Web Management Guide

(Hilbert Smart Lite Switches)

level one

FCC STATEMENT

Manual Description

This user guide is provided for using this type of switch. The manual includes the switch performance and function. Please read this manual before managing the device:

Intended Audience

This guide is intended for network administrators familiar with IT concepts and network terminology.

SAFETY NOTICES

Do not use this product near water, for example, in a wet basement or near a swimming pool. Avoid using this product during an electrical storm. There may be a remote risk of electric shock from lightning.

TABLE OF CONTENTS

Chapter 1: Introduction

1.1 Running the Application

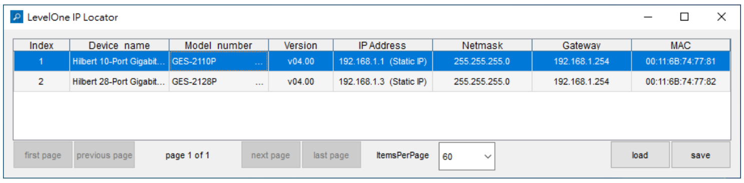
Can be matched with the latest LevelOne IP Locator, the software is the easiest to use switch discovery tool, it can search all Hilbert series switches, instantly know the forgotten IP and other info. Compatible with mainstream Windows and Mac operating systems.

1. Scan the Setup code, download the LevelOne IP Locator and launch it.
   http://level1.info/iplocator

levelone IP Locator

2. Execute the application "**LevelOne IP Locator.exe**".

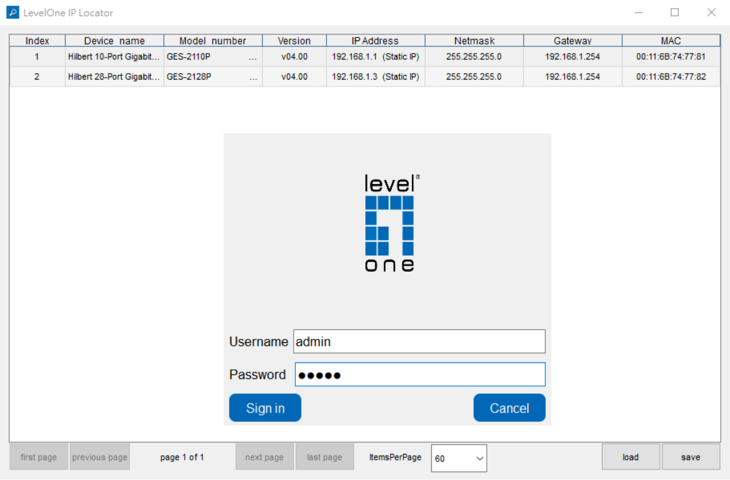
3. The LevelOne IP Locator Utility will search all Hilbert series switches based on the connect network interface card (NIC), instantly know the forgotten IP address and other info.



LevelOne IP Locator

Index	Device name	Model number	Version	IP Address	Netmask	Gateway	MAC
1	Hilbert 10-Port Gigabit...	GES-2110P ...	v04.00	192.168.1.1 (Static IP)	255.255.255.0	192.168.1.254	00:11:6B:74:77:81
2	Hilbert 28-Port Gigabit...	GES-2128P ...	v04.00	192.168.1.3 (Static IP)	255.255.255.0	192.168.1.254	00:11:6B:74:77:82

4. Simply click with the mouse on the device's IP address in the device list for configuration. On the displayed login screen, enter the factory username "admin" and password "admin", then click "Sign in".



LevelOne IP Locator

Index	Device name	Model number	Version	IP Address	Netmask	Gateway	MAC
1	Hilbert 10-Port Gigabit...	GES-2110P ...	v04.00	192.168.1.1 (Static IP)	255.255.255.0	192.168.1.254	00:11:6B:74:77:81
2	Hilbert 28-Port Gigabit...	GES-2128P ...	v04.00	192.168.1.3 (Static IP)	255.255.255.0	192.168.1.254	00:11:6B:74:77:82

Username admin

Password ●●●●●

1.2 Features

- Support link aggregation.
- Support port VLAN and IEEE 802.1Q VLAN.
- Support rate limit, port statistics.
- Support port mirroring.
- Support QoS, providing strict priority.
- Support Loop Prevention.
- Support MAC Address binding.
- Support storm control.
- Support the port Isolation.
- Support IGMP snooping, multicast probe.
- Support WEB-based management.
- Support WEB-based firmware upgrade.
- Support parameter backup and recovery.

Technical Specifications

The web-smart switch front panel has 8/16/24 port 10/100M adaptive UTP ports, and the LED indicator. The 8/16/24 ports support 10/100Mbps bandwidth connection device, auto-negotiation capability. Each port corresponds to a set of indicator, LNK / ACT.

Chapter 2: Mounting Device

2.1 Installation Precautions

Ensure the surface on which the device is placed is adequately secured to prevent it from becoming unstable Ensure the power outlet is placed within 1.8m (6feet) of the device. Ensure the device is connected safely to the power outlet with the AC power cable. Ensure the device around good ventilation and heat dissipation.
Do not place heavy objects on the device

2.2 AC POWER

The switch can be used with AC power supply 100 to 240V AC,50 to 60Hz.. Switch built-in power supply system can be the actual input voltage automatically adjusts its operating voltage. The power connector is located on the rear panel switch. Disconnect the power cord is a plug on the power switch on the rear panel interface,the other end plugged into a power outlet.

Chapter3: Login The Device

You can use the web browser-based configuration to manage Web-Smart Switch. The Web-Smart Switch to be configured through a web browser, at least a reasonable allocation of computer through an Ethernet connection to Web-Smart Switch.

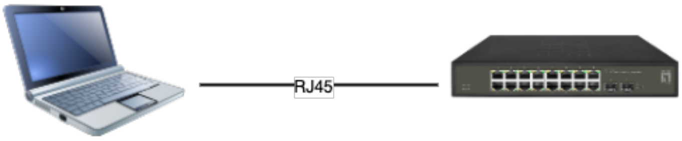


Figure 3-1

Default IP address of the switch:192.168.1.1. Subnet mask: 255.255.255.0.
When logging in the switch, make sure that the IP addresses of the host network card and the switch are in the same network segment: 192.168.1. *** (1 <*** <255， *** is not 11). See the following setting steps：

3.1 configure the computer

The Management switch is managed via WEB pages. The smart and friendly interfaces make the switch management an easy job. Due to the difference of Operating system, the WEB page display may differ between variable Operating System.

3.1.1 Windows 7/Windows Vista

Follow these steps to configure your computer
1、Start-Control Panel

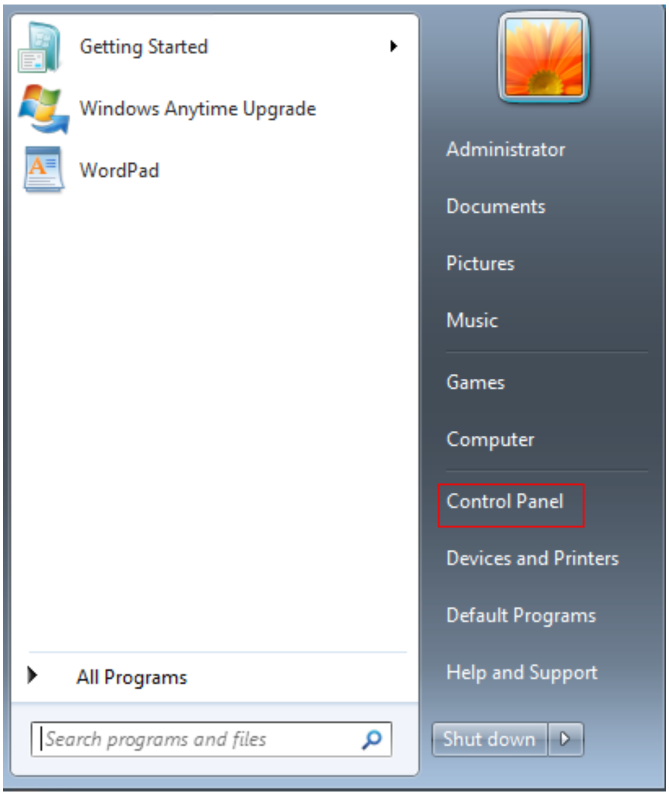


Figure 3-1-8

2、Click ”Network and Internet ”

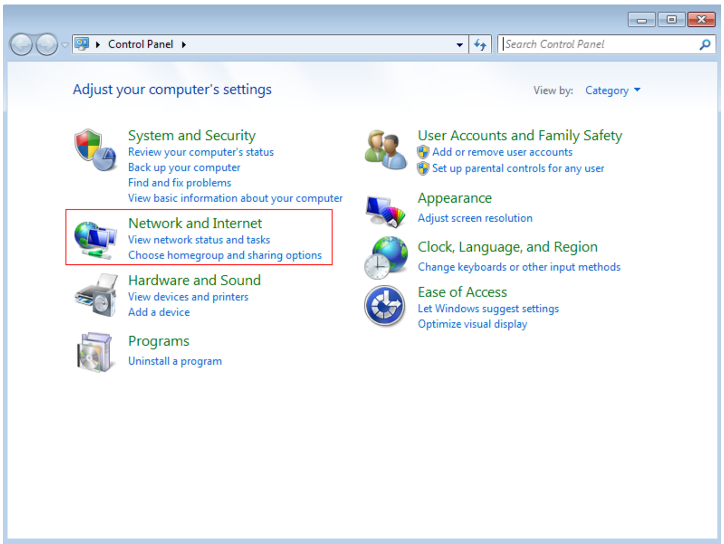
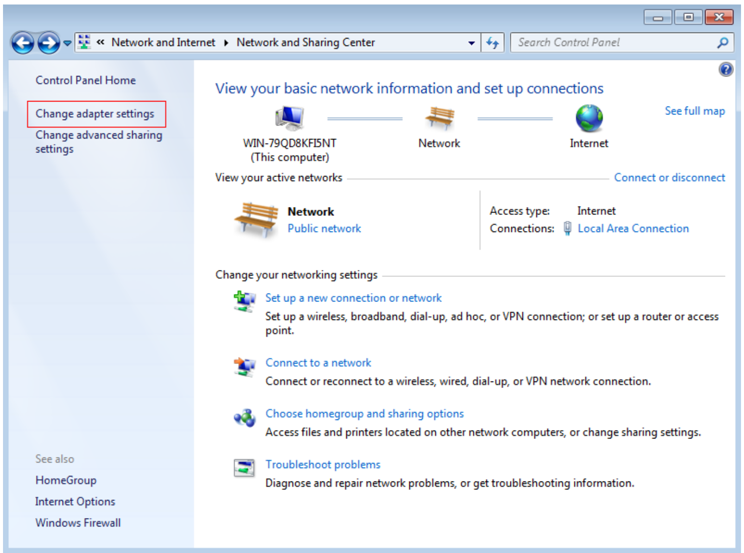

Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
View basic information about your computer
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Ease of Access
Let Windows suggest settings
Optimize visual display

Figure 3-1-9

3、Click ”Change adapter settings”


« Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
See also
HomeGroup
Internet Options
Windows Firewall
View your basic network information and set up connections
See full map
WIN-79QD8KFI5NT
(This computer)
Network
Internet
View your active networks
Connect or disconnect
Network
Public network
Access type: Internet
Connections: Local Area Connection
Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

Figure 3-1-10

4. click right-hand button on the adapter icon and click “Properties”

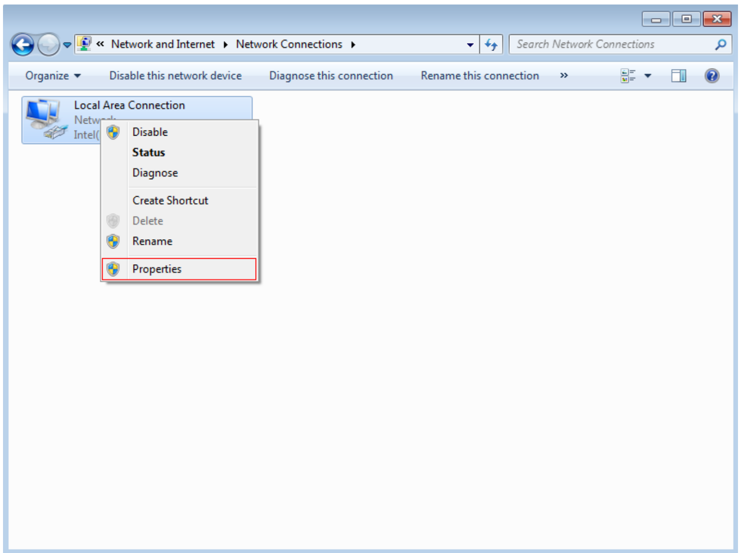
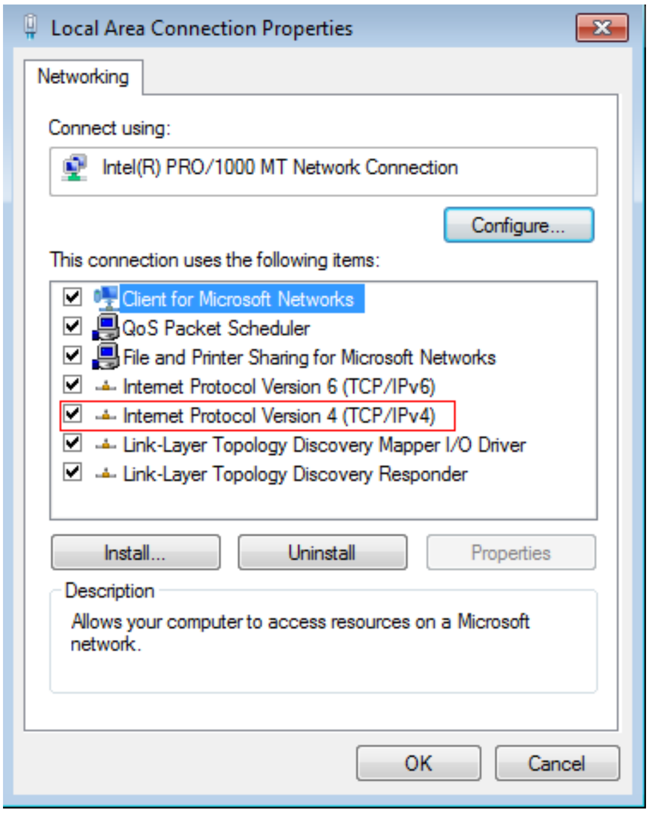


Figure 3-1-11

5.Double clik “Internet protocol Vertion 4(TCP/IPv4)”



Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Network Connection

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

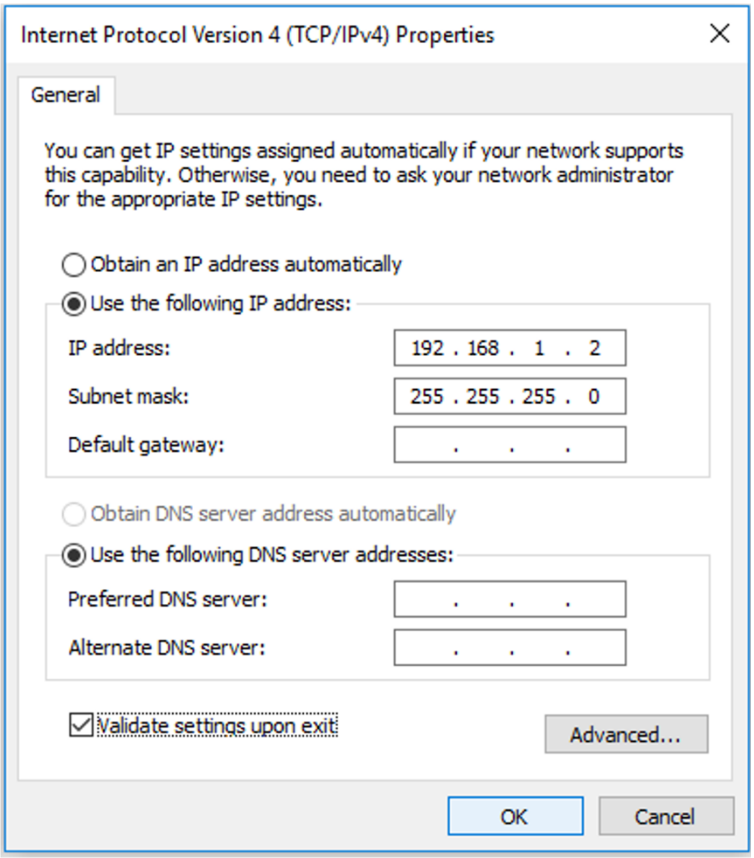
Description

Allows your computer to access resources on a Microsoft network.

Figure 3-1-12

5、Use the following IP address: input IP 192.168.1. *** (1 <*** <255, *** is not 11, because the default IP of the switch is 192.168.1.1), Subnet mask: 255.255.255.0. The default gateway and DNS server are optional, and then click “OK” to close the Internet TCP / IP properties window.

