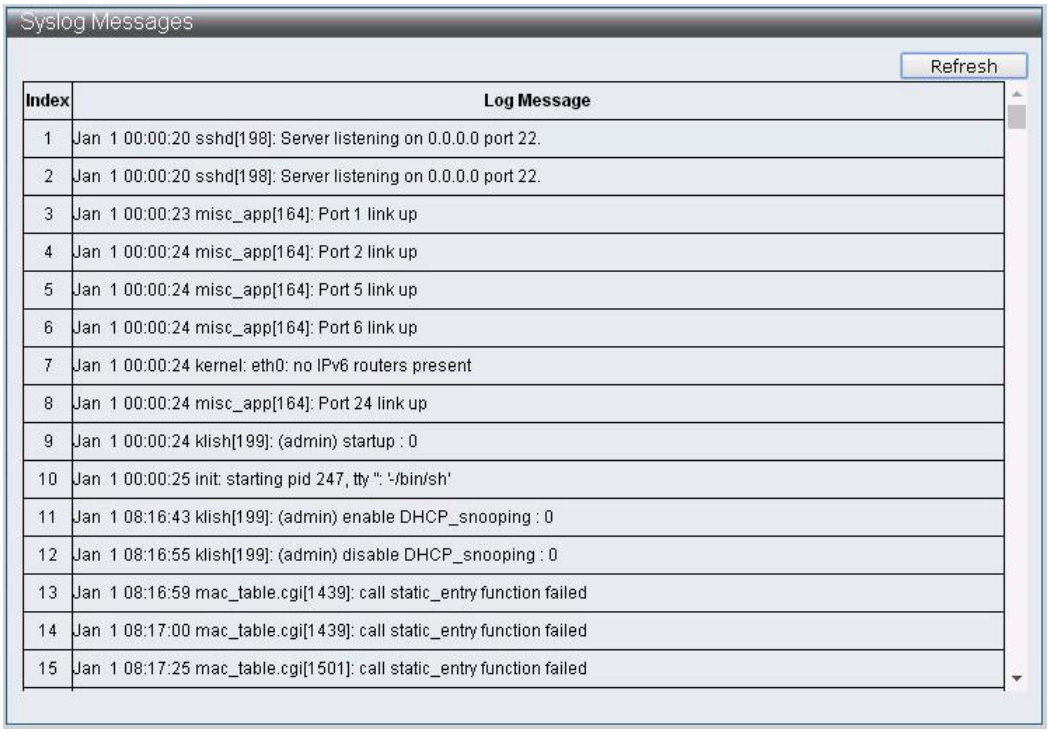
Parameter	Description
Port Selection	Select corresponding port
All	Select all port
Clear	Clear MAC address
Apply	Clear selected port's MAC Table
Refresh	Refresh MAC Table

8.3 Syslog

Syslog provides the configuration history of switch manager.

