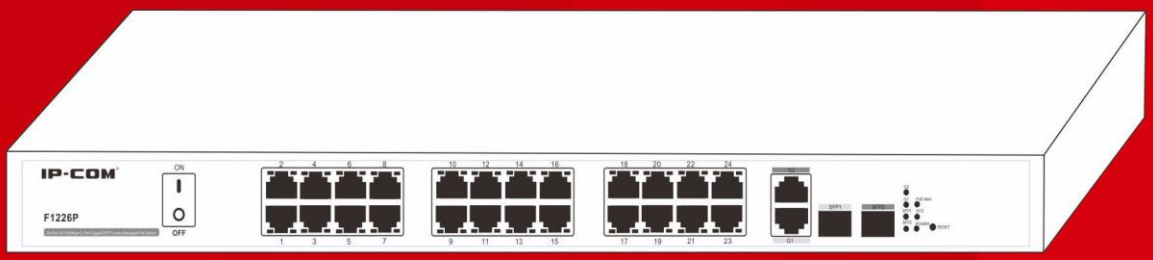
IP-COM®

User Guide



F1226P

24-Port 10/100Mbps+2-Port Gigabit/SFP Combo Managed PoE Switch

Copyright Statement

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, IP-COM reserves the right to make changes to the products described in this document without obligation to notify any person or organization of such revisions or changes. IP-COM does not assume any liability that may occur due to the use or application of the product or circuit layout(s) described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute the warranty of any kind, express or implied.

Technical Support

Website: http://www.ip-com.com.cn
Tel: (86 755) 2765 3089
Email: info@ip-com.com.cn

About This Manual

This IP-COM F1226P Manual describes how to install, configure, and operate the switch using its included web manager. This book describes the software configuration procedures and explains the options available within those procedures and safety guidelines. This document was created primarily for the system administrator who wishes to install and configure the F1226P in a network. This user guide assumes that the reader has a general understanding of switch platforms and a basic knowledge of Ethernet and networking concepts.

Safety Guidelines

Observe the following to avoid any potential harm caused from improper use.

- For your safety, DO NOT open the device's shell/outer case whether it is working or not;
- The device operates correctly only with a specified voltage range rating;
- Keep the device away from strong current or lightning, especially when connecting it to a power outlet using a power cord;
- To avoid potential short circuit and malfunction, DO NOT expose the device to humidity, heat, vibration or dust;
- Operate it in a well-ventilated working environment.

Contents

Chapter 1 Introduction

1.1 Product Overview

Thanks for purchasing this IP-COM Switch F1226P! The Switch is a state-of-the-art, high-performance, IEEE-compliant network solution designed for communities, businesses, system integrators and ISPs who require a large number of ports and want the power of Gigabit connectivity to eliminate bottlenecks, boost performance and increase productivity. The switch comes with 24 10/100Mbps ports and 2 Gigabit combo (SFP fiber/copper) ports, where fiber ports always take priority over copper ports. PoE optimizes the installation and management of network devices such as VoIP phones, wireless APs and IP-based surveillance cameras by requiring only a standard Cat 5 UTP cable to carry both power and data reducing installation time and cost. The switch connects up to 24 IEEE 802.3af-compliant devices (15.4W for each), or up to 12 high-power IEEE 802.3at-compliant devices (30W for each).

Plus, it also provides a complete package of enterprise-class features including VLAN, 802.1Q VLAN, QoS, SNMP, port mirroring and port aggregation, STP, PoE, etc. By default, the F1226P distributes power dynamically and each PoE capable port supplies power at IEEE802.3at standard.

1.2 Features

- Compliant with IEEE802.3, IEEE802.3u, IEEE802.3ab, IEEE802.3z, IEE802.3af, IEEE802.3at, IEEE802.1Q, IEEE802.1d, IEEE802.1w, IEEE802.3x
- 24 10/100Mbps and 2 10/100/1000Mbps ports with autosensing and auto-negotiation capabilities (auto-negotiation on duplex mode and speed)
- 2 Gigabit combo (SFP fiber/copper) ports, where fiber ports always take priority over copper ports
- Auto MDI/MDIX on all ports
- IEEE 802.3x flow control in full duplex and backpress flow control in half duplex
- 4K MAC address table with auto-learning and auto-aging capabilities
- Web based management
- Support DHCP client, VLAN, QoS, SNMP, port mirroring, port aggregation, IGMP Snooping, STP and PoE functions, etc.
- Internal high performance switching power supply; Power input: AC176-264V 50/60Hz

1.3 Physical Description

Front Panel

The front panel contains the following:

Power switch

RJ45 ports

Status LEDs

RESET button

PoE-MAX

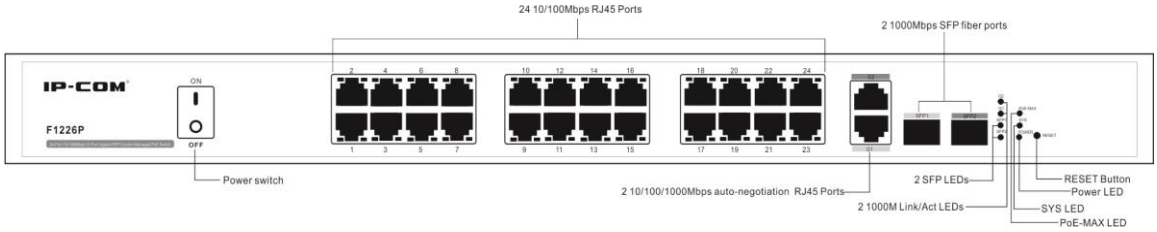


Figure 1 Switch Front Panel

1. RJ45 ports:

- 24 10/100Mbps and 2 10/100/1000Mbps ports with autosensing and auto-negotiation capabilities
- 2 1000Mbps SFP fiber ports