Figure 3-1-13



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

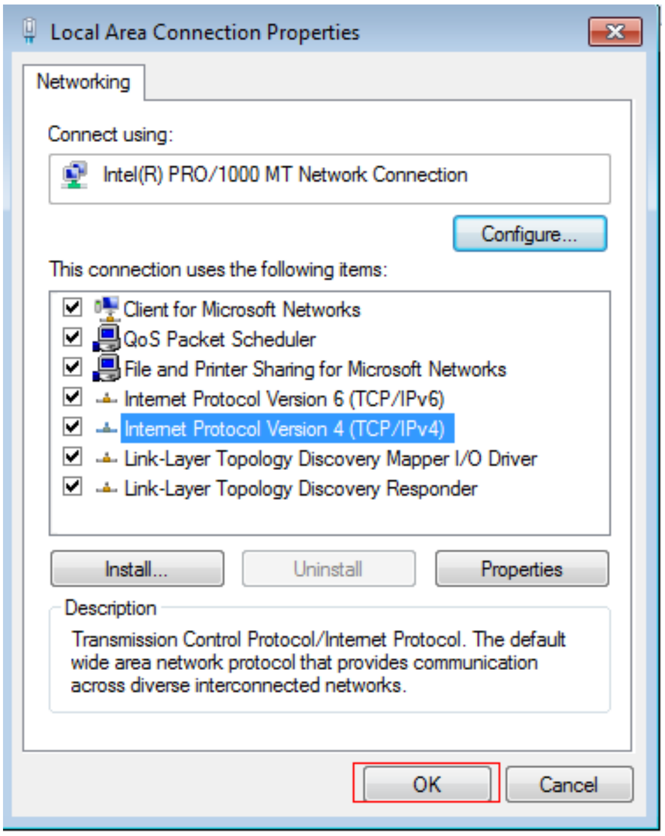
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☑ Validate settings upon exit

6、CLICK “OK” and Close the Local Area Connection Properties window


Local Area Connection Properties
Networking
Connect using:
Intel(R) PRO/1000 MT Network Connection
Configure...
This connection uses the following items:
☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties
Description
OK
Cancel

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

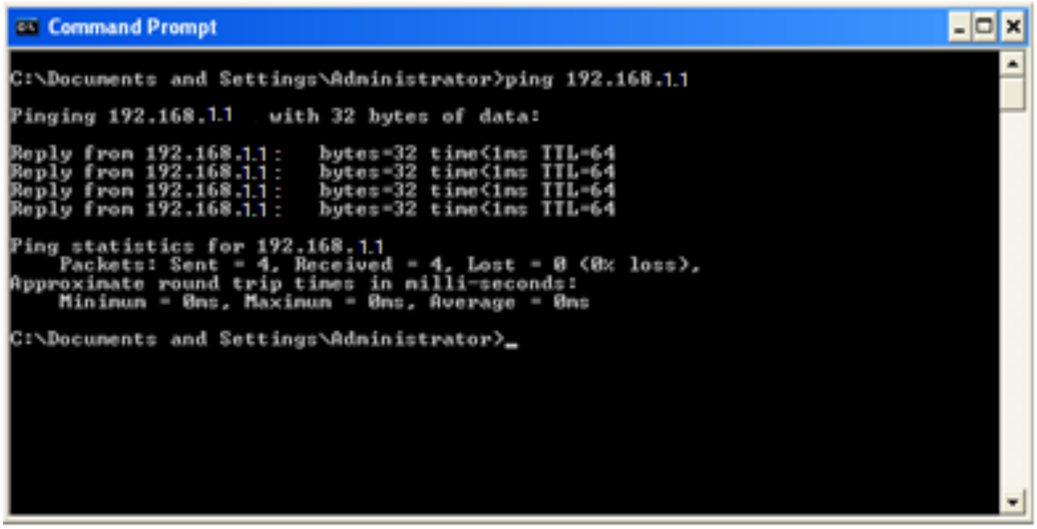
Figure 3-1-14

3.2 Check the connection

After setting the TCP / IP protocol, you can use the Ping command to verify whether the computer can communicate with Web-Smart Switch. To perform a ping command, open a command window, the IP address in the command prompt where the Ping Web-Smart Switch

Windows XP，START-Control，type cmd in the search bar and press Enter Windows 7，Click Start, type cmd in the search bar and press Enter where the DOS prompt, enter the following command.

If the command window return to something like the following:

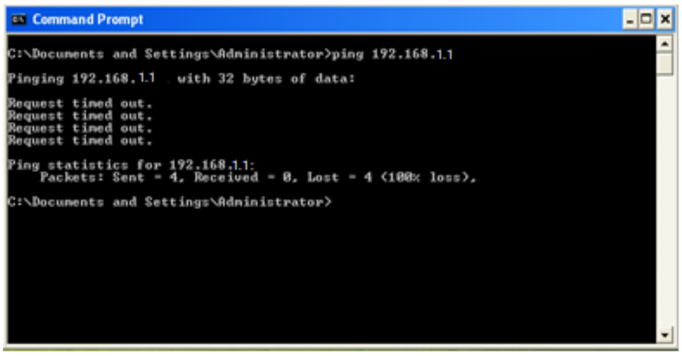


```
C:\Documents and Settings\Administrator>ping 192.168.1.1

Pinging 192.168.1.1   with 32 bytes of data:

Reply from 192.168.1.1:   bytes=32 time<1ms TTL=64
Reply from 192.168.1.1:   bytes=32 time<1ms TTL=64
Reply from 192.168.1.1:   bytes=32 time<1ms TTL=64
Reply from 192.168.1.1:   bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.1
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```

Figure 3-2-1

Then Connection between Web-Smart Switch and computer is successful

If the computer failed to connect on of Web-Smart Switch, the command window will return the following content