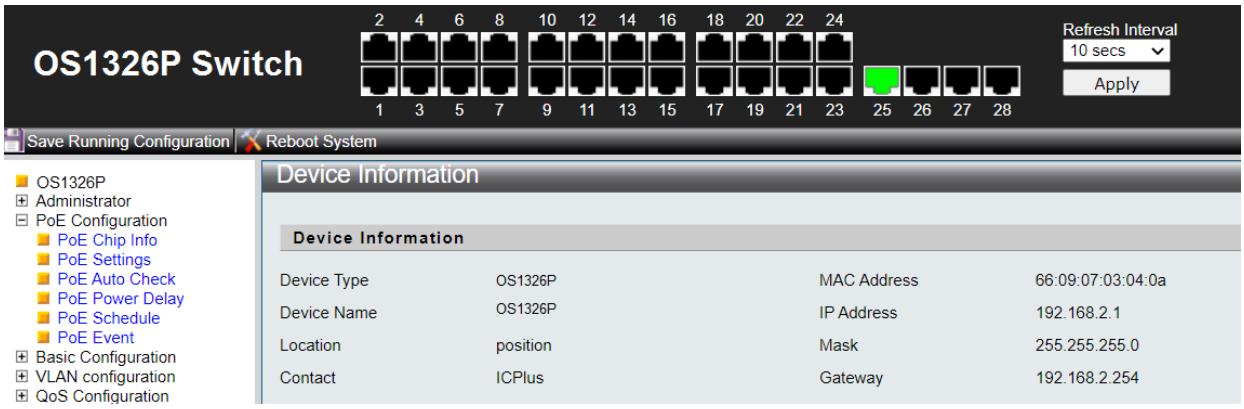
Syslog Configuration

Monitoring -> Syslog

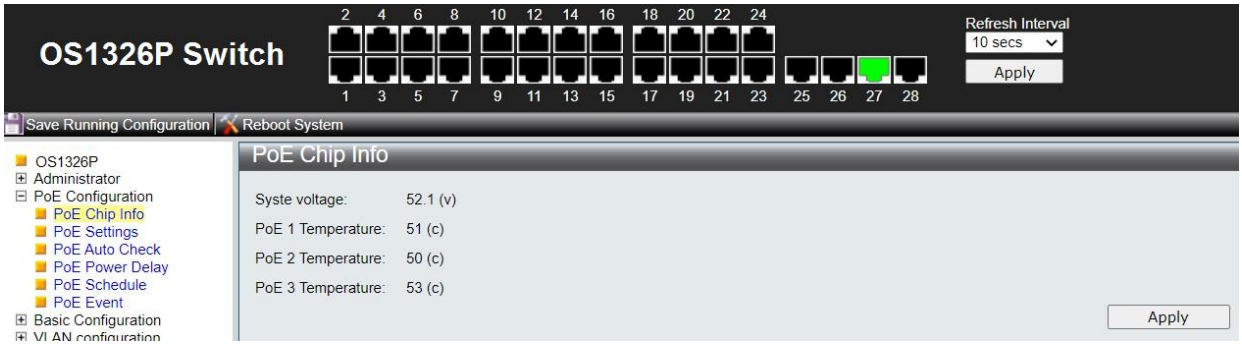


Parameter	Description
Refresh	Update system history

9 PoE Configuration

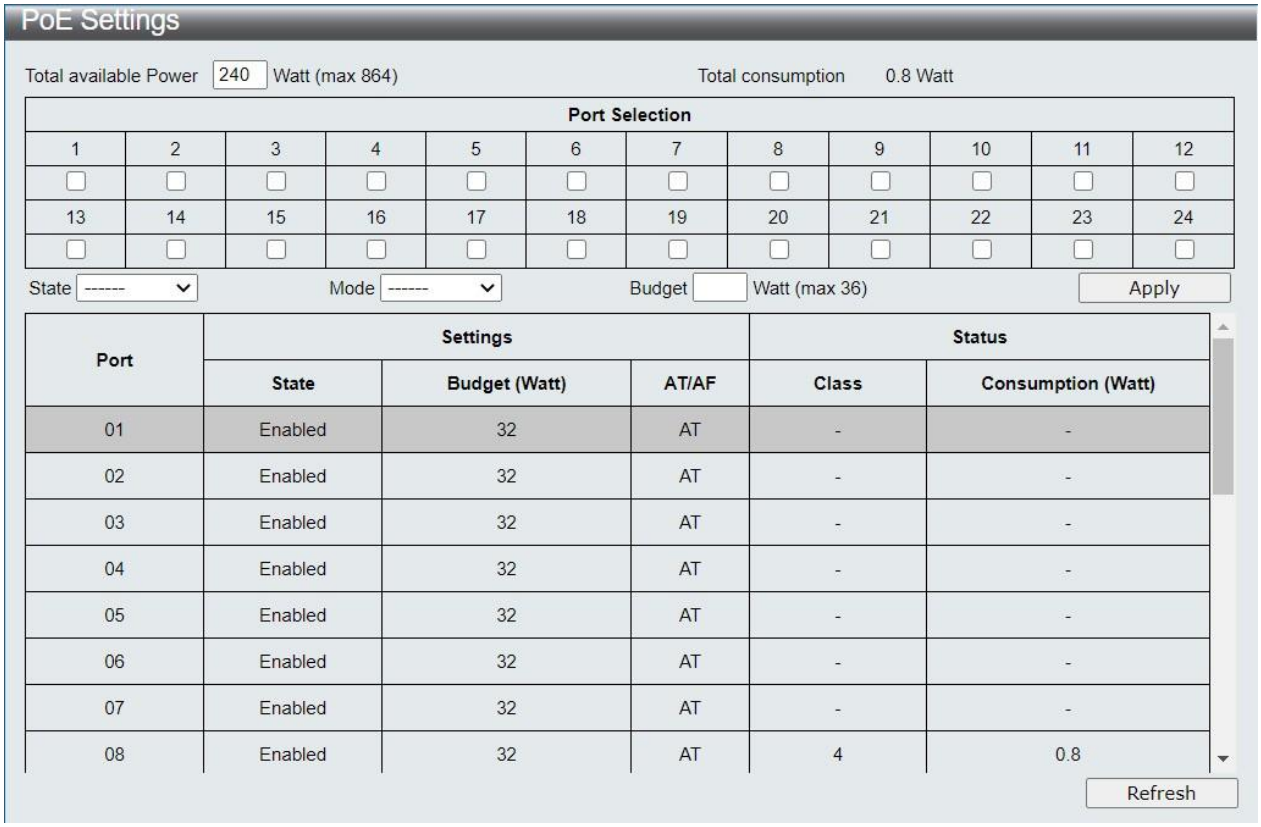


9.1 PoE Chip info