2. Status LEDs:

- Link/Act1~24: 24 10/100M port status LEDs
- PoE1~24: 24 PoE status LEDs
- G1~G2: 2 1000M Link/Act port status LEDs (Off when operating at 10/100M speed)
- SFP1~SFP2: 2 SFP fiber port LEDs
- Power: 1 Power LED
- SYS: 1 SYS LED
- PoE-MAX: PoE power usage threshold LED

The following table describes the LED designations.

LED	Color	Status	Designation
POWER	Green	Solid	Proper connection to power supply
		Off	Improper connection to power supply
SYS	Green	Solid / Off	System is operating improperly.
		Blinking	System is operating properly.
PoE-MAX	Green	Solid	Reaching max power budget and no more power available for another new PD
		Off	Power available for additional PDs
Link/Act1~24	Orange	Solid	Link is established on the port.
		Blinking	Packet transmission or reception is occurring on the port.
		Off	No link is established on the port.
PoE1~24	Green	Solid	The PoE powered device (PD) is connected and the port is supplying power successfully.
		Off	No PoE-powered device (PD) connected

G1~G2	Green (G1/G2 only lights up when operating at 1000M)	Solid	Link is established on the port.
		Blinking	Packet transmission or reception is occurring on the port.
		Off	No link is established on the port.
SFP1~SFP2	Green	Solid	Link is established or packet transmission is occurring on the port.
		Off	No link is established on the port.

3. Reset Button:

The **RESET** button located on the front panel of the switch can be used to restore switch back to factory default settings.

Press and hold it for over 5 seconds and then release, the SYS LED will first flash quickly for about 3 seconds and then regularly, which indicates switch has restarted automatically with factory default settings.

Note:

DO NOT press the **RESET** button unless you do want to delete current settings made on the switch and restore factory defaults.

Back Panel

The back panel contains the following:

- An AC power receptacle for accommodating the supplied power cord
- A grounding stud for lightning protection

Figure 2 Back Panel

1.4 Package Contents

Verify that the package contains the following:

- 1 Switch
- 4 Rubber Footpads (for tabletop installation)
- 1 Power Cord
- Rack-mount Kit (for installing the switch in a 19-inch rack)
- Install Guide

If any item is missing or damaged, contact the place of purchase immediately.

Chapter 2 Installation

2.1 Installation Considerations

To keep the switch in optimum working condition and prolong its life time, follow instructions below :

Please keep the switch in a dry and well ventilated environment.

For desktop installations, place the device on a flat table or shelf surface; for rack-mount installations, use a 19-inch (48.3-centimeter) EIA standard equipment rack that is grounded and physically secure. The rack-mount kit supplied with the switch is also required.

Do not restrict airflow by covering or obstructing air inlets of the switch. Keep more than 10 centimeters free on all sides for cooling. Be sure there is adequate airflow in the room or wiring closet where the switch is installed.

Don’t put heavy articles on the switch.

Verify there’s more than 1.5 centimeters vertical distance free between devices that overlap each other.

Ensure operating power supply accords with rated input standard.

2.2 Installing the Switch

The switch can be installed on a flat surface or in a standard 19-inch rack.

1. Installing the Switch on a Flat Surface

The switch ships with four self-adhesive rubber footpads. Stick one rubber footpad on each of the four concave spaces on the bottom of the switch to cushion the switch against shock/vibrations.

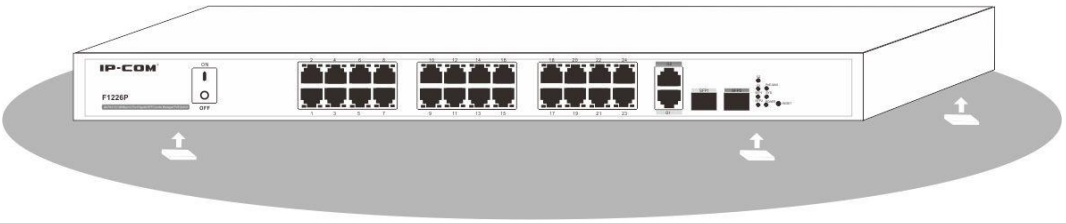


Figure 3: Attach Footpads to Switch

2. Installing the Switch in a Rack

To install the switch in a rack, use the following procedure (and refer to Figure 4). To perform this procedure, you need the 19-inch rack-mount kit supplied with switch.