```
C:\Documents and Settings\Administrator>ping 192.168.1.1

Pinging 192.168.1.1  with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\Administrator>
```

Figure 3-2-2

Then make sure that your computer's network settings are correct and the cable is intact.

Caution:

YOU need to use a twisted pair to connect the port of your computer's network card to the switch port before entering the above command

3.3 Login the device

1、Open IE browser,enter http://192.168.1.1 in the address bar, then return.

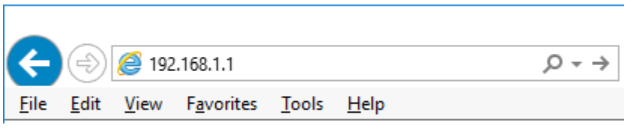

192.168.1.1

Figure 3-3-1

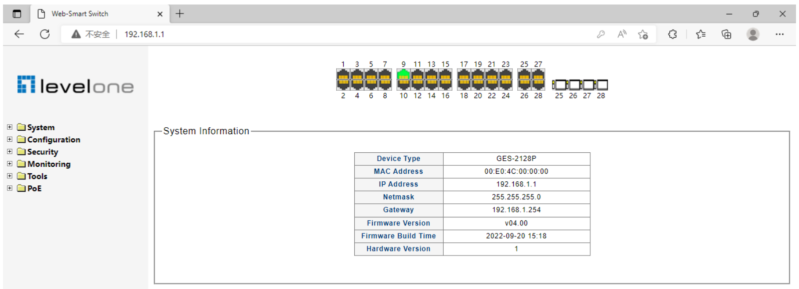
2、In the pop-up window to enter user name: admin, password: admin, then press the OK button.

NOTES:

If you are successful login into the switch webpage, the page from time to time automatically refresh, allowing you to dynamically view the port status.

3.4 Functional Overview

The Web-Smart Switch have rich feature, including the functions of system management, Port Management, Redundancy management, Security management, QoS management, Network Analysis, next chapter will introduce you these functions.



System Information

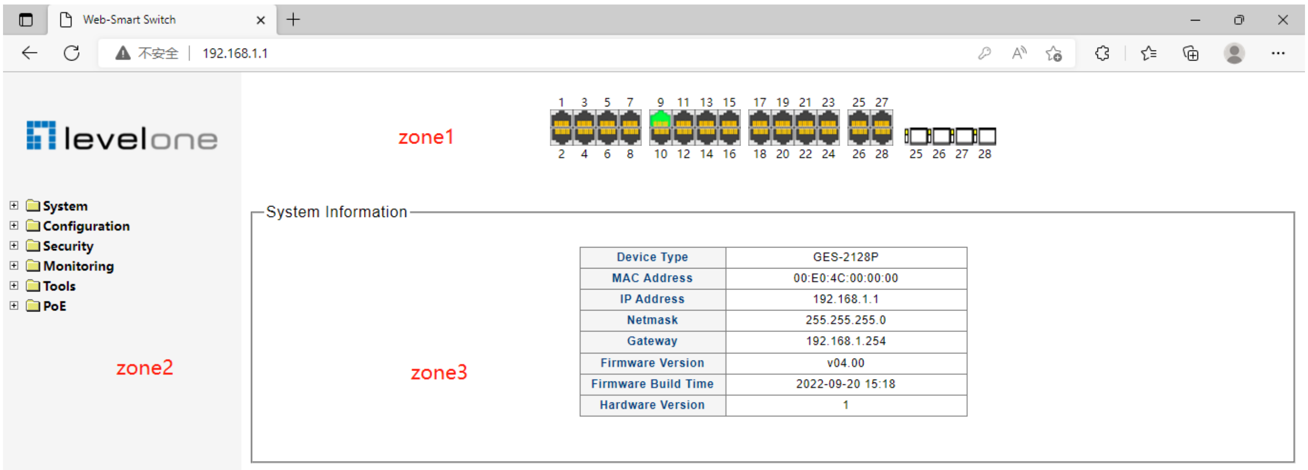
Device Type	GES-2128P
MAC Address	00:E0:4C:00:00:00
IP Address	192.168.1.1
Netmask	255.255.255.0
Gateway	192.168.1.254
Firmware Version	v04.00
Firmware Build Time	2022-09-20 15:18
Hardware Version	1

Figure 3-4-1

Chapter4: System

4.1 The Home page

After logging into the switch, the main page appears as the following. It contains three parts:



Device Type	GES-2128P
MAC Address	00:E0:4C:00:00:00
IP Address	192.168.1.1
Netmask	255.255.255.0
Gateway	192.168.1.254
Firmware Version	v04.00
Firmware Build Time	2022-09-20 15:18
Hardware Version	1

Figure 4-1-1

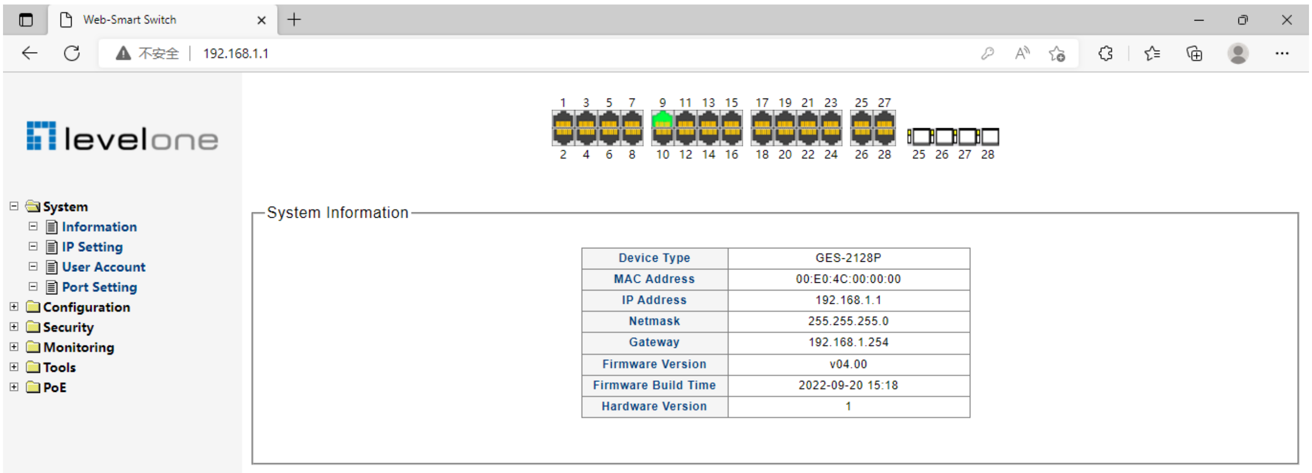
zone"1": The Port table lies at the top of the page. It provides a visual representation of the ports. The green icon indicates that the port is linked; the gray icon indicates that the port is not linked;

zone"2": On the left side of the page is the menu table. It contains 5 main menus. Each menu has some submenus. Click on a menu, it will open its submenus and the main window.

zone"3": The main part of the page is the main window to display the configuration page.

4.2 System Information

Click on the "System", the switch manage page will show as figure below, the system submenu have basic information, including: Information, IP Address, User Account, Port Setting. The following picture is the detailed description.

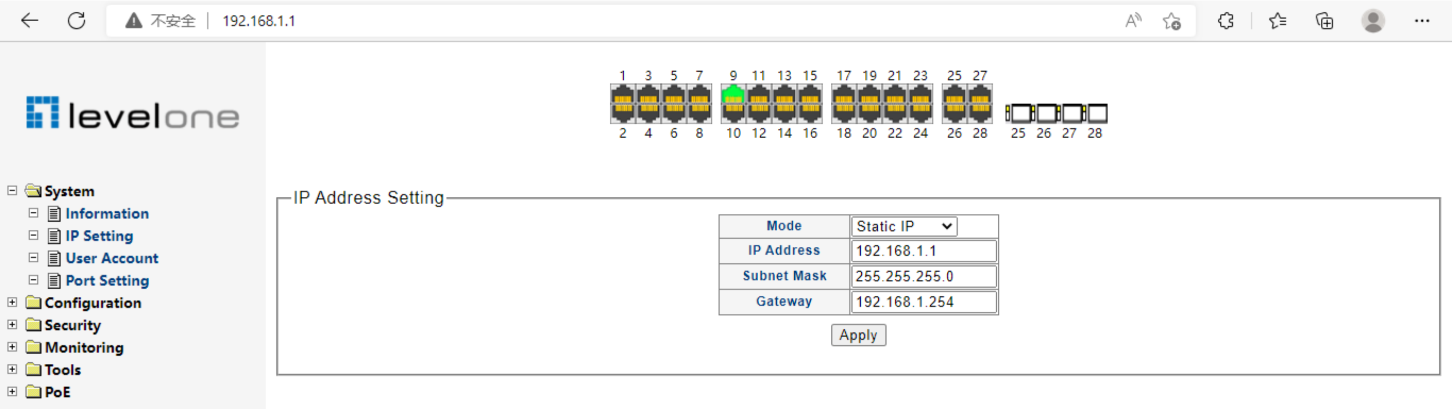


Device Type	GES-2128P
MAC Address	00:E0:4C:00:00:00
IP Address	192.168.1.1
Netmask	255.255.255.0
Gateway	192.168.1.254
Firmware Version	v04.00
Firmware Build Time	2022-09-20 15:18
Hardware Version	1

Figure 4-2-1

The System Information shows the system information of the switch, such as Device Type, MAC address, IP Address, Hardware and Software version information.

4.3 IP Address



IP Address Setting

Mode	Static IP
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	192.168.1.254

Figure 4-3-1

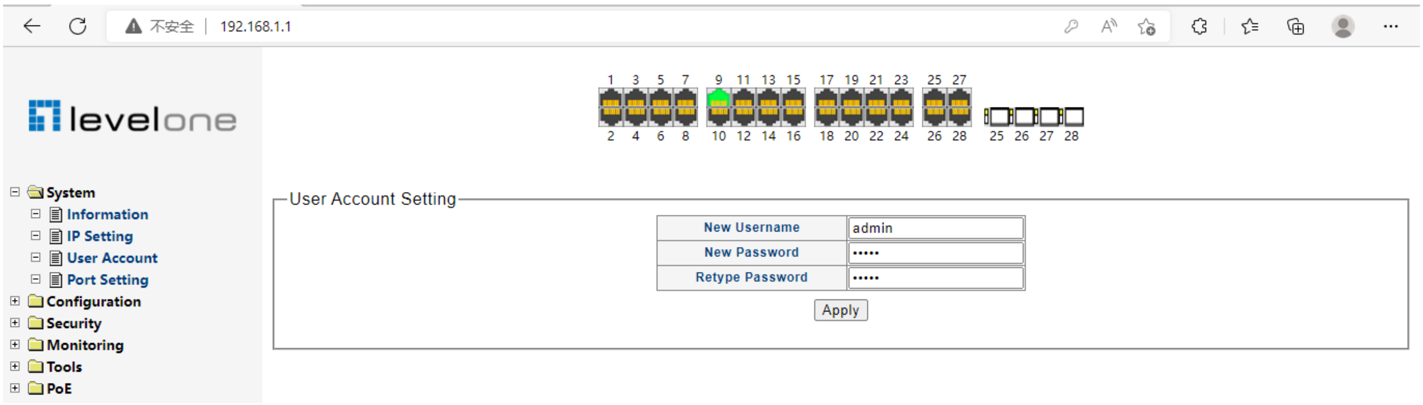
On this page you can manually set the IP address, subnet mask, gateway and other information; can also use your network, among other DHCP SERVER switch automatically assigns an IP address. The switch default IP address is: 192.168.1.1 default subnet mask: 255.255.255.0 Default Gateway: 192.168.1.254. When finished editing, click the "Apply" to complete the IP address settings.

Notes:

(1)When you select "DHCP Settings" is disabled, the switch will have to manually assign an IP address.
(2)When DHCP client is enabled, the IP parameters are obtained automatically from the DHCP server.

4.4 User Account

This page provides the interface of configuring username and password.



User Account Setting

New Username	admin
New Password	•••••
Retype Password	•••••

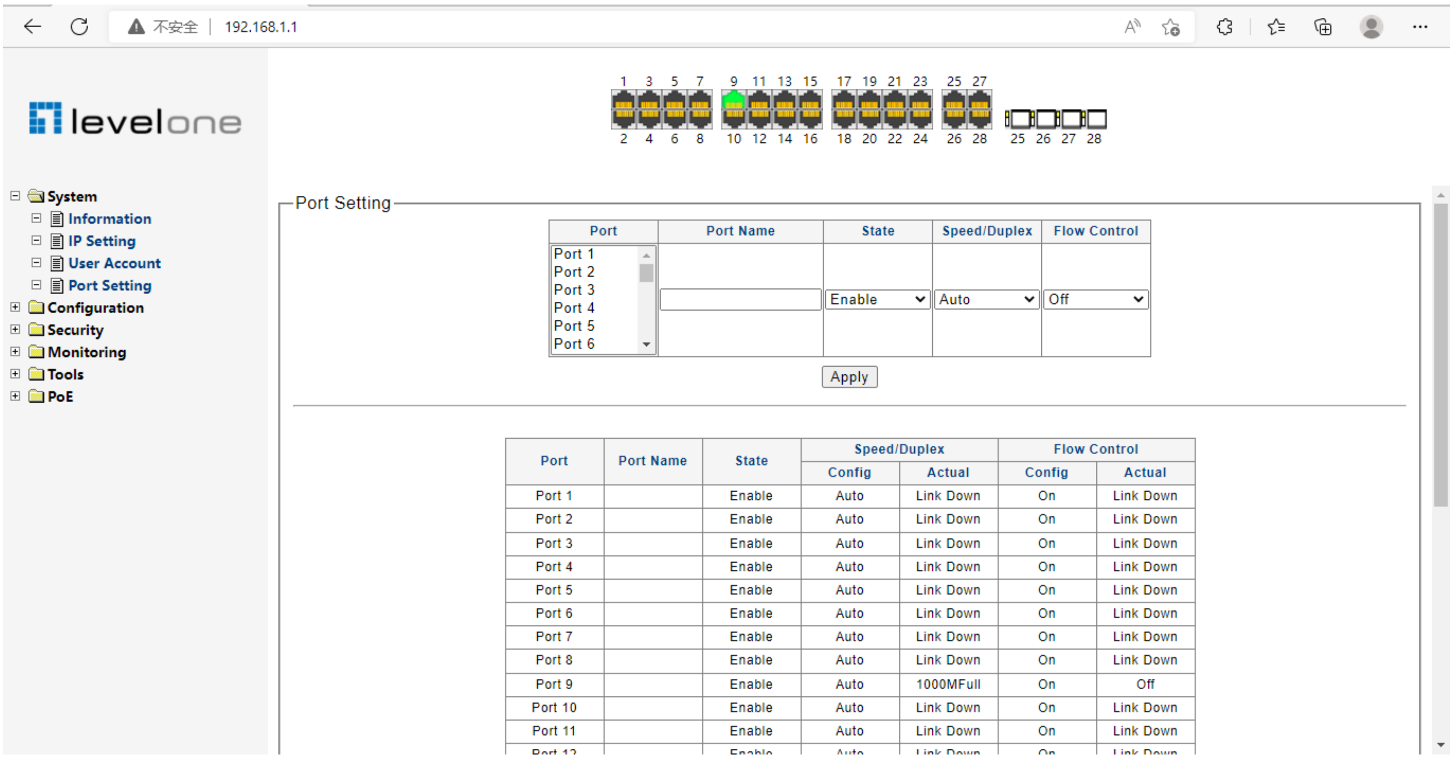
Figure 4-4-1

You are kindly suggested to retype the new password in "Confirm new password" box instead of copying in order to avoid typing mistakes.

Caution:
Only letters, numbers and punctuations can be input into username and password. The other characters are considered illegal. The initial password is admin.

Notes:
After modifying the password with immediate effect, the parameters will not be lost though is powered off.

4.5 Port Setting



Port Setting

Port	Port Name	State	Speed/Duplex	Flow Control
Port 1 Port 2 Port 3 Port 4 Port 5 Port 6		Enable	Auto	Off

Apply

Port	Port Name	State	Speed/Duplex		Flow Control	
			Config	Actual	Config	Actual
Port 1		Enable	Auto	Link Down	On	Link Down
Port 2		Enable	Auto	Link Down	On	Link Down
Port 3		Enable	Auto	Link Down	On	Link Down
Port 4		Enable	Auto	Link Down	On	Link Down
Port 5		Enable	Auto	Link Down	On	Link Down
Port 6		Enable	Auto	Link Down	On	Link Down
Port 7		Enable	Auto	Link Down	On	Link Down
Port 8		Enable	Auto	Link Down	On	Link Down
Port 9		Enable	Auto	1000MFull	On	Off
Port 10		Enable	Auto	Link Down	On	Link Down
Port 11		Enable	Auto	Link Down	On	Link Down
Port 12		Enable	Auto	Link Down	On	Link Down

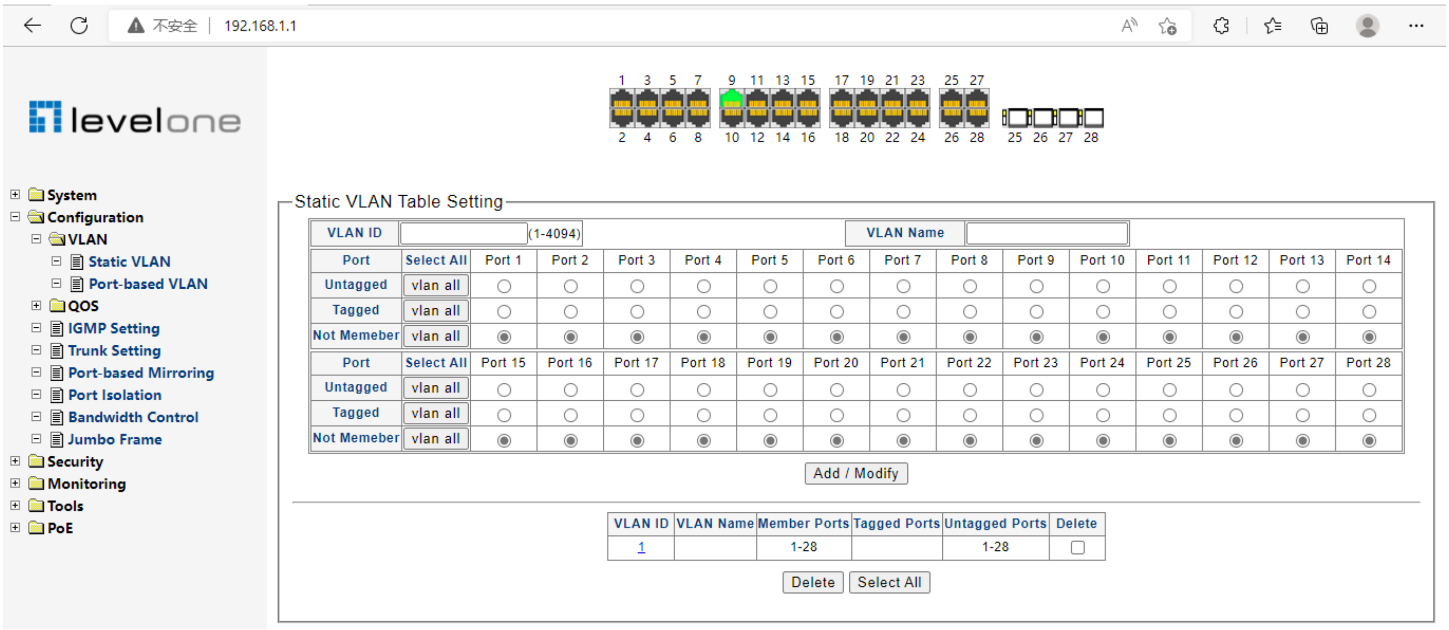
Figure 4-5-1

On this page, you can configure the basic parameter for the ports. When the port is disabled, the packers on the port will be discard. Shut down the port which is vacant for a long time can reduce the power consumption effectively. And you can enable the port when it is in need. The parameters will affect the working mode of the ports, please set the parameters appropriate. **Status:** Allows you to Enable/Disable the port. When Enable is set, the port can forward the packets normally.

Speed and Duplex: Select the speed and Duplex mode for the port. The device connected to the switch should be in the same Speed and Duplex mode with the switch. When “Auto” is set, the Speed and Duplex mode will be determined by auto-negotiation. But the SFP port, this Switch does not support auto-negotiation.