PoE chip Information displays system voltage and PSE chip temp.

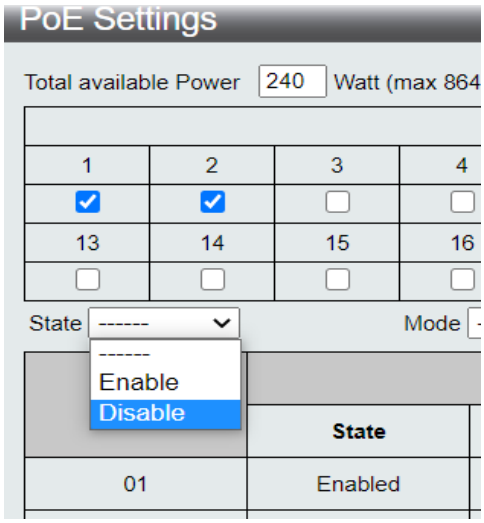
9.2 PoE setting



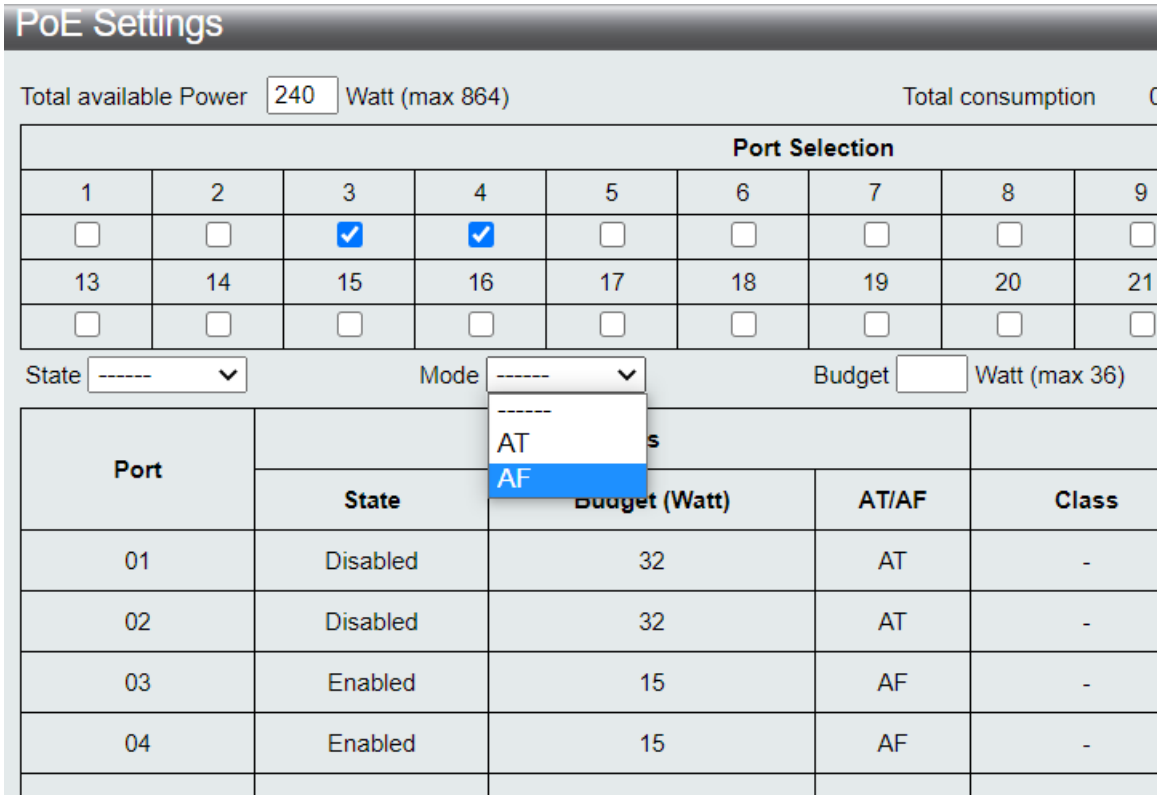
This page allows user to configure PoE system's total available power and port configuration such Port enable/disable, AF/AT mode and Port power budget