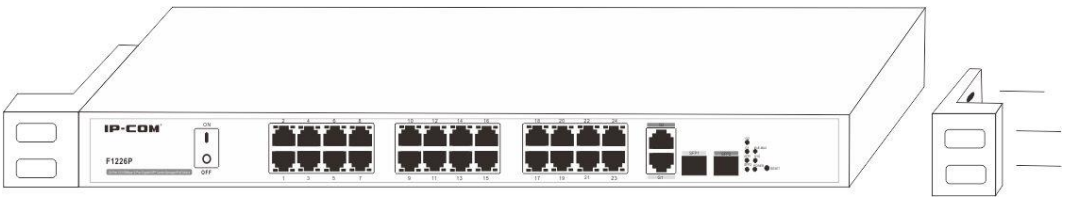


Figure 4: Attach Brackets to Switch

1). Make sure the 19-inch (48.3-centimeter) EIA standard equipment rack is well-grounded.

2). Attach the supplied mounting brackets to the side of the switch.

3). Insert the screws provided in the rack-mount kit through each bracket and into the bracket mounting holes in the switch.

4). Align the mounting holes in the brackets with the holes in the rack.

5). Tighten the screws with a screwdriver to secure each bracket.

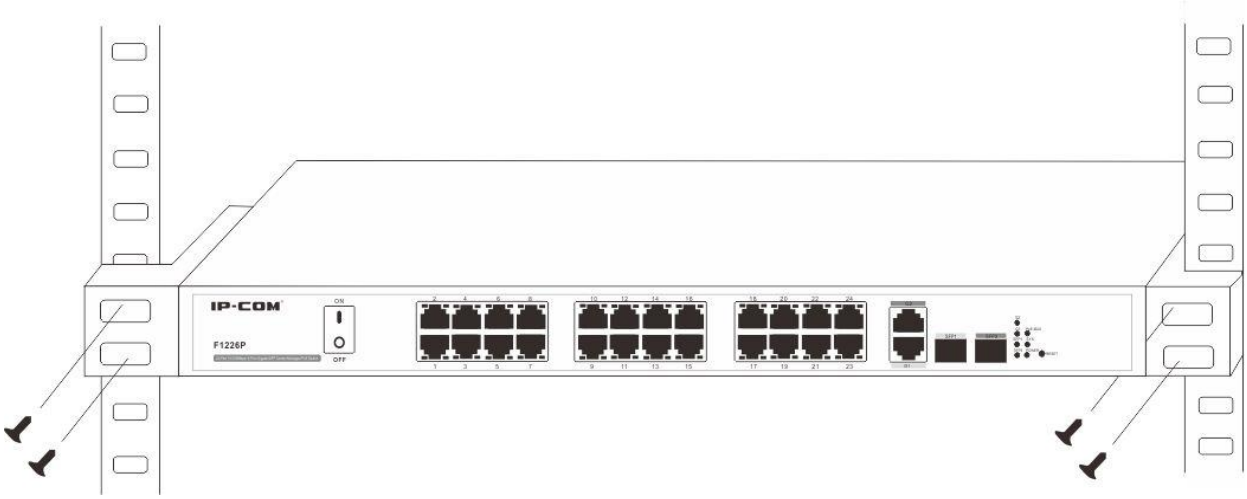


Figure 5 Install Switch in a 19-inch Rack

Note:

Always install devices from the bottom of the rack to the top. This will prevent the rack from over balancing and toppling over.

2.3 Hardware Connection

1. Applying AC Power

Make sure power source meets switch power specification: AC 100-240V 50/60Hz 6A.

a). Connect the female end of the supplied AC power adapter cable to the power receptacle on the back of the switch.

b). Connect the 3-pronged end of the AC power adapter cable to the 3-pronged AC source.

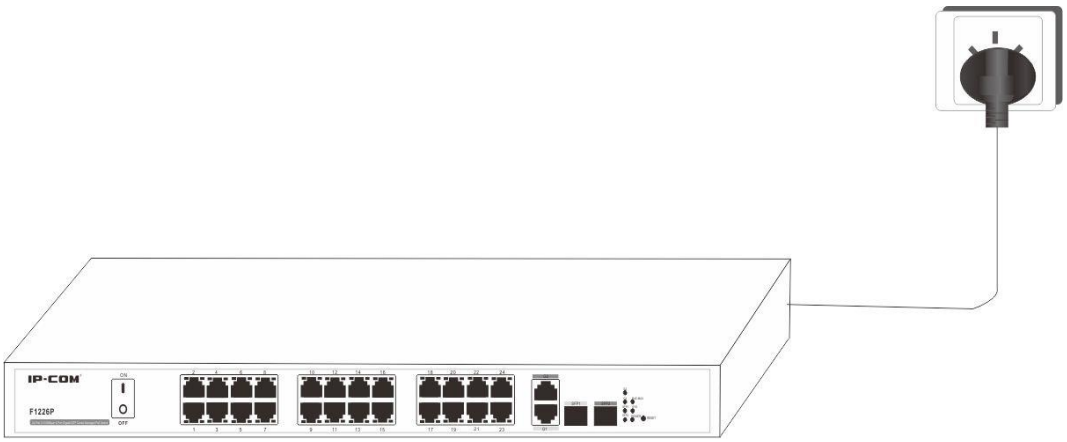


Figure 6: Connect Switch to Power Source

2. Connecting devices to the switch's RJ45 ports

Connect each PC to an RJ45 port on the switch's front panel (Figure 7) with an Ethernet cable.