Flow Control: Allows you to Enable /Disable the Flow Control feature. When Flow Control is enabled, the switch can synchronize the speed with its peer to avoid the congestion.

Chapter5: Configuration

5.1 VLAN



Static VLAN Table Setting

VLAN ID	(1-4094)	VLAN Name	

Port	Select All	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8	Port 9	Port 10	Port 11	Port 12	Port 13	Port 14
Untagged	vlan all	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Tagged	vlan all	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Memeber	vlan all	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Port	Select All	Port 15	Port 16	Port 17	Port 18	Port 19	Port 20	Port 21	Port 22	Port 23	Port 24	Port 25	Port 26	Port 27	Port 28
Untagged	vlan all	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Tagged	vlan all	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Memeber	vlan all	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Add / Modify

VLAN ID	VLAN Name	Member Ports	Tagged Ports	Untagged Ports	Delete
1		1-28		1-28	□

Delete Select All

Figure 5-1-1

Introduction to VLAN

The traditional Ethernet is a broadcast network, where all hosts are in the same broadcast domain and connected with each other through hubs or switches. Hubs and switches, which are the basic network connection devices, have limited forwarding functions.

- A hub is a physical layer device without the switching function, so it forwards the received packet to all ports except the inbound port of the packet.
- A switch is a link layer device which can forward a packet according to the MAC address of the packet. A switch builds a table of MAC addresses mapped to associated ports with that address and only sends a known MAC's traffic to one port. When the switch receives a broadcast packet or an unknown unicast packet whose MAC address is not included in the MAC address table of the switch, it will forward the packet to all the ports except the inbound port of the packet. The above scenarios could result in the following network problems.
- Large quantity of broadcast packets or unknown unicast packets may exist in a network, wasting network resources.
- A host in the network receives a lot of packets whose destination is not the host itself, causing potential serious security problems.
- Related to the point above, someone on a network can monitor broadcast packets and unicast packets and learn of other activities on the network. Then they can attempt to access other resources on the network, whether or not they are authorized to do this.

Isolating broadcast domains is the solution for the above problems. The traditional way is to use routers, which forward packets according to the destination IP address and does not forward broadcast packets in the link layer. However, routers are expensive and provide few ports, so they cannot split the network efficiently. Therefore, using routers to isolate broadcast domains has many limitations.

The Virtual Local Area Network (VLAN) technology is developed for switches to control broadcasts in LANs.

A VLAN can span multiple physical spaces. This enables hosts in a VLAN to be located in different physical locations. By creating VLANs in a physical LAN, you can divide the LAN into multiple logical LANs, each of which has a broadcast domain of its own. Hosts in the same VLAN communicate in the traditional Ethernet way. However, hosts in different VLANs cannot communicate with each other directly but need the help of network layer devices, such as routers and Layer 3 switches.

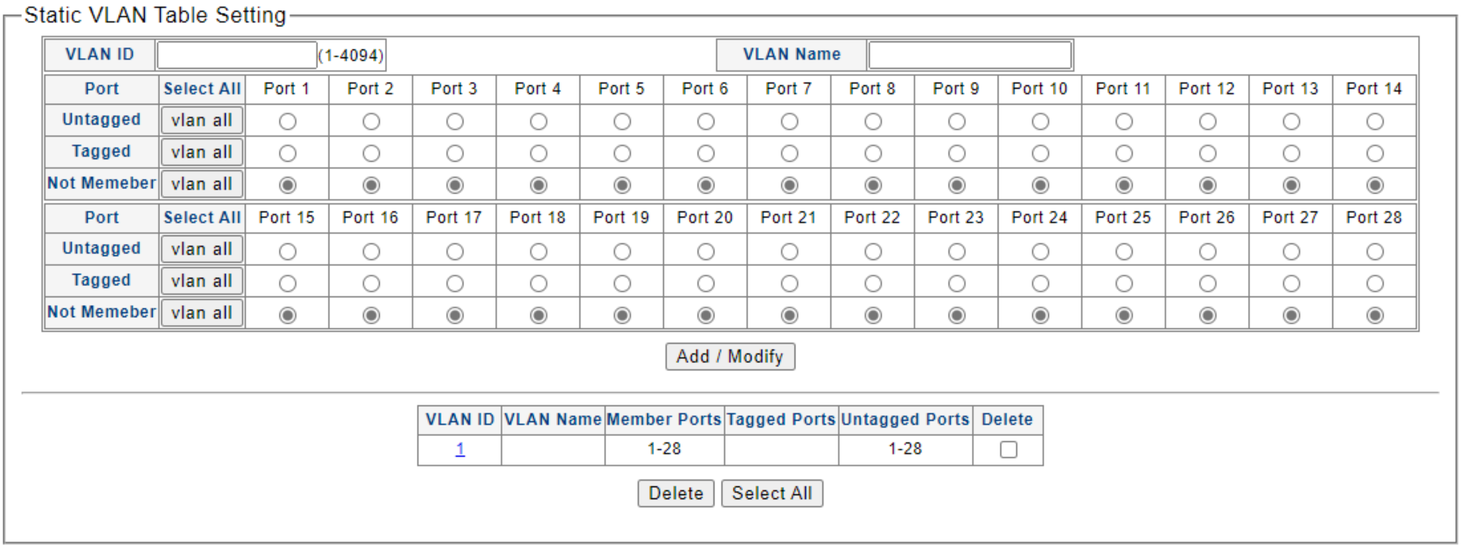
Advantages of VLANs

Compared with traditional Ethernet technology, VLAN technology delivers the following benefits:

- Confining broadcast traffic within individual VLANs. This saves bandwidth and improves network performance.
- Improving LAN security. By assigning user groups to different VLANs, you can isolate them at Layer 2. To enable communication between VLANs, routers or Layer 3 switches are required.
- Flexible virtual workgroup creation. As users from the same workgroup can be assigned to the same VLAN regardless of their physical locations, network construction and maintenance is much easier and more flexible.

5.1.1 Static VLAN (802.1Q VLAN) Configure

1. Choose the menu **Configuration →VLAN →Static VLAN** to load VLAN page.



Static VLAN Table Setting

VLAN ID (1-4094) VLAN Name

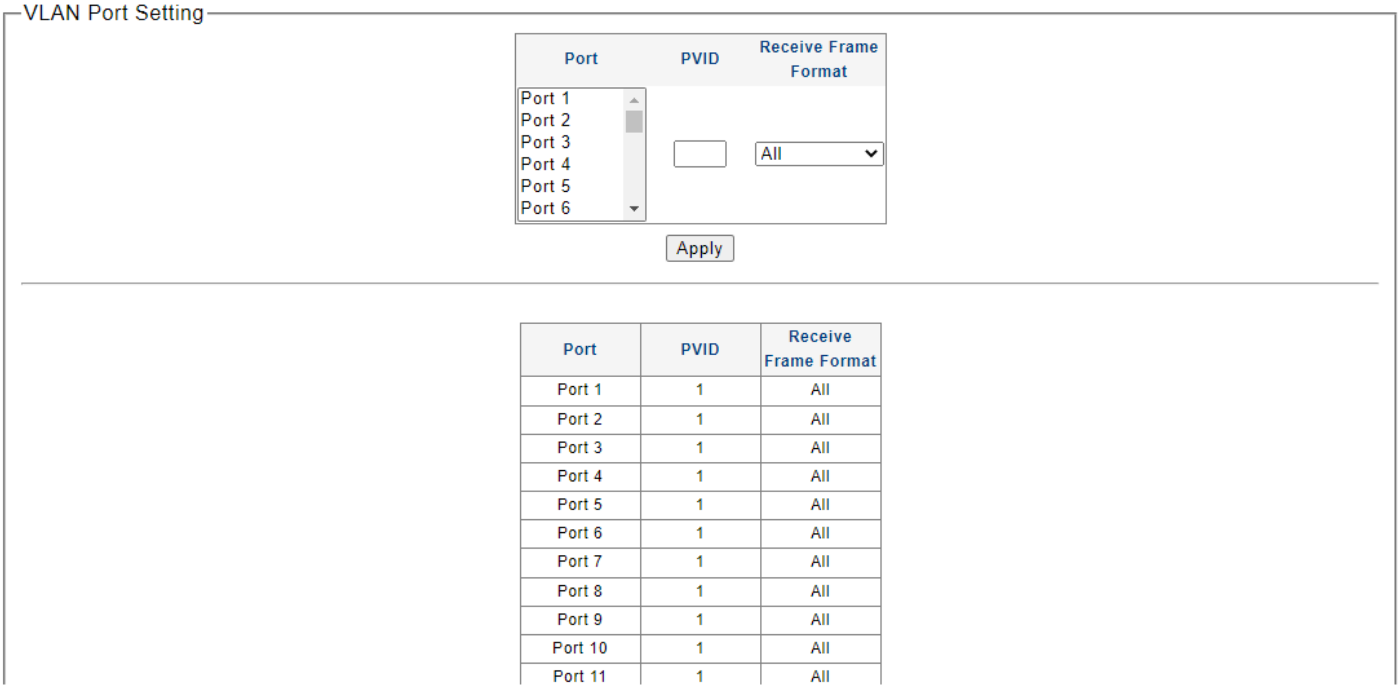
Port	Select All	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8	Port 9	Port 10	Port 11	Port 12	Port 13	Port 14
Untagged	vlan all	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Tagged	vlan all	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Memeber	vlan all	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Port	Select All	Port 15	Port 16	Port 17	Port 18	Port 19	Port 20	Port 21	Port 22	Port 23	Port 24	Port 25	Port 26	Port 27	Port 28
Untagged	vlan all	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Tagged	vlan all	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Memeber	vlan all	●	●	●	●	●	●	●	●	●	●	●	●	●	●

VLAN ID	VLAN Name	Member Ports	Tagged Ports	Untagged Ports	Delete
1		1-28		1-28	□

Figure 5-1-2

5.1.2 Port-base VLAN Configure

2. Choose the menu **Configuration →VLAN →802.1Q PVID** to load the following page.
   Configure PVID on this page.



VLAN Port Setting

Port	PVID	Receive Frame Format
Port 1 Port 2 Port 3 Port 4 Port 5 Port 6		All

Apply

Port	PVID	Receive Frame Format
Port 1	1	All
Port 2	1	All
Port 3	1	All
Port 4	1	All
Port 5	1	All
Port 6	1	All
Port 7	1	All
Port 8	1	All
Port 9	1	All
Port 10	1	All
Port 11	1	All

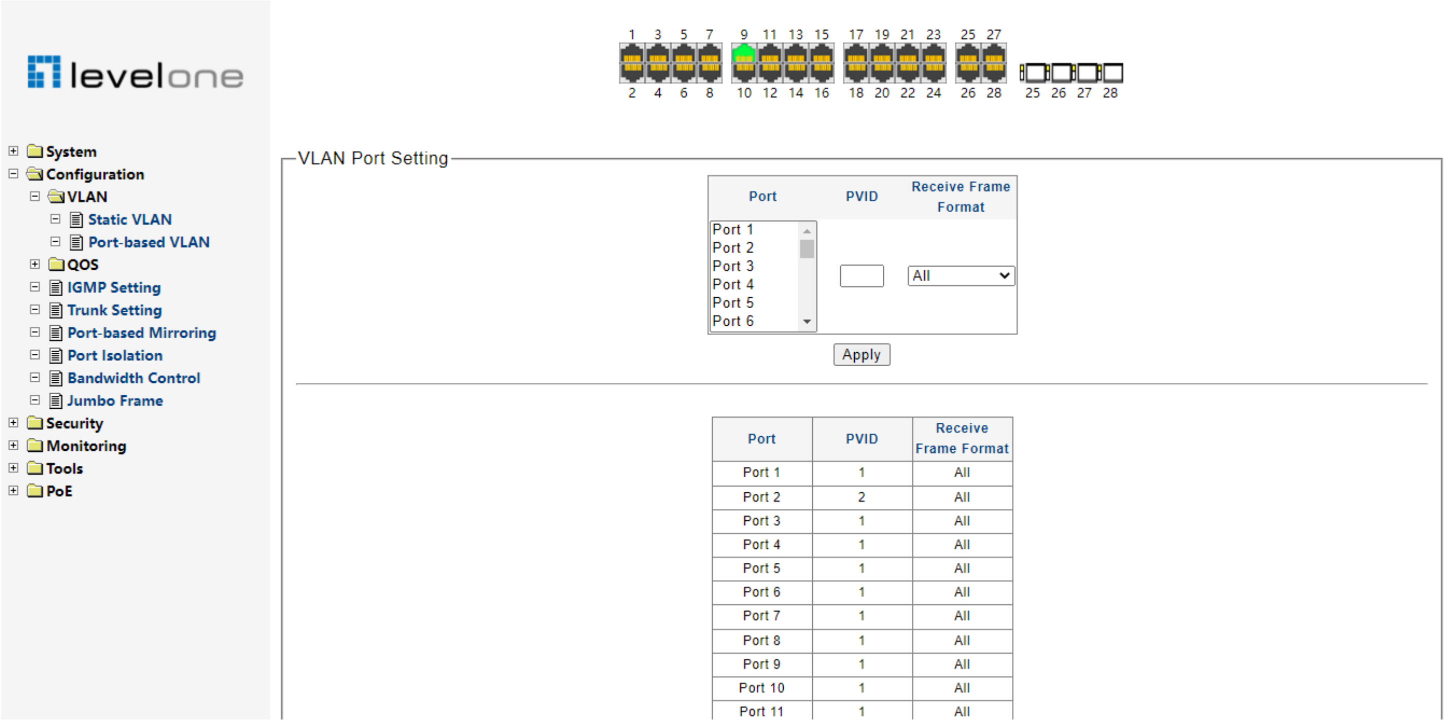
Figure 5-1-3

1). Select the desired port which to set PVID. Here is port 2 e.g.

2). Specify the PVID number of this port. Here is VLAN 2 e.g.

3). Select the frame type allowed of this port: ALL, Only with tag or Only no with tag.

4). Click Apply to change PVID of port 2.



VLAN Port Setting

Port	PVID	Receive Frame Format
Port 1 Port 2 Port 3 Port 4 Port 5 Port 6		All