PoE setting page also displays System total power consumption and port status Information such as Port state, Port power budget, AF/AT mode, Class of connected PD and Port power consumption .

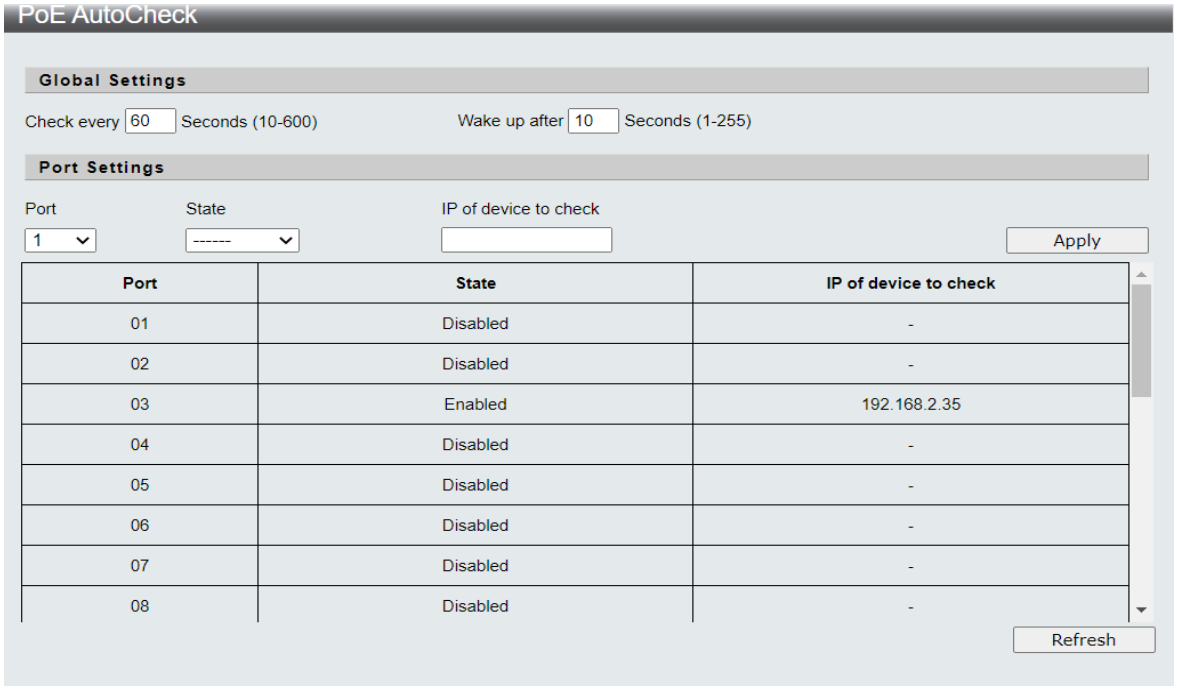
Ex. Port state setting(Enable/Disable) of Port 1 & 2