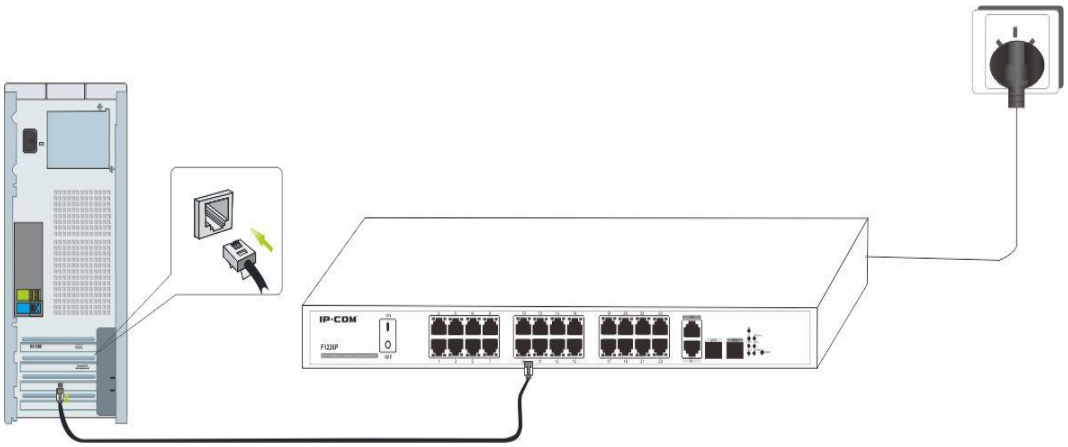


Figure 7: Connect PC to Switch's RJ45 Port

3. Connect PDs

Connect PDs (PoE powered devices, for example, 802.3at-/802.3af-compliant AP, IP telephone or IP camera) to the switch. Power is transmitted on conductors: 1, 2, 3 and 6.

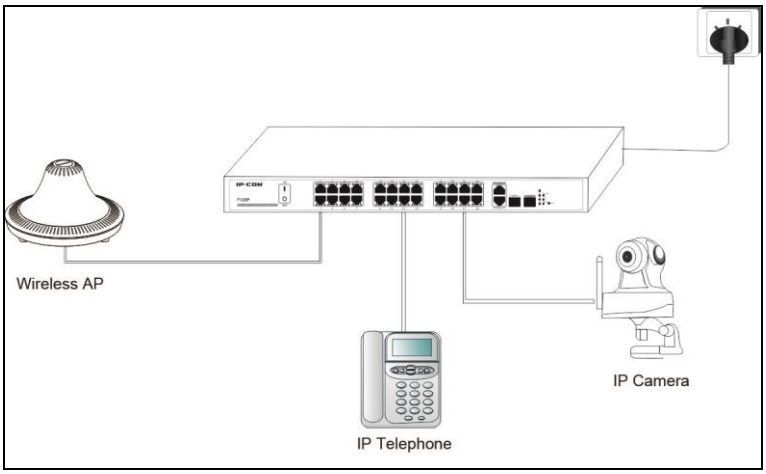


Figure 8: Connect PDs to Switch

Chapter 3 Configuration Guide

3.1 Getting Started with Switch Management Interface

3.1.1 System Requirements

This Switch provides a built-in browser interface that enables you to configure and manage it using a standard Web browser such as Microsoft Internet Explorer. The following hardware and software facilities are required to run the applications described in this manual:

• Network facilities:

– Ethernet network with or without DHCP server as appropriate

– Ethernet cable to connect the switch to a PC

• For Web Management:

Browser: Internet Explorer 8.0, Firefox 10.0 or higher

PC at an IP address of 192.168.0.xxx (Switch's default management IP is 192.168.0.1 and management VLAN is 1, which is unchangeable)

Installed NIC

OS software: Windows XP or higher version

3.1.2 Web Login

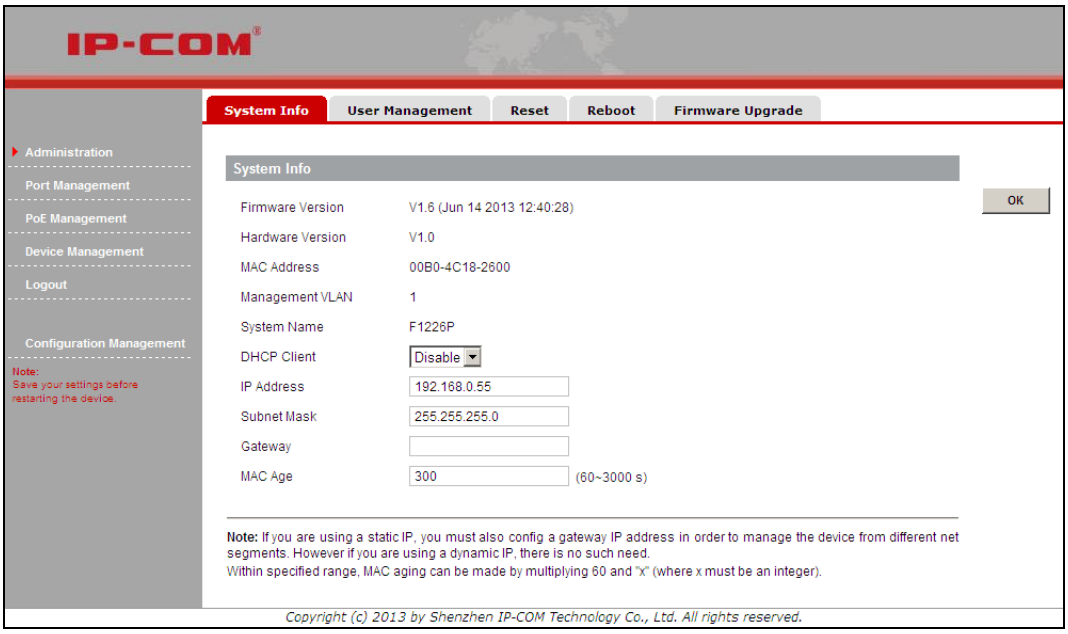
For first time login to switch's web manager, connect the switch only to a PC (recommended) instead of to other switches or routers to avoid possible IP conflict. Default parameters preset on the switch are listed below:

Parameter	Default
Default IP	192.168.0.1
Default User Name	admin
Default Password	admin

To log in to the switch's management interface with a manually configured IP address, do as follows:

1. Connect one RJ45 port on the switch to the PC's NIC port using an Ethernet cable.
2. Connect the switch to a nearby power outlet.
3. On your PC, manually configure an IP address: 192.168.0.X, where X represents any number between 2 and 254. For TCP/IP settings, see Chapter 5.
4. Run the Internet Explorer, enter the IP address: 192.168.0.1, and the Web manager's user authentication window pops up, as seen below:

Enter “admin” in both the User Name field and the Password field and click **Login**. This will open the Web-based user interface as seen below.



3.1.3 Introduction to the Web Browser Interface

This section introduces the Web browser interface that enables you to configure and manage your switch. The Menus and submenus on the web browser interface are described below:

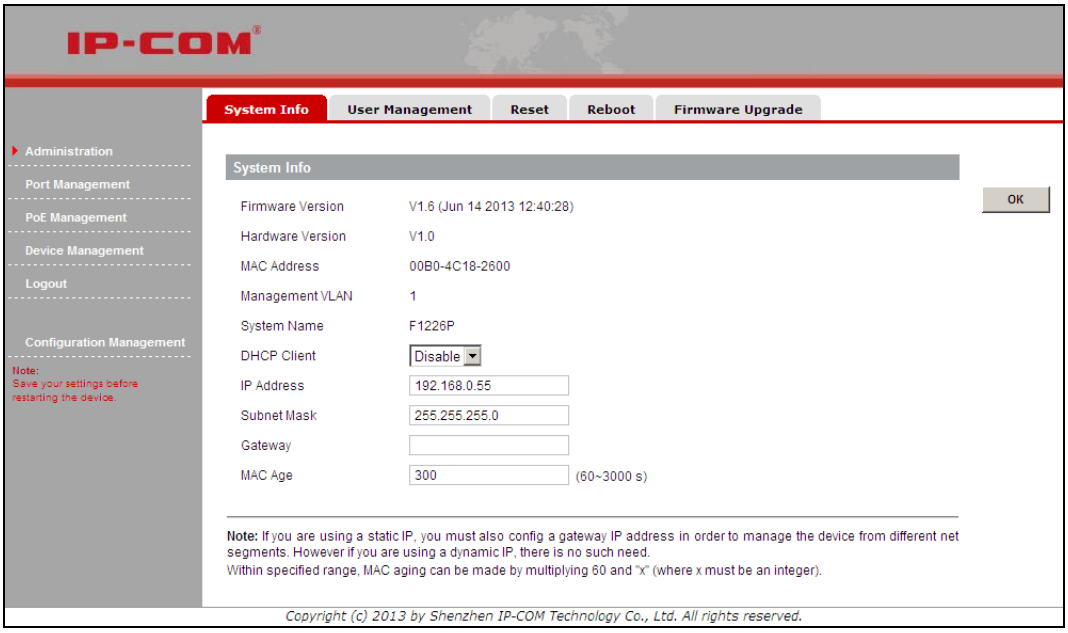
Menu	Submenu	Description
Administration	System Info	This section displays switch's system parameters; some fields such as IP address, subnet, MAC age, etc. are configurable. The switch supports cross-gateway management
	User Management	This section allows you to change user name and password.
	Reset	Restore all settings back to factory defaults.