Apply

Port	PVID	Receive Frame Format
Port 1	1	All
Port 2	2	All
Port 3	1	All
Port 4	1	All
Port 5	1	All
Port 6	1	All
Port 7	1	All
Port 8	1	All
Port 9	1	All
Port 10	1	All
Port 11	1	All

Figure 5-1-4

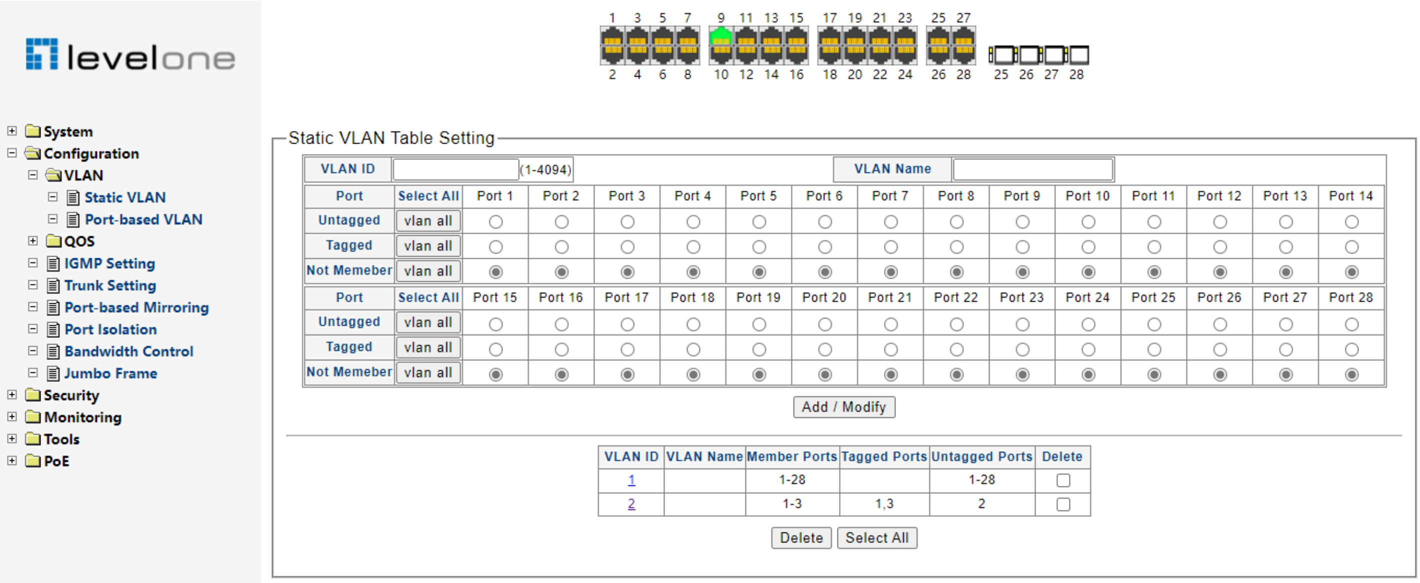
3. Choose the menu **Configuration →VLAN →802.1Q VLAN** to load the following page.
Configure 802.1Q VLAN member port on this page.

Here configure port 2 as access=2, port 1,3 as trunk =2 e.g.

1). Specify the VLAN ID need to configure. Here is VLAN 2 e.g.

2). Specify the VLAN Name of VLAN 2. Here is VLAN2.

3). Select the member port of VLAN 2, and frame type supported: Untagged or Tagged. Select port 2 as Untagged. Select port 1,3 as Tagged e.g.



Static VLAN Table Setting

VLAN ID (1-4094) VLAN Name

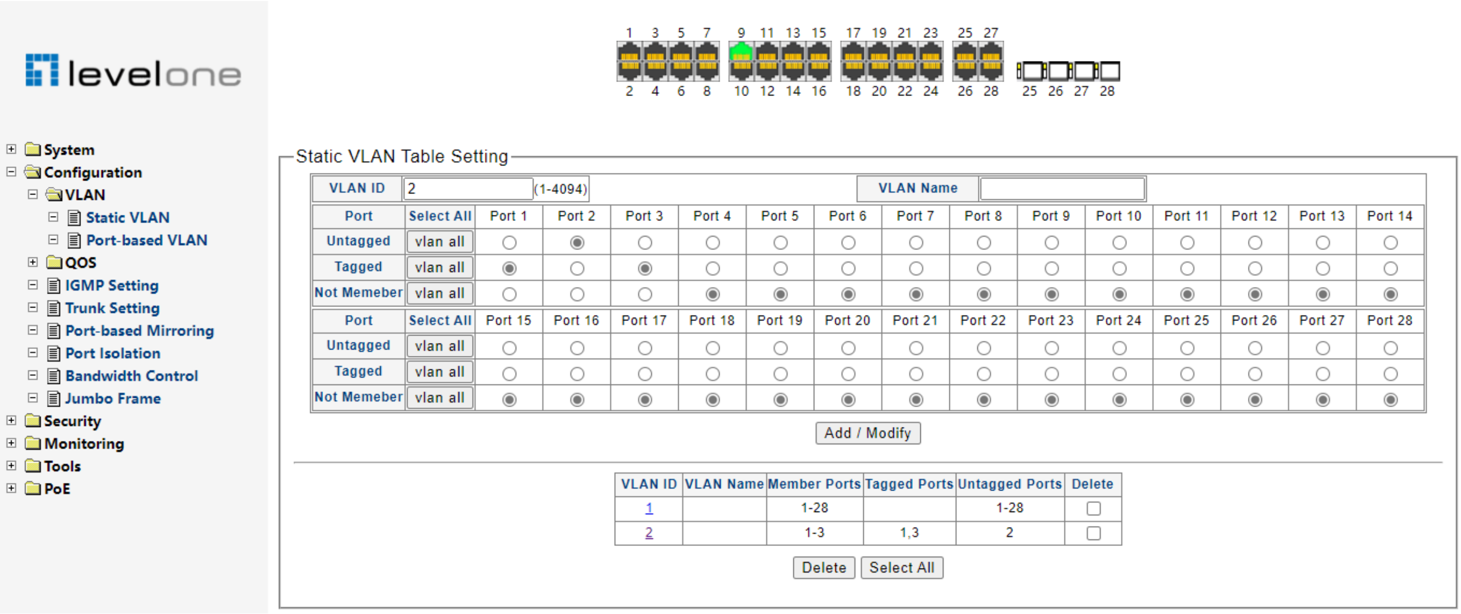
Port	Select All	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8	Port 9	Port 10	Port 11	Port 12	Port 13	Port 14
Untagged	vlan all	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Tagged	vlan all	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Memeber	vlan all	●	●	●	●	●	●	●	●	●	●	●	●	●	●

Port	Select All	Port 15	Port 16	Port 17	Port 18	Port 19	Port 20	Port 21	Port 22	Port 23	Port 24	Port 25	Port 26	Port 27	Port 28
Untagged	vlan all	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Tagged	vlan all	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Memeber	vlan all	●	●	●	●	●	●	●	●	●	●	●	●	●	●

VLAN ID	VLAN Name	Member Ports	Tagged Ports	Untagged Ports	Delete
1		1-28		1-28	□
2		1-3	1,3	2	□

Figure 5-1-5

4). Click vlan id 2 to see the detailed configuration parameters of vlan 2.



Static VLAN Table Setting

VLAN ID 2 (1-4094) VLAN Name

Port	Select All	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8	Port 9	Port 10	Port 11	Port 12	Port 13	Port 14
Untagged	vlan all	○	●	○	○	○	○	○	○	○	○	○	○	○	○
Tagged	vlan all	●	○	●	○	○	○	○	○	○	○	○	○	○	○
Not Memeber	vlan all	○	○	○	●	●	●	●	●	●	●	●	●	●	●

Port	Select All	Port 15	Port 16	Port 17	Port 18	Port 19	Port 20	Port 21	Port 22	Port 23	Port 24	Port 25	Port 26	Port 27	Port 28
Untagged	vlan all	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Tagged	vlan all	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Not Memeber	vlan all	●	●	●	●	●	●	●	●	●	●	●	●	●	●

VLAN ID	VLAN Name	Member Ports	Tagged Ports	Untagged Ports	Delete
1		1-28		1-28	□
2		1-3	1,3	2	□

Figure 5-1-6

5.2 QoS

QoS (Quality of Service) functions to provide different quality of service for various network applications and requirements and optimize the bandwidth resource distribution so as to provide a network service experience of a better quality.

QoS

This switch classifies the ingress packets, maps the packets to different priority queues and then forwards the packets according to specified scheduling algorithms to implement QoS function.

Traffic classification: Identifies packets conforming to certain characters according to certain rules.

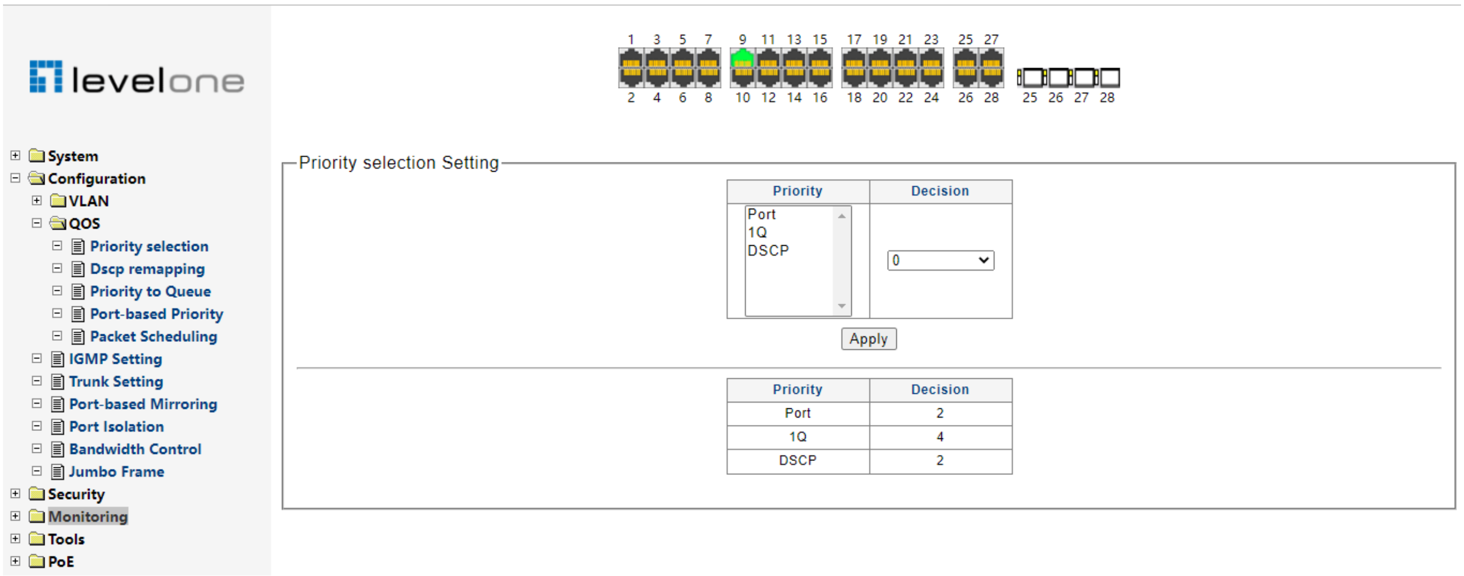
Map: The user can map the ingress packets to different priority queues based on the priority modes. This switch implements priority modes based on port.

Queue scheduling algorithm: When the network is congested, the problem that many packets compete for resources must be solved, usually in the way of queue scheduling. The switch supports three schedule modes: SP, WFQ,WRR

5.2.1 Priority selection Setting

This switch implements three priority modes based on port, on 802.1P and on DSCP. By default, it is based on port, 802.1P and DSCP priority modes.

Choose the menu **Configuration →Priority selection Setting** to load the following page.



Priority selection Setting

Priority	Decision
Port 1Q DSCP	0

Priority	Decision
Port	2
1Q	4
DSCP	2

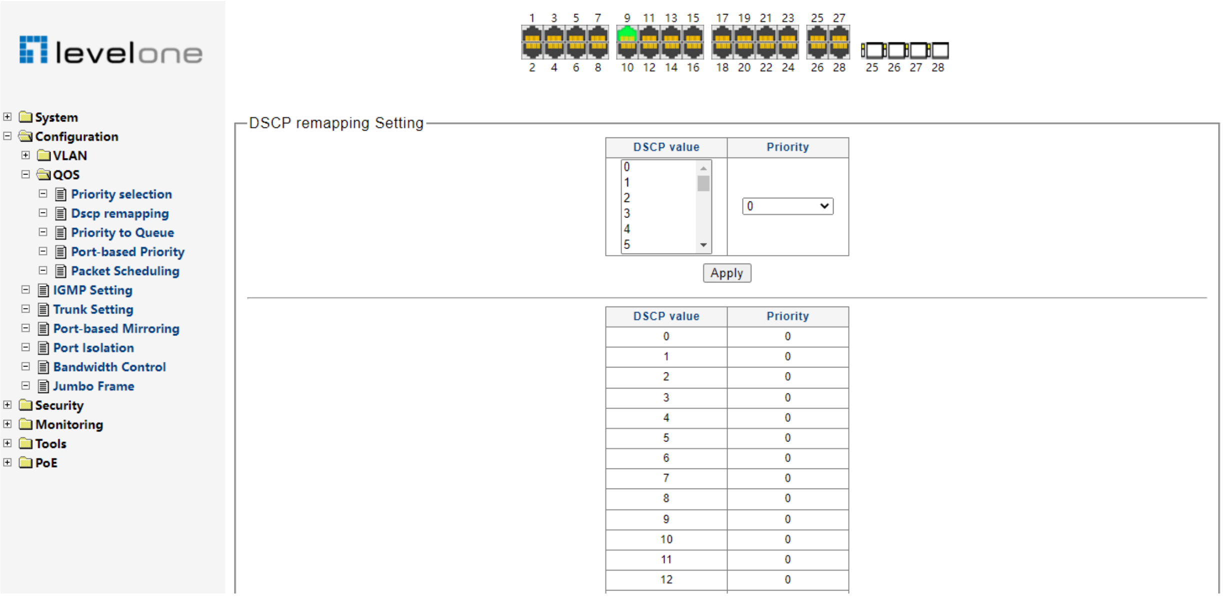
Figure 5-2-1

5.2.2 DSCP remapping

The device provides various types of priority maps. By looking through a priority map, the device decides which priority value to assign to a packet for subsequent packet processing.

You can configure the mapping relationship between dscp and priority.

Choose the menu **Configuration →QoS →DSCP Remapping** to load the following page.



DSCP remapping Setting

DSCP value	Priority
0 1 2 3 4 5	0

Apply

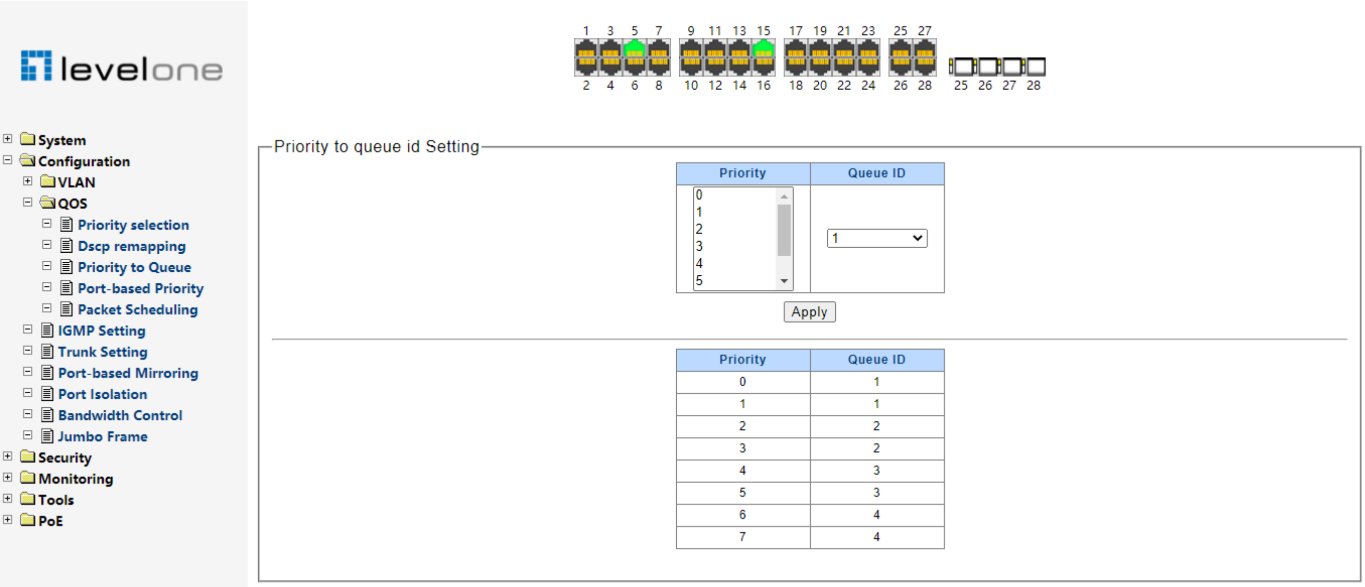
DSCP value	Priority
0	0
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0

Figure 5-2-2

5.2.3 Priority to Queue

The switch sends packets to the specified queue based on the mappings between local priorities and queues. Configuration of priority and queue mapping relationship.

Choose the menu **Configuration →QoS →Priority to Queue** to load the following page.



Priority to queue id Setting

Priority	Queue ID
0 1 2 3 4 5	1

Apply

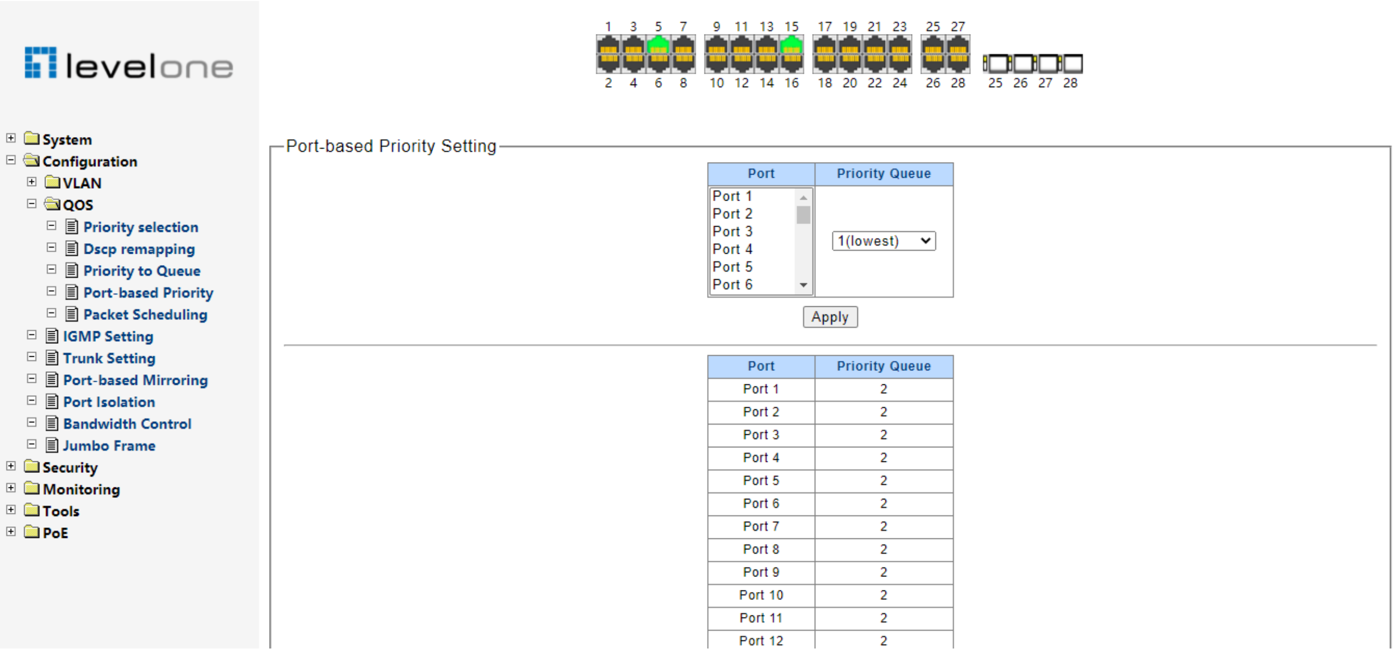
Priority	Queue ID
0	1
1	1
2	2
3	2
4	3
5	3
6	4
7	4

Figure 5-2-3

5.2.4 Port-based Priority

Port priority is a priority level of the port. After port priority is configured, the data stream will be mapped to the egress queues directly according to the priority level of the port.

Choose the menu **Configuration →QoS →Port-based Priority** to load the following page.



Port-based Priority Setting

Port	Priority Queue
Port 1 Port 2 Port 3 Port 4 Port 5 Port 6	1(lowest)

Port	Priority Queue
Port 1	2
Port 2	2
Port 3	2
Port 4	2
Port 5	2
Port 6	2
Port 7	2
Port 8	2
Port 9	2
Port 10	2
Port 11	2
Port 12	2

Figure 5-2-4

1. Displays the physical port number of the switch.
2. Select the desired port to configure its priority.
3. Specify the priority for the port.

5.2.5 Packet Scheduling

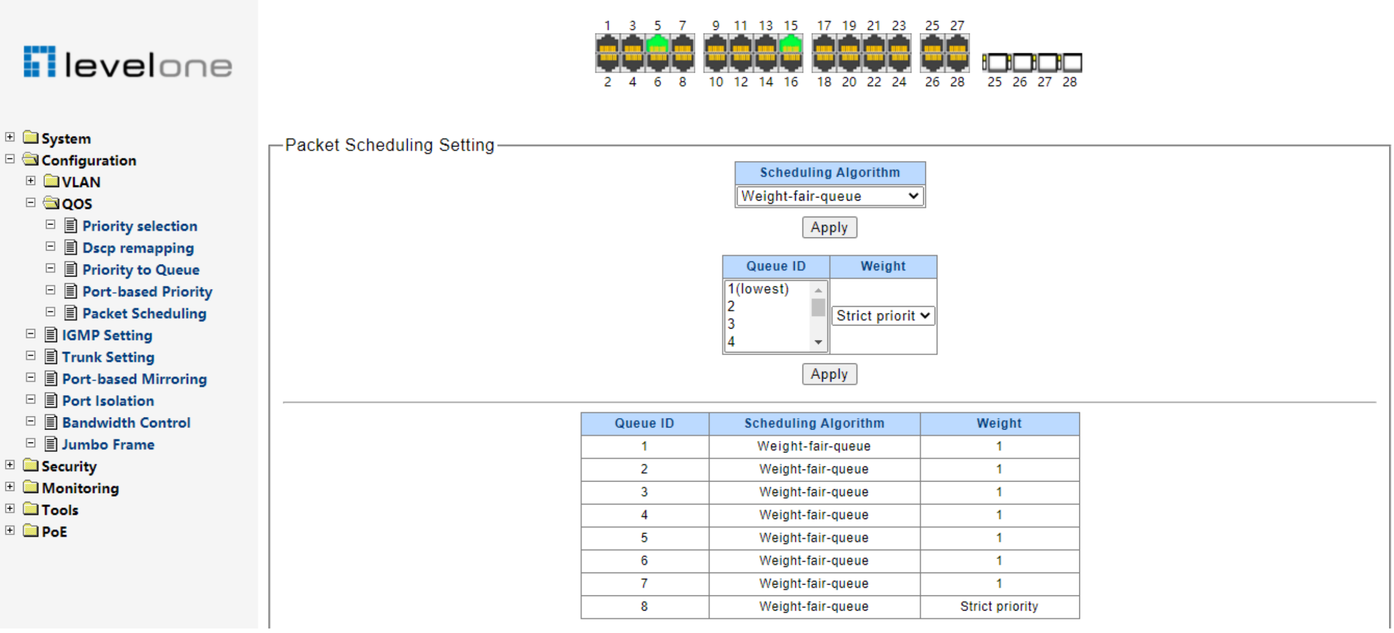
When the network is congested, the problem that many packets compete for resources must be solved, usually in the way of queue scheduling. The switch implements eight scheduling queues.

SP-Mode: Strict-Priority Mode. In this mode, the queue with higher priority will occupy the whole bandwidth. Packets in the queue with lower priority are sent only when the queue with higher priority is empty. The switch has four egress queues labeled. The disadvantage of SP queue is that: if there are packets in the queues with higher priority for a long time in congestion, the packets in the queues with lower priority will be “starved to death” because they are not served.