Ex. Port state setting(Enable/Disable) of Port 3 & 4



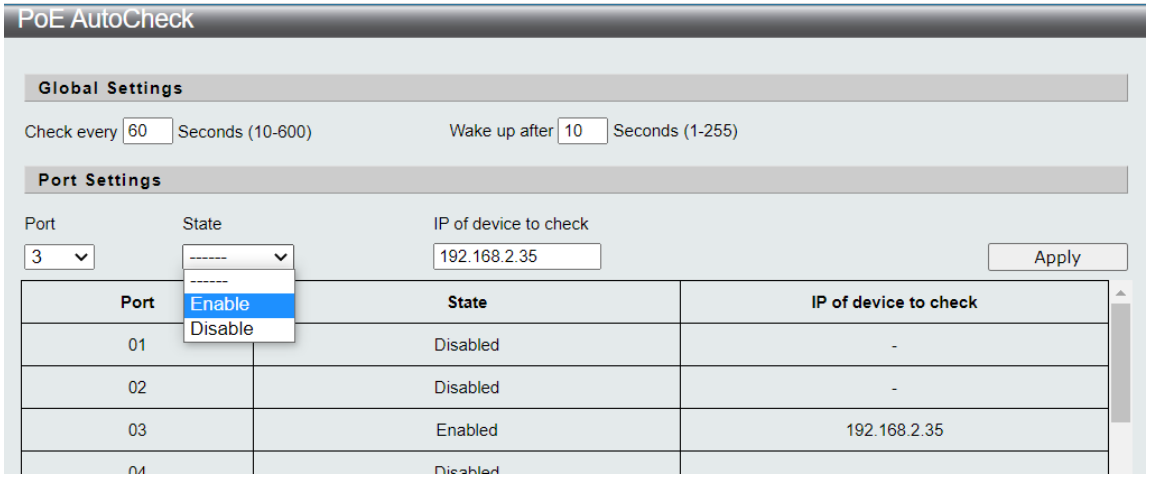
9.3 PoE Auto Check



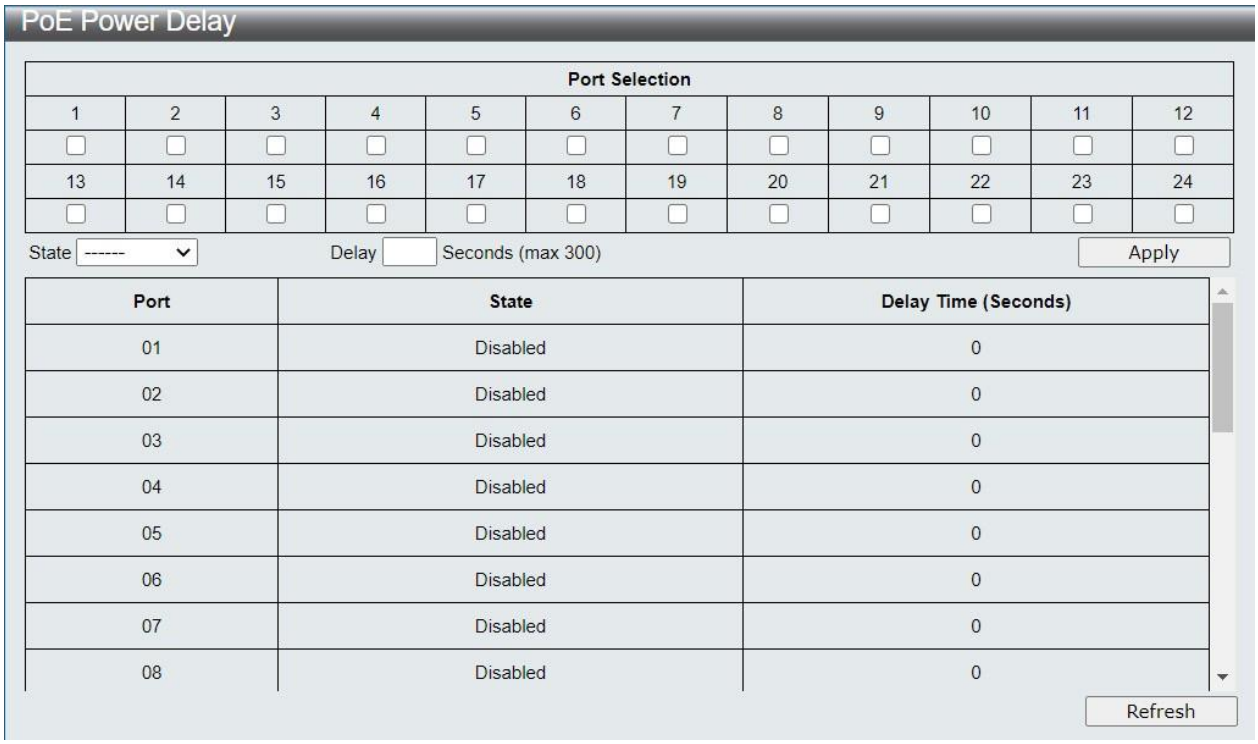
PoE Auto Check provides PD auto recovery function through PD status checking and power on/off. User can set the Checking time, wake up time and IP of each connected PD on this page.
IP211 CPU will follow this configuration to ping connected PD, if ping ACK received by CPU Means PD works normally and if no ACK response from PD, IP211 CPU will power off port and Re-power on again.

Checking time: From 10 ~ 600 seconds
Wake up after: From 1 ~ 255 seconds

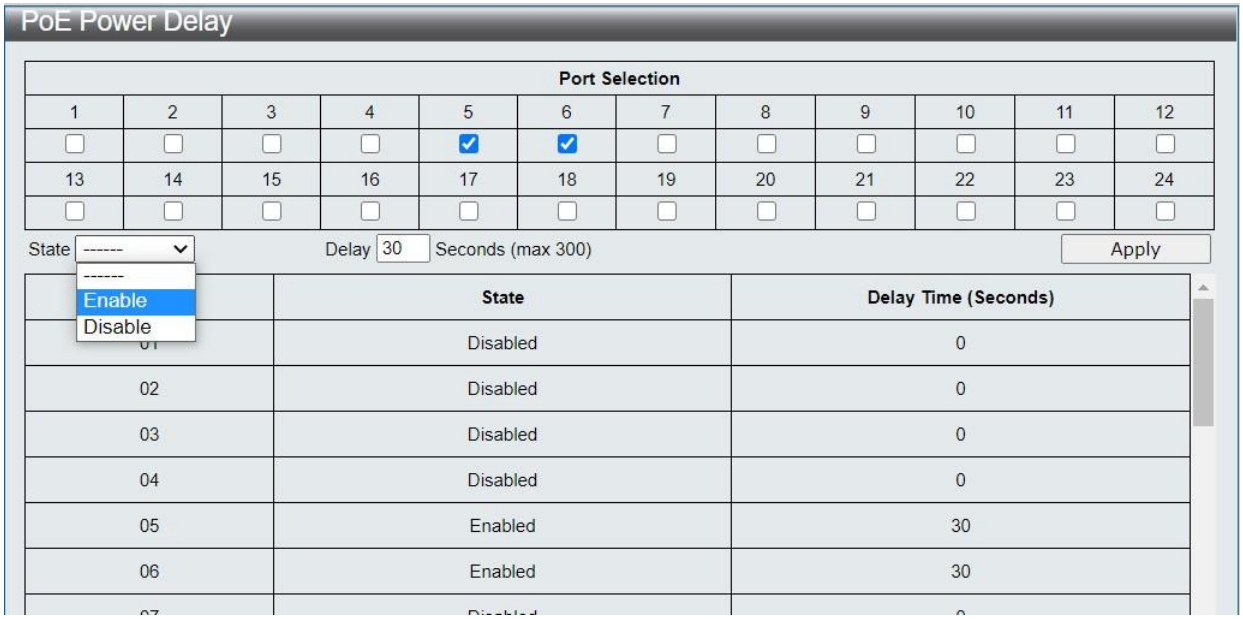
Ex. PoE Auto Check setting of port 3, IP: 192.168.2.35