WFQ-Mode: Weighted fair queueing (WFQ) is a method of automatically smoothing out the flow of data in packet-switched communication networks by sorting packets to minimize the average latency and prevent exaggerated discrepancies between the transmission efficiency afforded to narrowband versus broadband signals. In WFQ, the priority given to network traffic is inversely proportional to the signal bandwidth. Thus, narrowband signals are passed along first, and broadband signals are buffered.

WRR-Mode: Weighted Round Robin (WRR) — In WRR mode the number of packets sent from the queue is proportional to the weight of the queue (the higher the weight the more frames are sent). WRR queuing schedules all the queues in turn to ensure that every queue is served for a certain time.

Choose the menu **Configuration →QoS →Packet Scheduling** to load the following page.



Packet Scheduling Setting

Scheduling Algorithm: Weight-fair-queue

Queue ID	Weight
1(lowest) 2 3 4	Strict priorit

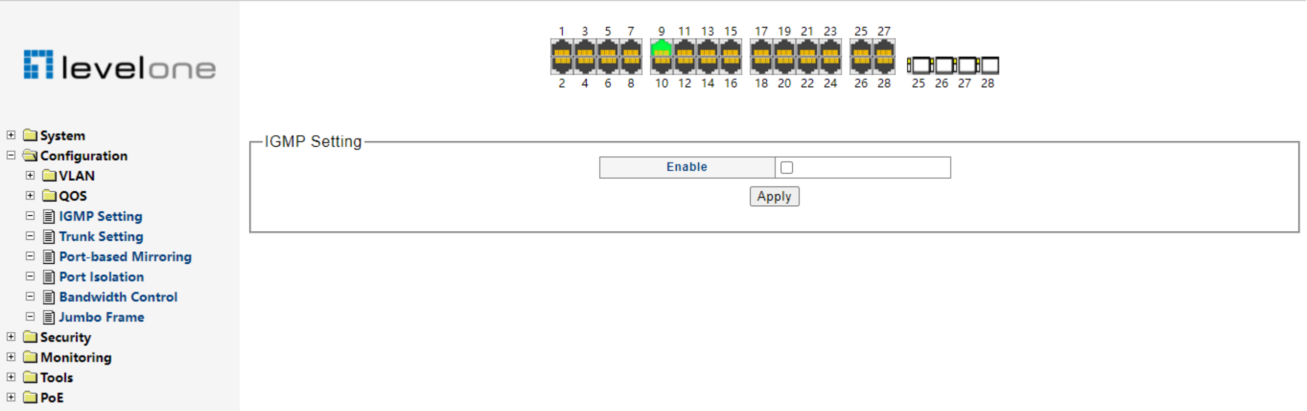
Queue ID	Scheduling Algorithm	Weight
1	Weight-fair-queue	1
2	Weight-fair-queue	1
3	Weight-fair-queue	1
4	Weight-fair-queue	1
5	Weight-fair-queue	1
6	Weight-fair-queue	1
7	Weight-fair-queue	1
8	Weight-fair-queue	Strict priority

Figure 5-2-5

5.3 IGMP Snooping

Internet Group Management Protocol Snooping (IGMP Snooping) is a multicast constraining mechanism that runs on Layer 2 devices to manage and control multicast groups.

The switch, running IGMP Snooping, listens to the IGMP messages transmitted between the host and the router, and tracks the IGMP messages and the registered port. When receiving IGMP report message, the switch adds the port to the multicast address table; when the switch listens to IGMP leave message from the host, the router sends the Group-Specific Query message of the port to check if other hosts need this multicast, if yes, the router will receive IGMP report message; if no, the router will receive no response from the hosts and the switch will remove the port from the multicast address table. The router regularly sends IGMP query messages. After receiving the IGMP query messages, the switch will remove the port from the multicast address table if the switch receives no IGMP report message from the host within a period of time.



IGMP Setting

Enable □

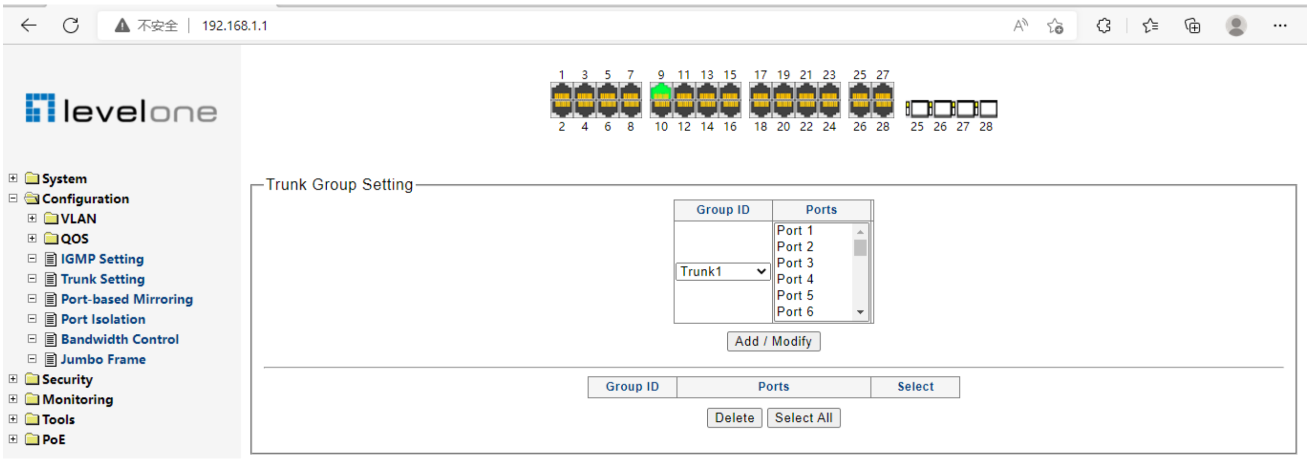
Figure 5-3-1

Unknown multicast data refers to multicast data for which no entries exist in the IGMP Snooping forwarding table. When the switch receives such multicast traffic:

- With the function of dropping unknown multicast data, the switch drops all the unknown multicast data received.
- With the function of forwarding unknown multicast data, the switch floods unknown multicast data in the VLAN which the unknown multicast data belongs to.

5.4 Link Aggregation

Link Aggregation is to combine a number of ports together to make a single high-bandwidth data path, so as to implement the traffic load sharing among the member ports in the group and to enhance the connection reliability.



Trunk Group Setting

Group ID	Ports
Trunk1	Port 1 Port 2 Port 3 Port 4 Port 5 Port 6

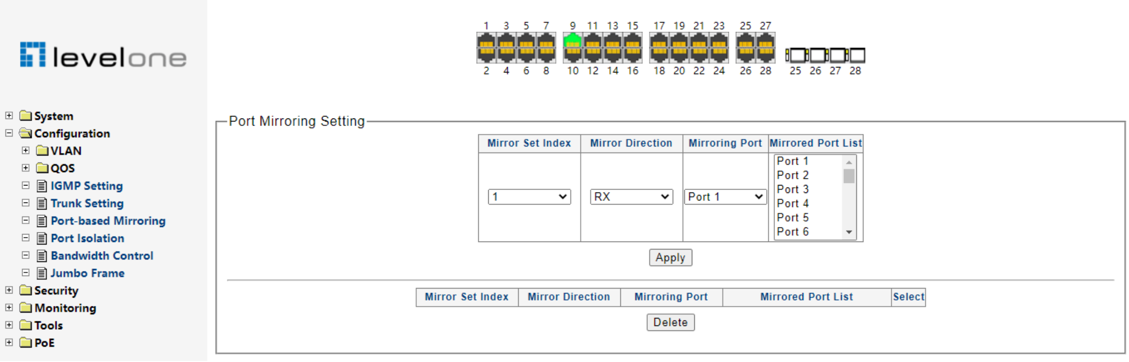
Group ID	Ports	Select

Figure 5-4-1

Select a aggregation group number, then add port in the left form to the right form, that make port join into aggregation group. Web-Smart Switch has max 8 groups, and one aggregation group can support max 8 member ports.

5.5 Port-based Mirroring

Port mirroring allows you to duplicate the packets passing specified ports to the destination mirroring port. As destination mirroring ports usually have data monitoring devices connected to them, you can analyze the packets duplicated to the destination mirroring port on these devices so as to monitor and troubleshoot the network.



Port Mirroring Setting

Mirror Set Index	Mirror Direction	Mirroring Port	Mirrored Port List
1	RX	Port 1	Port 1 Port 2 Port 3 Port 4 Port 5 Port 6

Mirror Set Index	Mirror Direction	Mirroring Port	Mirrored Port List	Select

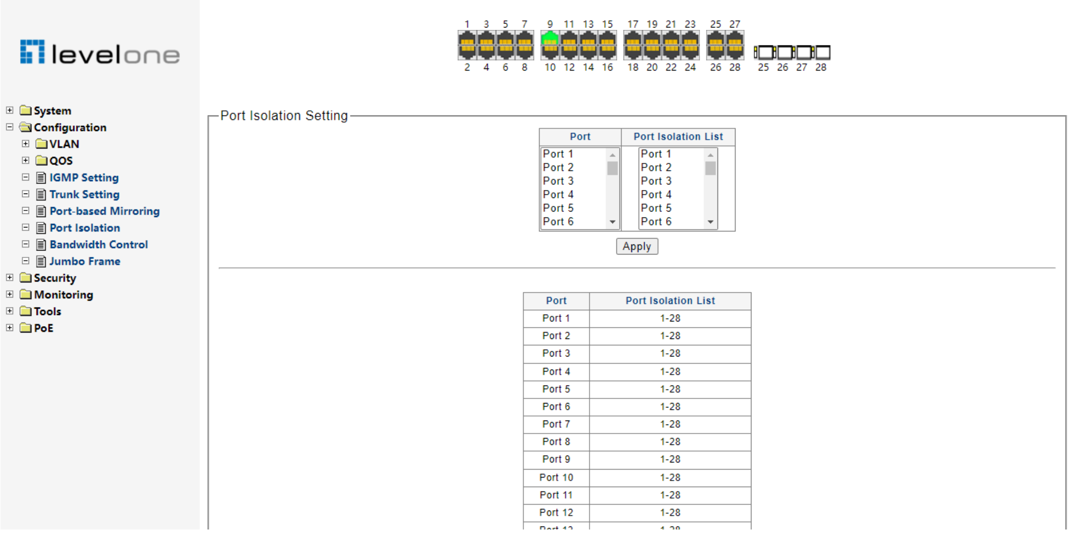
Figure 5-5-1

Choose the menu **Configuration→ Port-based Mirroring** to load the following page.
Select the Source Port from where you want to copy frames and the Target Port, which receives the copies from the source port.

1. Change the Port-base Mirroring Status menu to On.
2. Click Apply to let the changes take effect.
3. Select the Source Direction, RX, TX, Both.

5.6 Port Isolation

To implement isolation, you can add different ports to different VLANs. However, this will waste the limited VLAN resource. With port isolation, the ports can be isolated within the same VLAN. Thus, you need only to add the ports to the isolation group to implement isolation. This provides you with more secure and flexible networking schemes.
Choose the menu **Configuration→ Port Isolation** to load the following page.



Port Isolation Setting

Port	Port Isolation List
Port 1 Port 2 Port 3 Port 4 Port 5 Port 6	Port 1 Port 2 Port 3 Port 4 Port 5 Port 6

Port	Port Isolation List
Port 1	1-28
Port 2	1-28
Port 3	1-28
Port 4	1-28
Port 5	1-28
Port 6	1-28
Port 7	1-28
Port 8	1-28
Port 9	1-28
Port 10	1-28
Port 11	1-28
Port 12	1-28

Figure 5-6-1

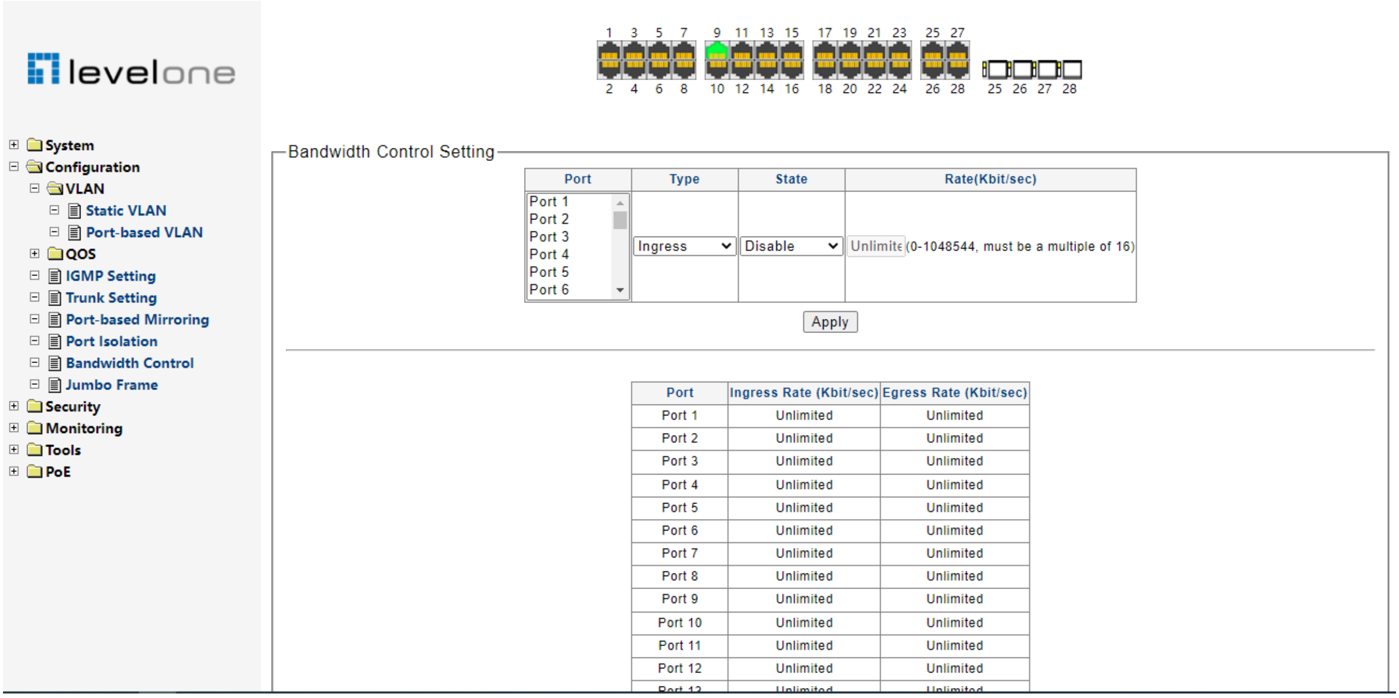
On the current device:

- Currently, each port can be configured on the device to forward data to other ports.

5.7 Bandwidth Control

Rate limit functions to control the ingress/egress traffic rate on each port via configuring the available bandwidth of each port. In this way, the network bandwidth can be reasonably distributed and utilized.

Choose the menu **Configuration→ Bandwidth Control** to load the following page.



Bandwidth Control Setting

Port	Type	State	Rate(Kbit/sec)