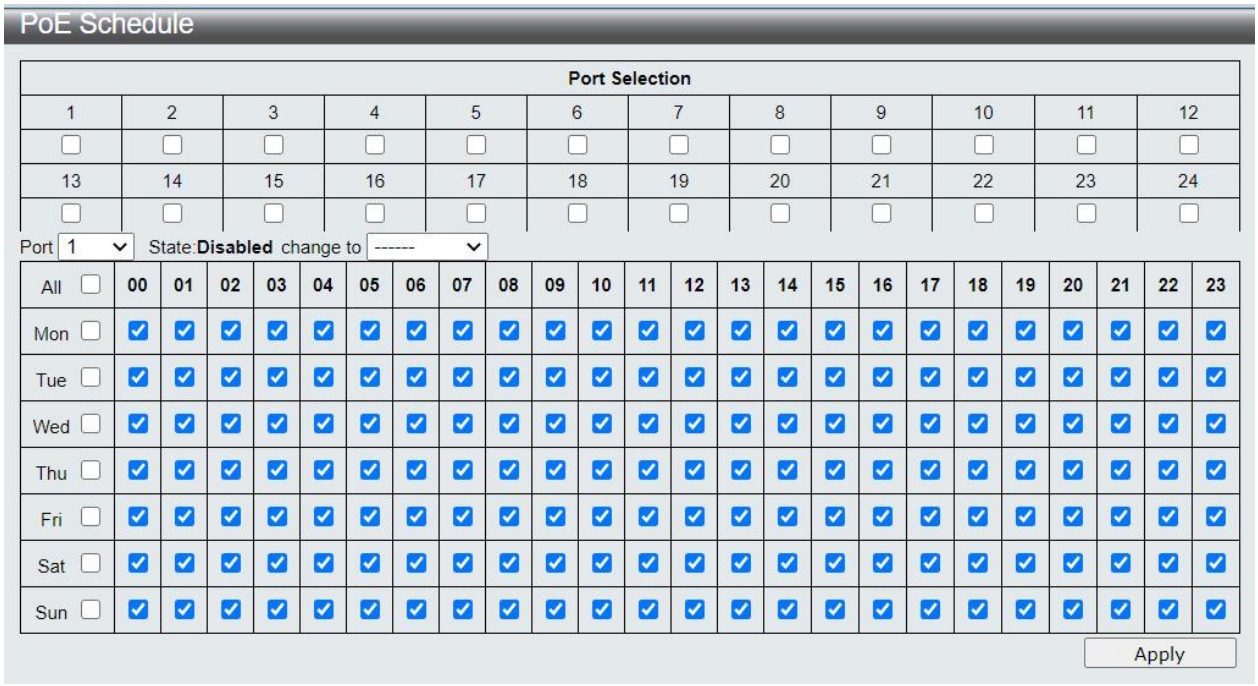
9.4 PoE Power delay



Allow user to set power on delay after system initial, during this period, PoE port will be disable.



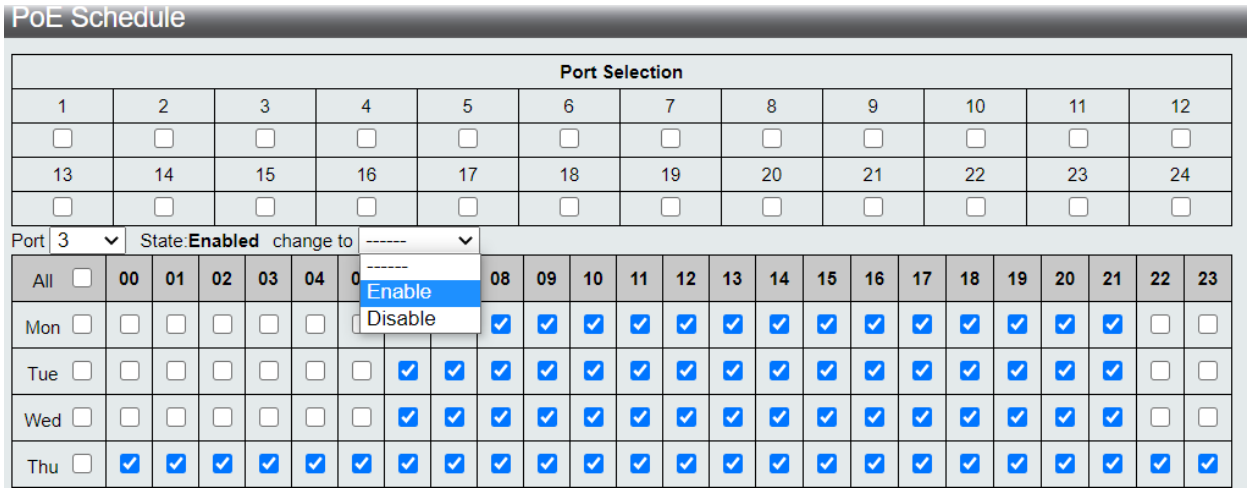
9.5 PoE Schedule



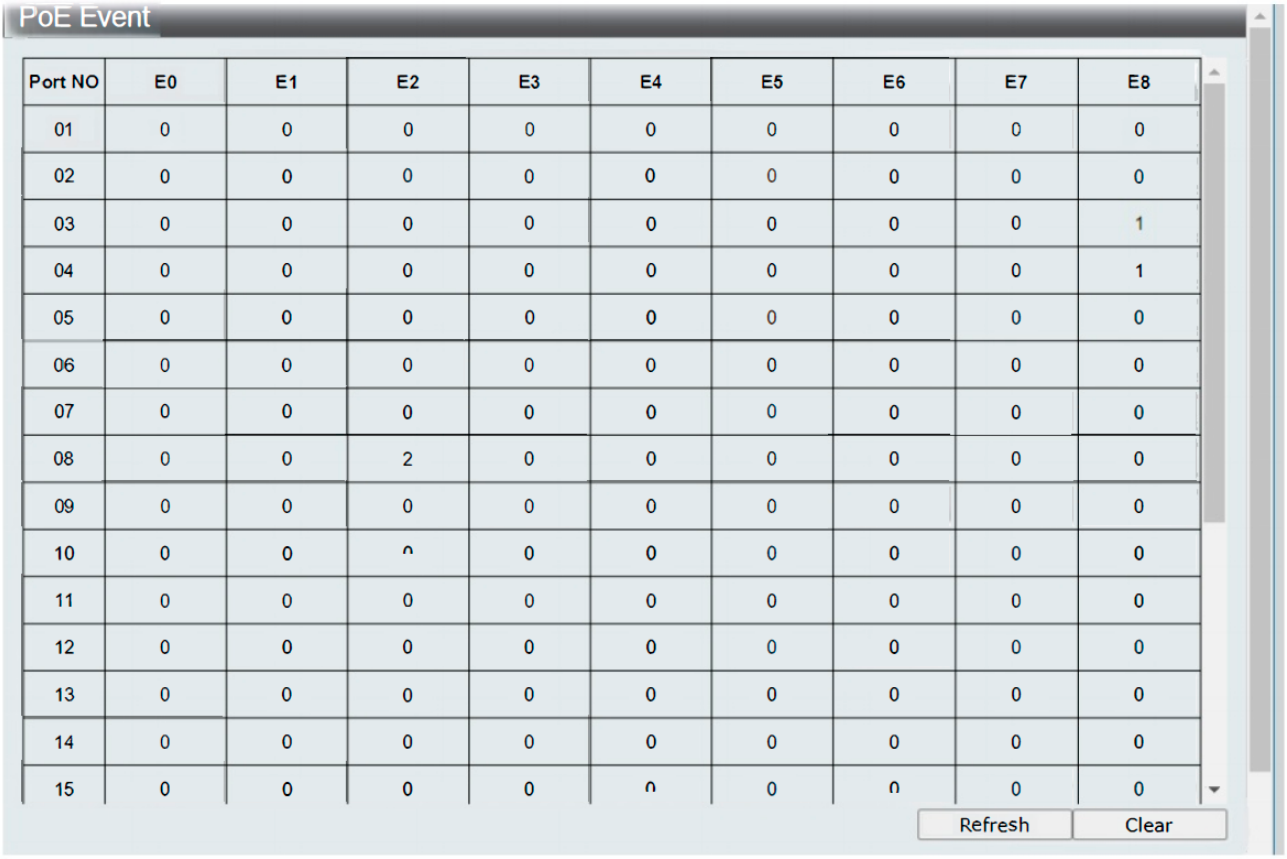
Allow user to configure PoE port power on period. Through NTP function, switch can remain accurate time to manage port power on/off time.

User can select port, Enable/Disable, date and hour for scheduling configuration.

Ex. Port 3 scheduling configuration.



9.6 PoE Event



PoE event displays the power off events of PoE ports which allows user to identify PoE power off record of each port.

E0:Port Overload (ICUT) Event
E1:Port Short Circuit Limit (ILIM) Event
E2:Port MPS Error (DC Disconnect) Event
E3:Port Thermal Shutdown Event
E4:Main Power Overload Event
E5:Port Voltage Limit Event
E6:Port Temperature Limit Event
E7:PoE Auto Check Timeout Event
E8:PoE Schedule Event