Port 1 Port 2 Port 3 Port 4 Port 5 Port 6	Ingress	Disable	Unlimite (0-1048544, must be a multiple of 16)

Port	Ingress Rate (Kbit/sec)	Egress Rate (Kbit/sec)
Port 1	Unlimited	Unlimited
Port 2	Unlimited	Unlimited
Port 3	Unlimited	Unlimited
Port 4	Unlimited	Unlimited
Port 5	Unlimited	Unlimited
Port 6	Unlimited	Unlimited
Port 7	Unlimited	Unlimited
Port 8	Unlimited	Unlimited
Port 9	Unlimited	Unlimited
Port 10	Unlimited	Unlimited
Port 11	Unlimited	Unlimited
Port 12	Unlimited	Unlimited
Port 13	Unlimited	Unlimited

Figure 5-7-1

If you select port to set ingress/egress rate, the system will automatically select integral multiple of 16Kbps that closest to the rate you entered as the real ingress/egress rate.

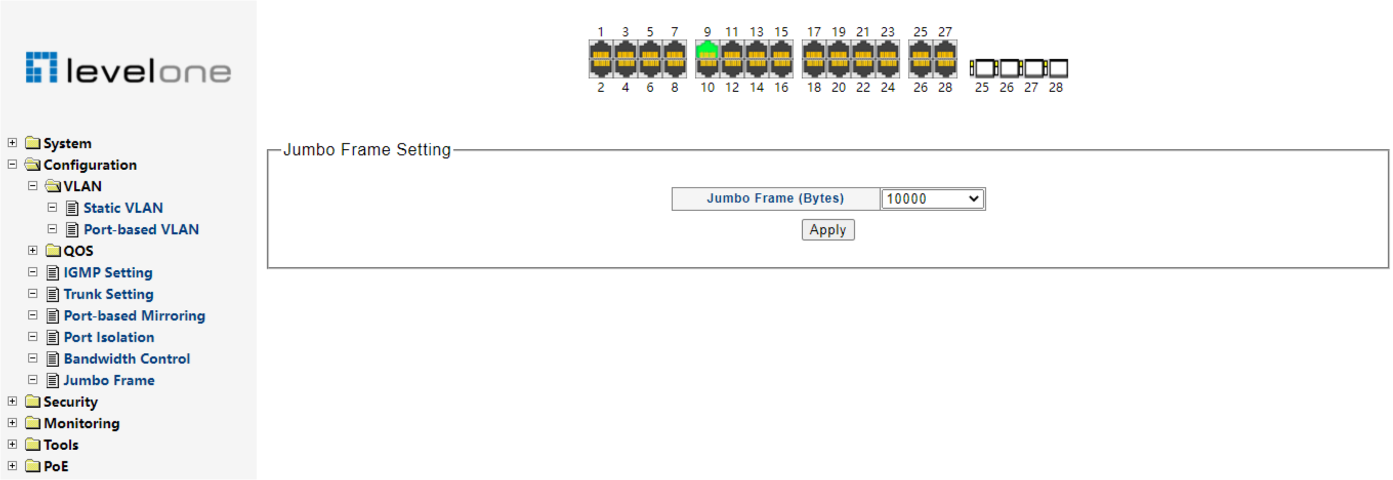
Ingress: Configure the bandwidth for receiving packets on the port. You can select a port to set Ingress rate, the system will automatically select integral multiple of 16Kbps that closest to the rate you entered as the real Ingress rate.

Egress: Configure the bandwidth for sending packets on the port. You can select a port to set Egress rate, the system will automatically select integral multiple of 16Kbps that closest to the rate you entered as the real Egress rate.

5.8 Jumbo Frame

Due to tremendous amount of traffic occurring in Ethernet, it is likely that some frames might have a frame size greater than the standard Ethernet frame size. By allowing such frames (called jumbo frames) to pass through Ethernet ports, you can forward frames with a size greater than the standard Ethernet frame size and yet still within the specified parameter range.

Choose the menu **Configuration→ Jumbo Frame** to load the following page.



Jumbo Frame Setting

Jumbo Frame (Bytes): 10000

Figure 5-8-1

you can set the length of jumbo frames that can pass through all the Ethernet ports.

By default, the device allows jumbo frames with the length of 1522/1536/1552/9216/10000 bytes to pass through all Ethernet ports.

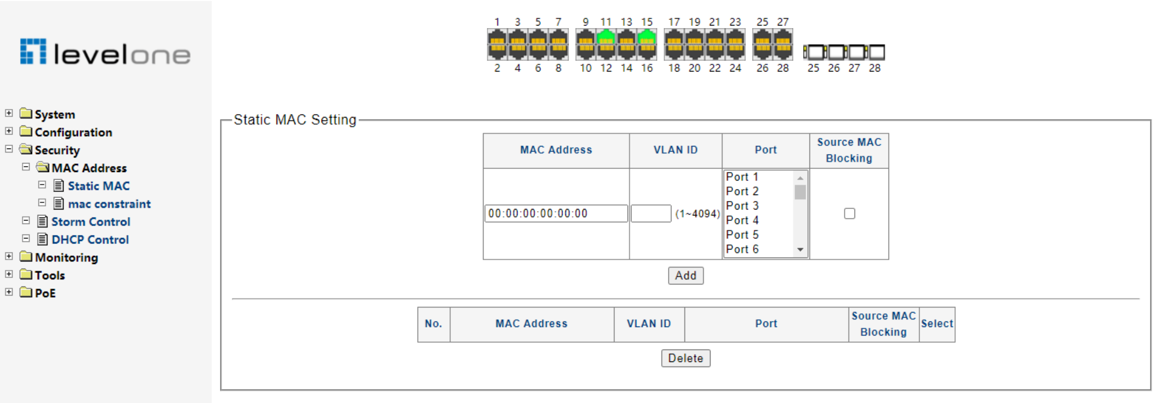
Chapter6: Security

6.1 MAC Address

A switch maintains a MAC address table for frame forwarding. Each entry in this table contains the MAC address of a connected device, to which port this device is connected and to which VLAN the port belongs.

6.1.1 Static MAC

A MAC address table consists of two types of entries: static and dynamic. Static entries are manually configured and never age out. Dynamic entries can be manually configured or dynamically learned and may age out.



Static MAC Setting

MAC Address	VLAN ID	Port	Source MAC Blocking
00:00:00:00:00:00	(1~4094)	Port 1 Port 2 Port 3 Port 4 Port 5 Port 6	☐

Add

No.	MAC Address	VLAN ID	Port	Source MAC Blocking	Select

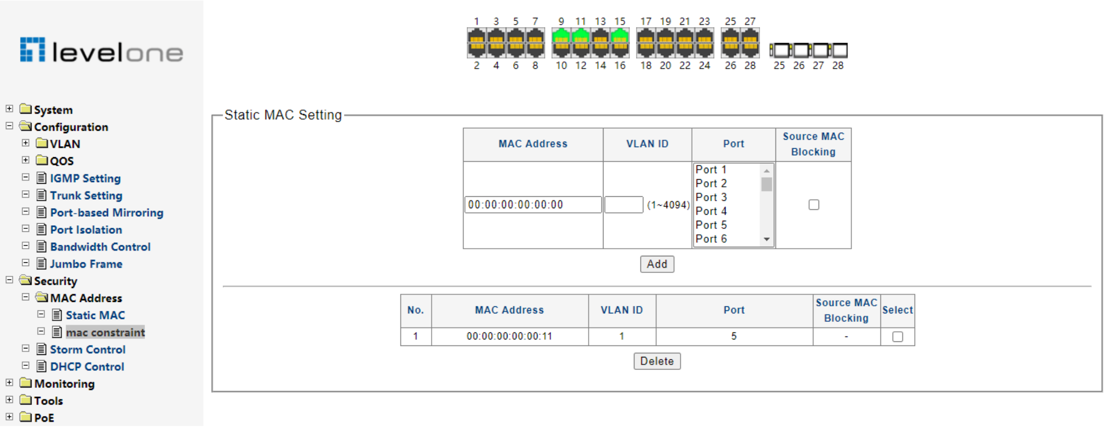
Delete

Figure 6-1-1

6.1.1.1 MAC Bingding

The static address table maintains the static address entries which can be added or removed manually. In the stable networks, the static MAC address entries can facilitate the switch to reduce broadcast packets and remarkably enhance the efficiency of packets forwarding without learning the address. The static MAC address learned by the port in the binding mode will be displayed in the Static Address Table.

Choose the menu **Configuration→ Security→ mac static** to load the following page.



Static MAC Setting

MAC Address	VLAN ID	Port	Source MAC Blocking
00:00:00:00:00:00	(1~4094)	Port 1 Port 2 Port 3 Port 4 Port 5 Port 6	☐

Add

No.	MAC Address	VLAN ID	Port	Source MAC Blocking	Select
1	00:00:00:00:00:11	1	5	-	☐

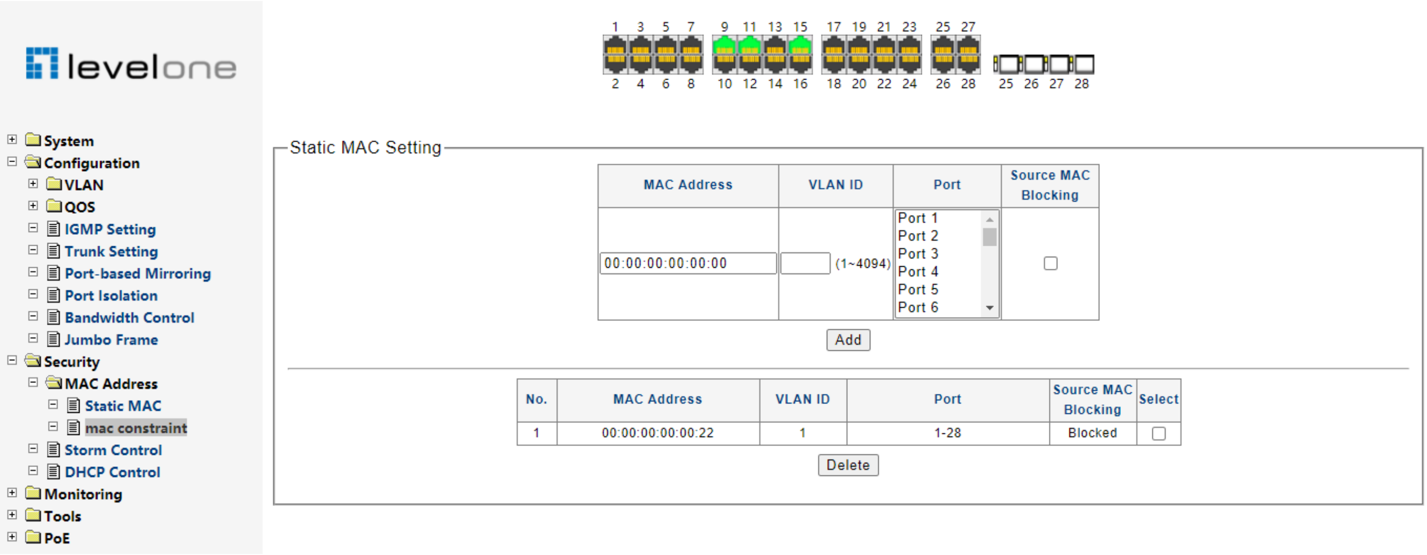
Delete

Figure 6-1-2

The above configuration means that mac 0000.0000.0011 is bound to port 5 and can only communicate with vlan1.
If you want the devices to be connected as planned, you can use this function. The mac can only be used on this port 5.

6.1.1.2 MAC Blocking

If the MAC address blocking table entry is set in this switch, if the message with this MAC address whether in source MAC or destination MAC, it will be discarded as long as the switch receives it.



Static MAC Setting

MAC Address	VLAN ID	Port	Source MAC Blocking
00:00:00:00:00:00	(1~4094)	Port 1 Port 2 Port 3 Port 4 Port 5 Port 6	□

Add

No.	MAC Address	VLAN ID	Port	Source MAC Blocking	Select
1	00:00:00:00:00:22	1	1-28	Blocked	□

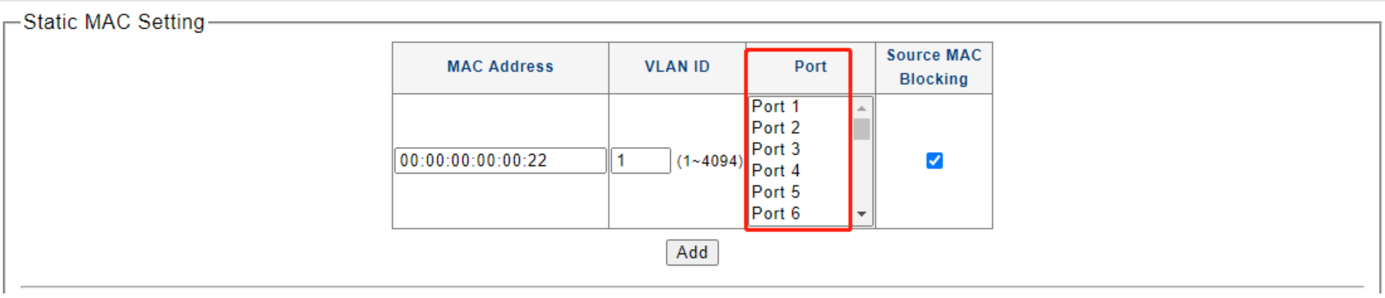
Delete

Figure 6-1-3

The above configuration indicates that mac 0000.0000.0022 is blocking in vlan1.

If it is found that the attack message is sent all the time with a certain MAC address, but the port from which the MAC is sent is unknown, you can do this.

Note: When configuring mac blocking, do not select the port number. All ports will be selected by default. E.g.



Static MAC Setting

MAC Address	VLAN ID	Port	Source MAC Blocking
00:00:00:00:00:22	1 (1~4094)	Port 1 Port 2 Port 3 Port 4 Port 5 Port 6	☑

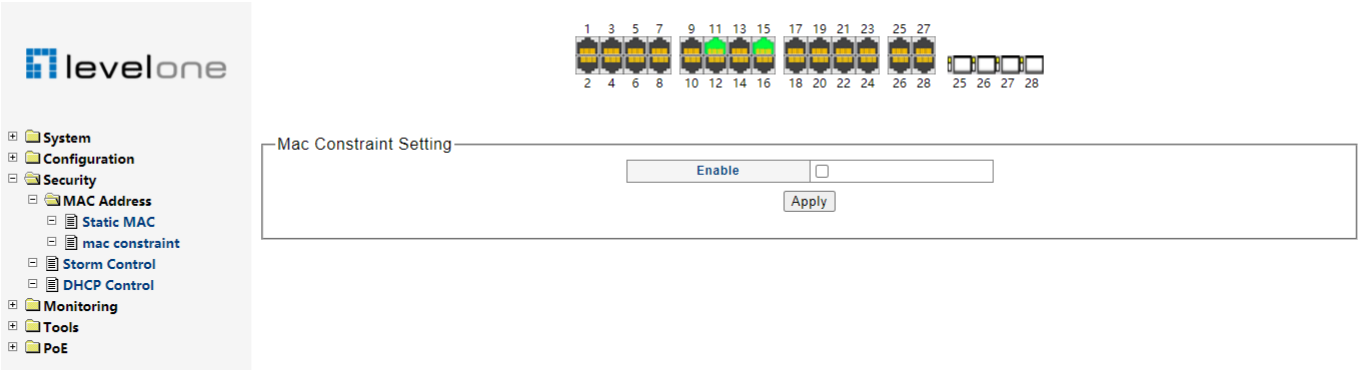
Add

Figure 6-1-4

6.1.2 MAC Constraint

MAC address learning capability, If this function is enabled, the switch will not learn the MAC address on the port.

Choose the menu **Configuration→MAC Constraint** to load the following page.



Mac Constraint Setting

Enable □

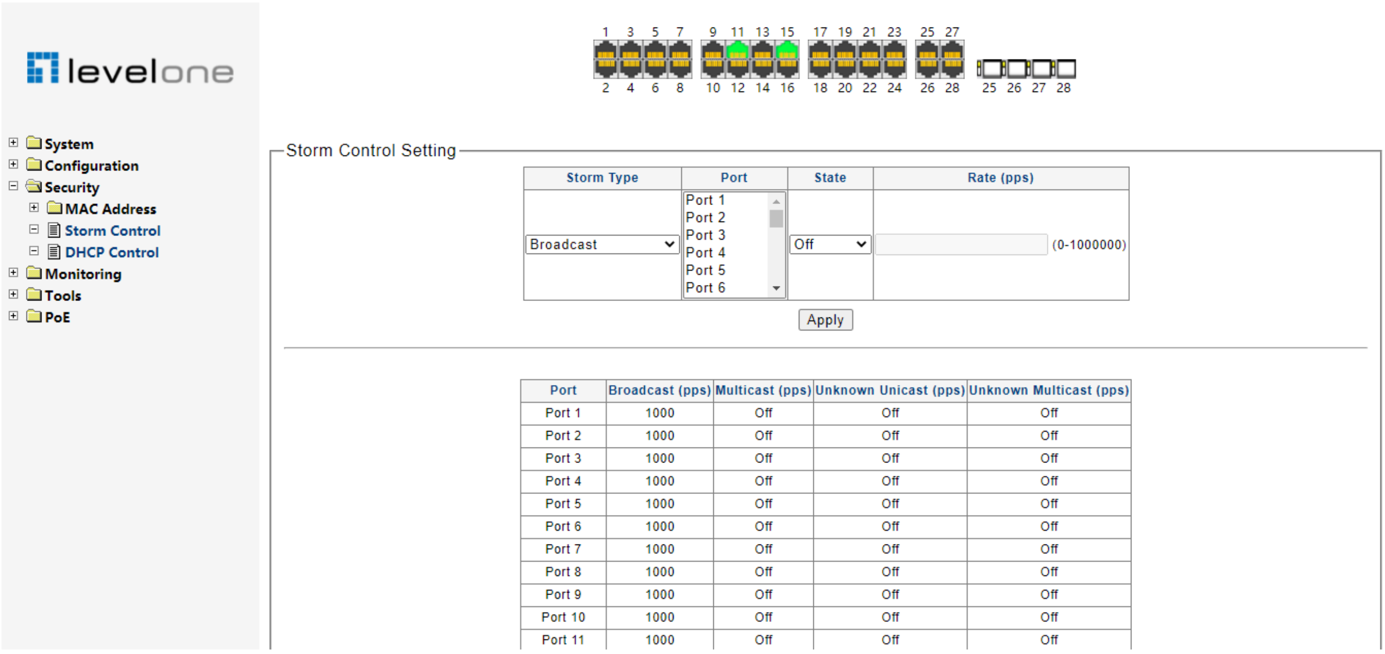
Apply

Figure 6-1-5

6.2 Storm Control Setting

Storm Control function allows the switch to filter Broadcast, Multicast and Unknown Unicast frame in the network. If the transmission rate of the three kind packets exceeds the set bandwidth, the packets will be automatically discarded to avoid network broadcast storm.

Choose the menu **Security→Storm Control** to load the following page.



Storm Control Setting

Storm Type	Port	State	Rate (pps)
Broadcast	Port 1 Port 2 Port 3 Port 4 Port 5 Port 6	Off	(0-1000000)

Apply

Port	Broadcast (pps)	Multicast (pps)	Unknown Unicast (pps)	Unknown Multicast (pps)
Port 1	1000	Off	Off	Off
Port 2	1000	Off	Off	Off
Port 3	1000	Off	Off	Off
Port 4	1000	Off	Off	Off
Port 5	1000	Off	Off	Off
Port 6	1000	Off	Off	Off
Port 7	1000	Off	Off	Off
Port 8	1000	Off	Off	Off
Port 9	1000	Off	Off	Off
Port 10	1000	Off	Off	Off
Port 11	1000	Off	Off	Off

Figure 6-2-1

Storm control is used to stop broadcast, multicast or ARP request storms that may result when a loop is created. The

Destination Look Up Failure control is a method of shutting down a loop when a storm is formed because a MAC address cannot be located in the Switch’s forwarding database and it must send a packet to all ports or all ports on a VLAN.

To configure Traffic Control, select the port, you want to configure. Broadcast Storm, Multicast Storm and Unknown Unicast may be Enabled or Disabled. The Threshold value is the upper threshold at which the specified traffic control is switched on. This is the number of Broadcast, Multicast or Unknown Unicast packets, in Kbps, received by the switch that will trigger the storm traffic control measures. The Threshold value can be set from 0 to100000Kbps.

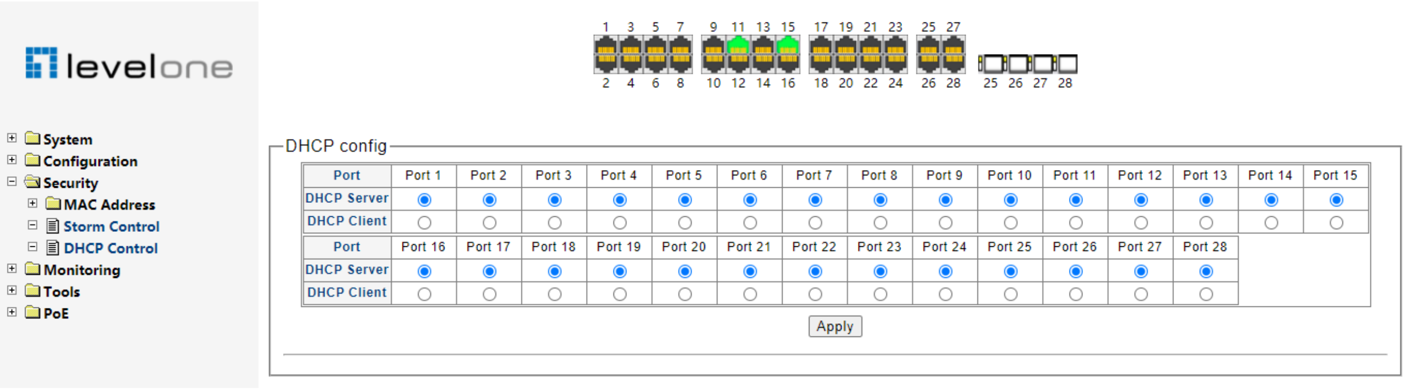
6.3 DHCP Snooping

Introduction to DHCP Snooping Trusted/Untrusted Ports
When an unauthorized DHCP server exists in the network, a DHCP client may obtains an illegal IP address. To ensure that the DHCP clients obtain IP addresses from valid DHCP servers, The switches can specify a port to be a trusted port or an untrusted port by the DHCP snooping function.

- Trusted: A trusted port is connected to an authorized DHCP server directly or indirectly. It forwards DHCP messages to guarantee that DHCP clients can obtain valid IP addresses.
- Untrusted: An untrusted port is connected to an unauthorized DHCP server. The DHCP-ACK or DHCP-OFFER packets received from the port are discarded, preventing DHCP clients from receiving invalid IP addresses.

Choose the menu **Security→ DHCP Snooping** to load the following page.

By default, all ports of the switch are trusted ports. When confirming which ports are not connected to the DHCP Server, these ports should be set as DHCP Client ports, that is untrusted ports.



DHCP config

Port	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8	Port 9	Port 10	Port 11	Port 12	Port 13	Port 14	Port 15
DHCP Server	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
DHCP Client	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Port	Port 16	Port 17	Port 18	Port 19	Port 20	Port 21	Port 22	Port 23	Port 24	Port 25	Port 26	Port 27	Port 28		
DHCP Server	●	●	●	●	●	●	●	●	●	●	●	●	●		
DHCP Client	○	○	○	○	○	○	○	○	○	○	○	○	○		

Figure 6-3-1

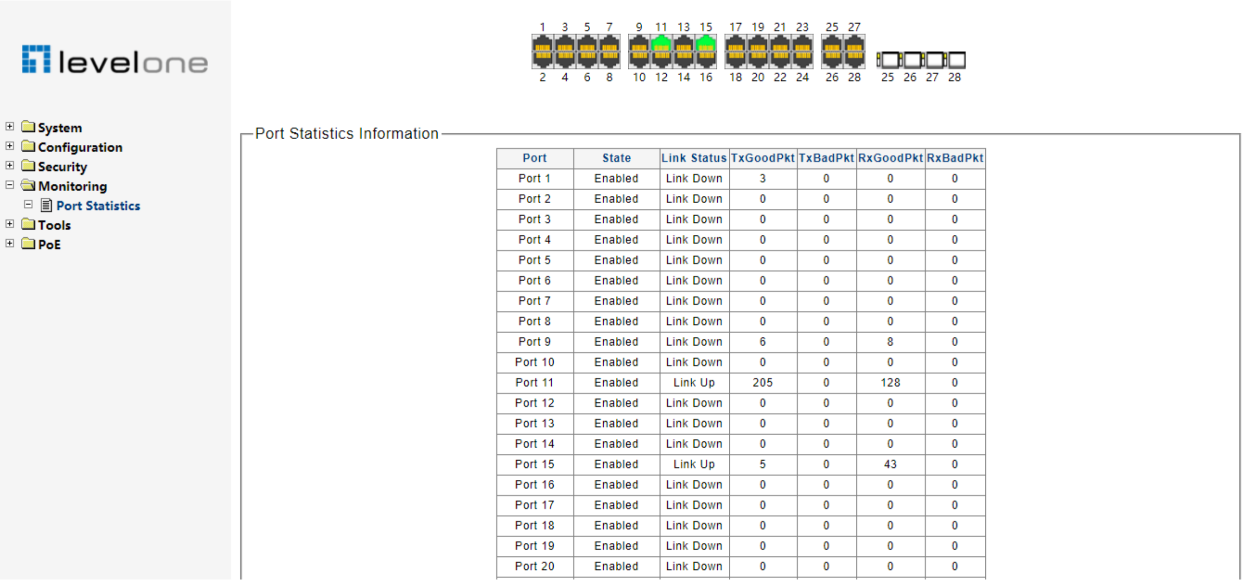
Chapter7: Monitoring

7.1 Port Statistics

The Traffic Monitor function, monitoring the traffic of each port, is implemented on the Traffic Summary and Traffic Statistics pages.

Traffic Summary screen displays the traffic information of each port, which facilitates you to monitor the traffic and analyze the network abnormity.

Choose the menu **Monitoring→ Port Statistics** to load the following page.



Port Statistics Information

Port	State	Link Status	TxGoodPkt	TxBadPkt	RxGoodPkt	RxBadPkt
Port 1	Enabled	Link Down	3	0	0	0
Port 2	Enabled	Link Down	0	0	0	0
Port 3	Enabled	Link Down	0	0	0	0
Port 4	Enabled	Link Down	0	0	0	0
Port 5	Enabled	Link Down	0	0	0	0
Port 6	Enabled	Link Down	0	0	0	0
Port 7	Enabled	Link Down	0	0	0	0
Port 8	Enabled	Link Down	0	0	0	0
Port 9	Enabled	Link Down	6	0	8	0
Port 10	Enabled	Link Down	0	0	0	0
Port 11	Enabled	Link Up	205	0	128	0
Port 12	Enabled	Link Down	0	0	0	0
Port 13	Enabled	Link Down	0	0	0	0
Port 14	Enabled	Link Down	0	0	0	0
Port 15	Enabled	Link Up	5	0	43	0
Port 16	Enabled	Link Down	0	0	0	0
Port 17	Enabled	Link Down	0	0	0	0
Port 18	Enabled	Link Down	0	0	0	0
Port 19	Enabled	Link Down	0	0	0	0
Port 20	Enabled	Link Down	0	0	0	0

Figure 7-1-1

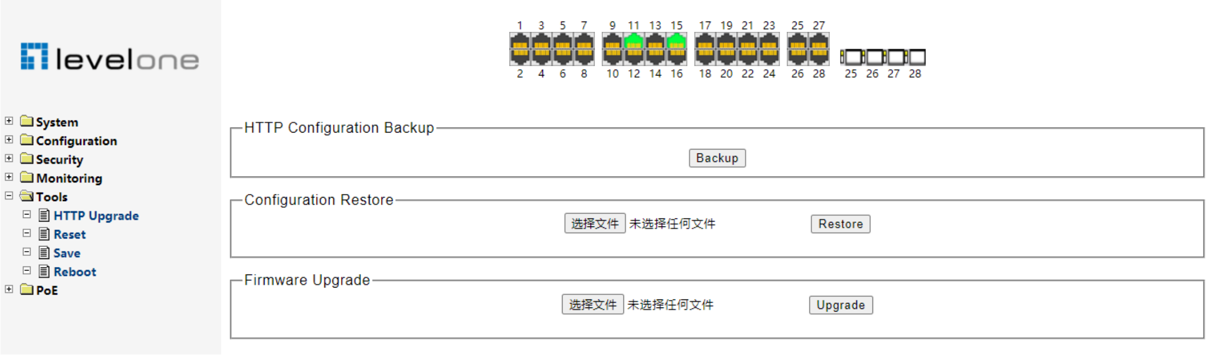
Chapter8: Tools

8.1 Backup Configuration

On this page you can download the current configuration and save it as a file to your computer for your future configuration restore.

On this page you can upload a backup configuration file to restore your switch to this previous configuration.

Choose the menu **Tools→ HTTP Upgrade** to load the following page.



HTTP Configuration Backup

Configuration Restore

Firmware Upgrade

Figure 8-1-1

Click the Backup button to save the current configuration as a file to your computer. You are suggested to take this measure before upgrading.

Click the Restore button to restore the backup configuration file. **Select "Configuration Restore", click "Select File"** button. It will take effect after the switch automatically reboots.

8.2 Fimware Upgrade

The switch system can be upgraded via the Web management page. To upgrade the system is to get more functions and better performance.

Choose the menu **Tools→HTTP Upgrade, Select "Firmware Upgrade" , click "Select File" button** to load the following page.

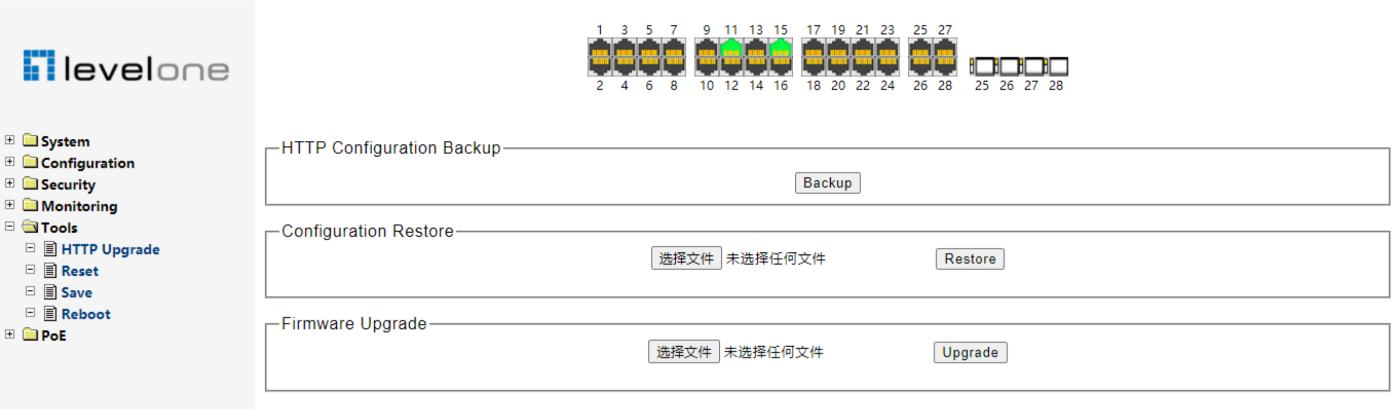


Figure 8-2-1

Don't interrupt the upgrade, to avoid damage, please don't turn off the device while upgrading.

8.3 Reboot

On this page you can reboot the switch and return to the login page. Please save the current configuration before rebooting to avoid losing the configuration unsaved

Choose the menu **Tools→ Reboot** to load the following page.

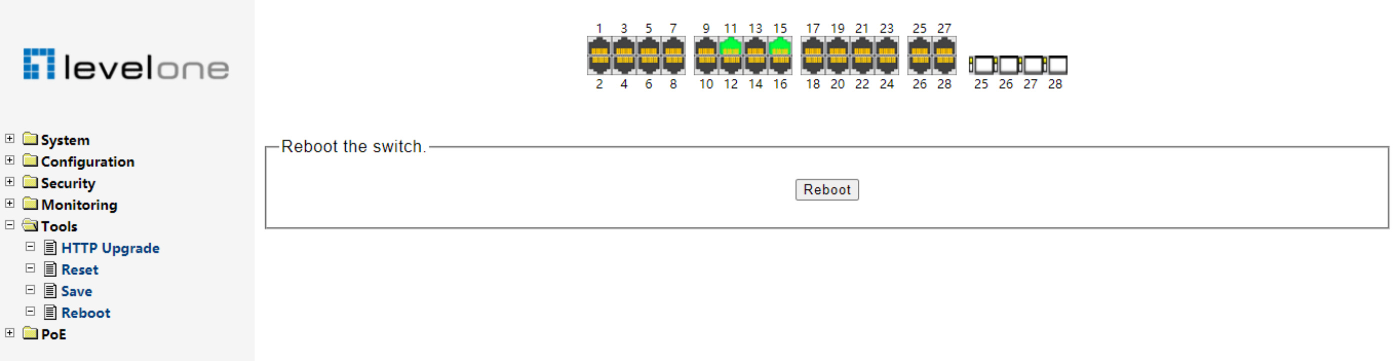
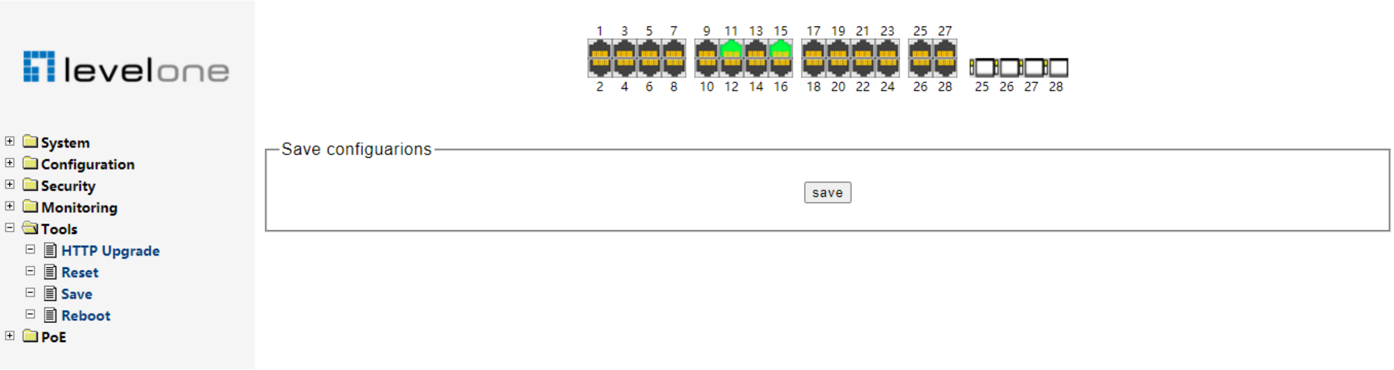


Figure 8-3-1

8.4 Save Configuration

When the switch is saved configuration, the settings will be immediately applied to the switching software in RAM, and will immediately take effect.

Choose the menu **Tools→ Save Configuration** to load the following page.



Save configuarions

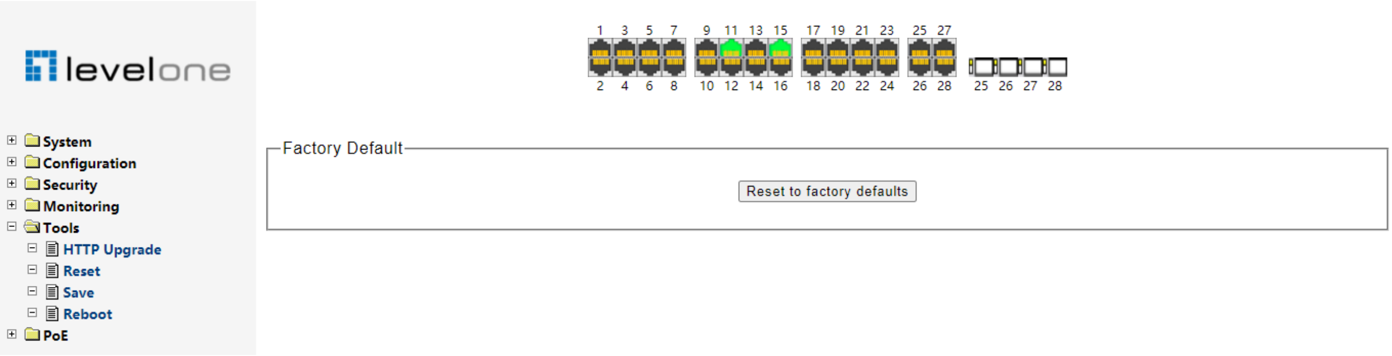
Figure 8-4-1

Click the save button, which can make parameters to be saved, your configuration will still work after restart.

8.5 Reset Factory Default

On this page you can reset the switch to the default. All the settings will be cleared after the switch is reset.

Choose the menu **Tools→ Reset Factory Default** to load the following page.



Factory Default

Figure 8-5-1

After the system is reset, the switch will be reset to the default and all the settings will be cleared.