	Reboot		Force device to restart. Configurations will be erased after Reboot. So please do save them before you restart the switch.
	Firmware Upgrade		Upgrade firmware.
	Port Management	Port Configuration	Display and allow you to config basic port parameters, such as link status, speed/duplex, MAC address learning, flow control (enabled by default) and broadcast storm control (enabled by default), etc.
		Port Mirroring	Display and allow you to config port mirroring settings. Aggregation enabled or STP enabled port cannot be configured as a mirroring destination port.
		Statistics	Display the number of packets transmitted and received on corresponding ports. Statistics info will be cleared automatically if statistic mode is changed.
		Rate Limit	Display and allow you to config port rate limit settings
		Link Aggregation	Provide 3 groups of aggregation and 4 algorithms to increase bandwidth and implement load balancing.
PoE Management	Global Settings		a).Configure power management mode (The default is Dynamic Allocation); b). View Current Power Utilization and PSE Temperature.
	Port Configuration		a). Configure PoE status, PoE standard, priority and static power allocation; b). View the amount of power supplied to connected PDs and PD class.
Device Management	VLAN	VLAN Mode Toggle	Change VLAN mode.
		Port VLAN	Display port VLAN configurations.
		802.1Q VLAN	Display 802.1Q VLAN configurations.
		Port Properties	Display and allow configuring PVID and tagging settings on the port.
	MAC		Configure MAC address binding feature
	QoS		Configure QoS settings
	STP	Global Settings	Configure STP global settings (enable/disable STP, STP version, system priority, Hello Time, delay, Max age time), loopback detection settings (enable/disable

			loopback detection, Auto-Wakeup and Wakeup Time Interval)
		Port Configuration	Configure priority and path cost settings for each port; Display port role and status in spanning tree.
	IGSP		Configure IGMP snooping settings.
	SNMP	SNMP Configuration	Configure SNMP status, community name and read/write settings.
		Trap Configuration	Enable/disable Trap and configure Trap destination host IP address.
Logout			Exit from switch's Web manager.
Configuration Management			Save/backup/restore settings.

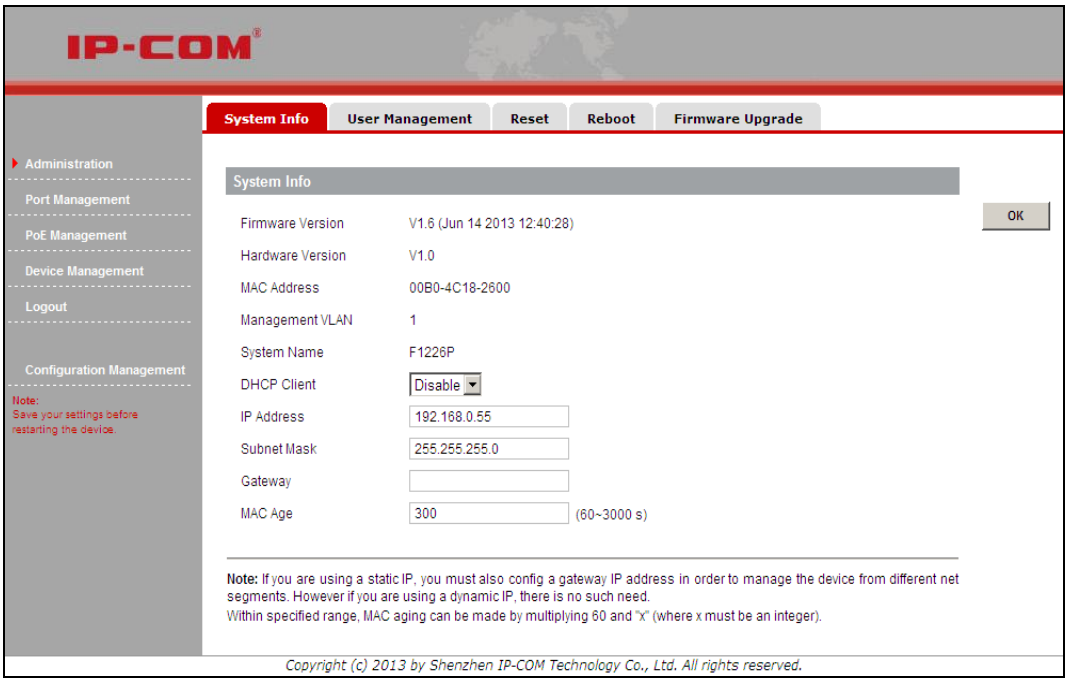
3.2 Administration

This section describes configuring and managing maintenance options in the switch as seen in the screenshot below:



3.2.1 System Info

The System Info screen contains parameters for configuring or displaying general device information as seen below:



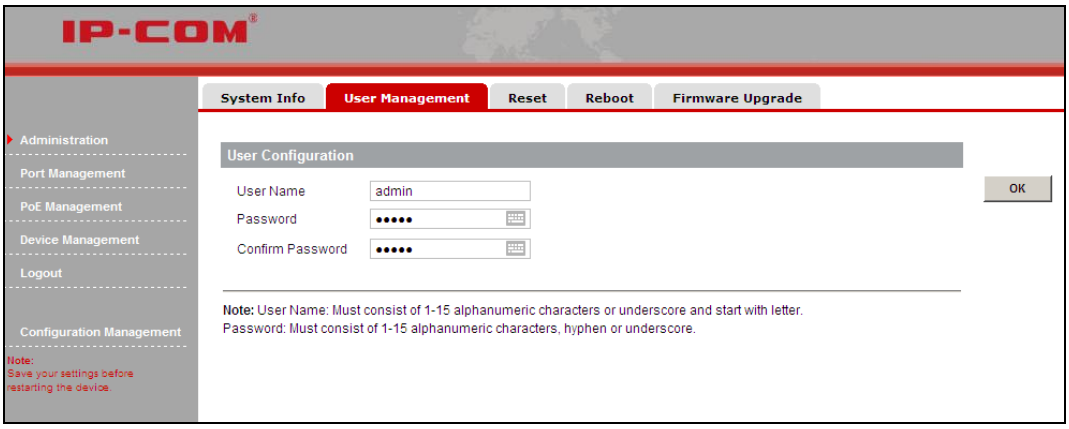
Fields on the screen are described below:

Field	Description
Firmware Version	Display switch's current firmware version
Hardware Version	Display switch's current firmware version
MAC Address	Display switch’s physical address
Management VLAN	VLAN1 is preset to management VLAN by default.
DHCP Client	Enable DHCP client to obtain an IP address automatically from the DHCP server on network. If the device fails to retrieve an IP address through DHCP, the previous IP address will be used Note the displayed IP address assigned by the DHCP server. You will need this value to access the switch directly from a web browser. Do not enable it if you cannot access the DHCP server to see the displayed IP address. If your network has no DHCP service, you must disable the DHCP client and assign a static IP address to your switch. You can also assign the switch a static IP address even if your network has DHCP service.
IP Address	Configure a static IP address, which will be used to access the switch's web manager. The default is 192.168.0.1.
Subnet Mask	Configure the corresponding subnet mask of the IP address specified above. The default is 255.255.255.0.
Gateway	Specify a gateway address for the switch. The default is 0.0.0.0.

MAC Age	This field specifies the length of time a learned dynamic MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). The MAC Address Aging Time can be set to any value between 60-3000 seconds. The default setting of 300 seconds is recommended.

3.2.2 User Management

The switch only supports a user. Once you change the user name or password, you must use the new user name or new password to access the web manager. If you unfortunately forget the login user name and/or password, simply press the RESET button on the front panel for about 5 seconds.



3.2.3 Restore Factory Defaults

This screen allows network managers to reset the device to the factory defaults shipped with the switch. Restoring factory defaults results in erasing the configuration file. The reset process takes about 30 seconds. Don't operate or interrupt the switch during this time.

Note:

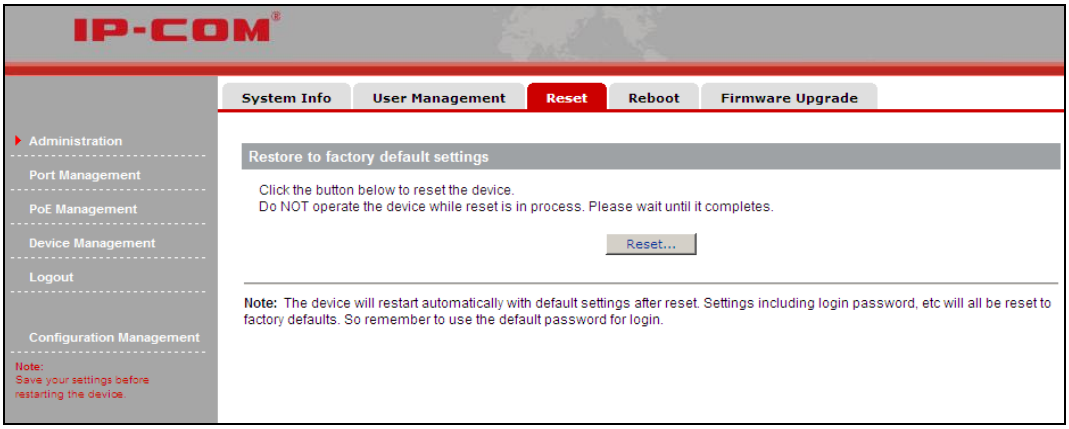
System will prompt you to restart the switch. All settings will return to their default values after reset. You will need to use the factory default settings to re-log in to the switch after restart.

Factory default settings:

IP address: 192.168.0.1

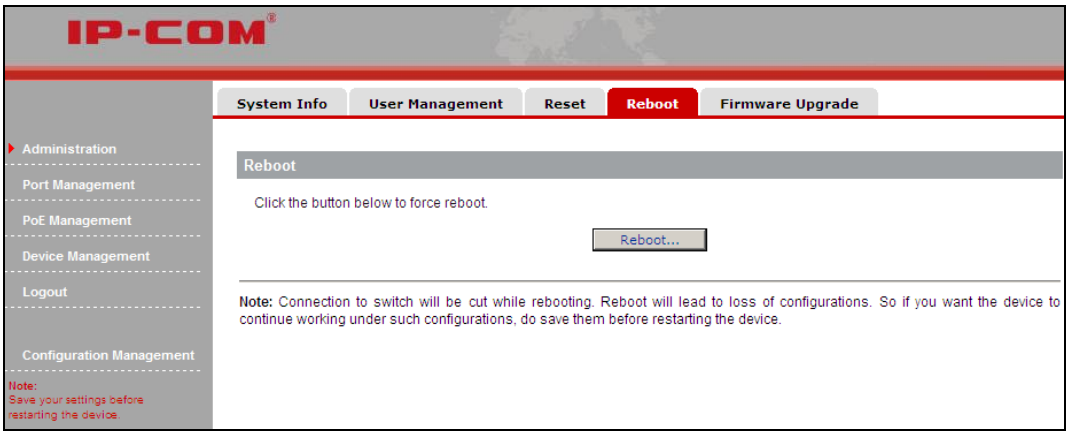
User Name: admin

Password: admin



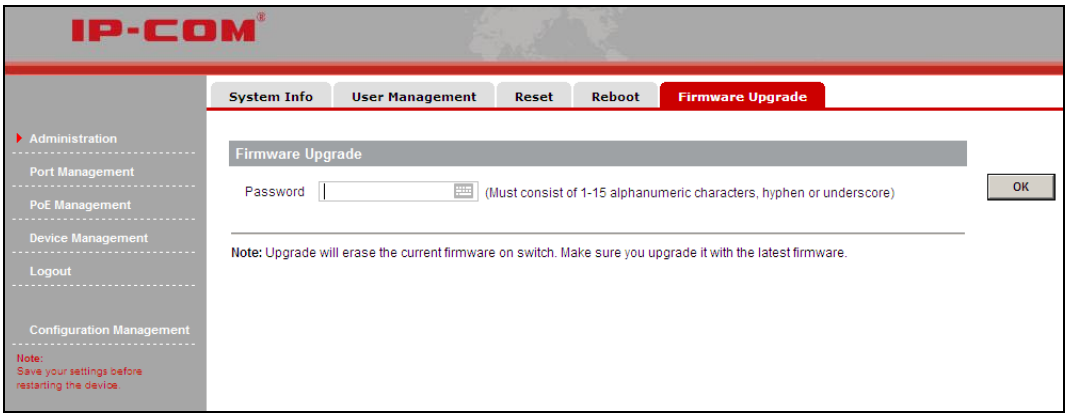
3.2.4 Reboot

Here you can reboot the switch. To reboot the switch, click **Reboot…** on the screen below.



3.2.5 Firmware Upgrade

The switch software is upgradeable, and enables your switch to take advantage of improvements and additional features as they become available. The upgrade procedure assumes that you have downloaded or otherwise obtained the firmware upgrade and that you have it available on your computer.



Password: Enter your login password for firmware upgrade.

OK: Click to confirm upgrade.

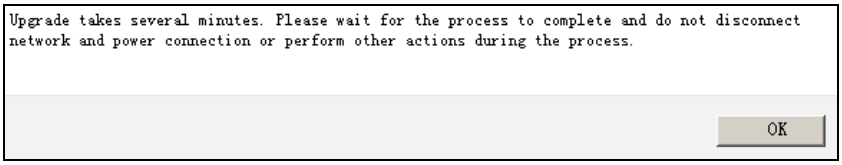
Cancel: Click to cancel upgrade.

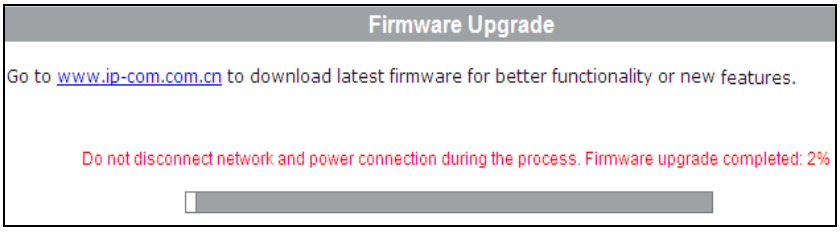
Browse: Click to locate the upgrade file.

Upgrade: Click to update the software.

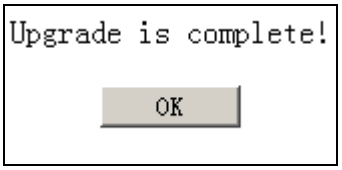
Note:

Software upgrade takes about 5 minutes. Please wait for the process to complete and do not disconnect network and power connection during the process.





Click **OK** on the window below to complete the process and system will return to management interface.



Note:

1. Do NOT interrupt power and network connections during software upgrading. If network is interrupted during the process, you must re-enter the upgrade screen and re-upgrade the software.
2. To return to management interface when you already enter the upgrade screen, simply click **Back**. But you cannot return to the management interface if upgrade is in process or upgrade fails.

3.3 Port Management

3.3.1 Port Configuration

1. Port Configuration

This section allows you to configure link rate, duplex mode, flow control and MAC address learning, priority and broadcast storm control settings on each individual port as well as enable or disable a particular port. You can select 10Mbps half-duplex, 10Mbps full-duplex, 100Mbps full-duplex, 100Mbps half-duplex, 1000 full-duplex (only available for ports 25-26) or auto-negotiation for the port to operate on. The default mode is Auto (auto-negotiation), in which the port automatically negotiates with the link partner for optimum speed/duplex mode. In this mode, a port communicates and negotiates automatically with linked partner to determine an optimum speed/duplex mode. Before selecting other options than “Auto”, ensure that the linked partner is operating in the same mode or in auto-negotiation mode; otherwise, communication may fail.

For packets not carrying 802.1Q tag, the switch uses port priority as 802.1p priority to look up in local priority mapping table and mark a local priority for it. In case of congestions, the switch forwards packets based on their priority levels.

Flow control regulates the rate of data transmission between two nodes to prevent a fast sender from outrunning a slow receiver, so that the receiving node does not drop packets due to buffer overflow.

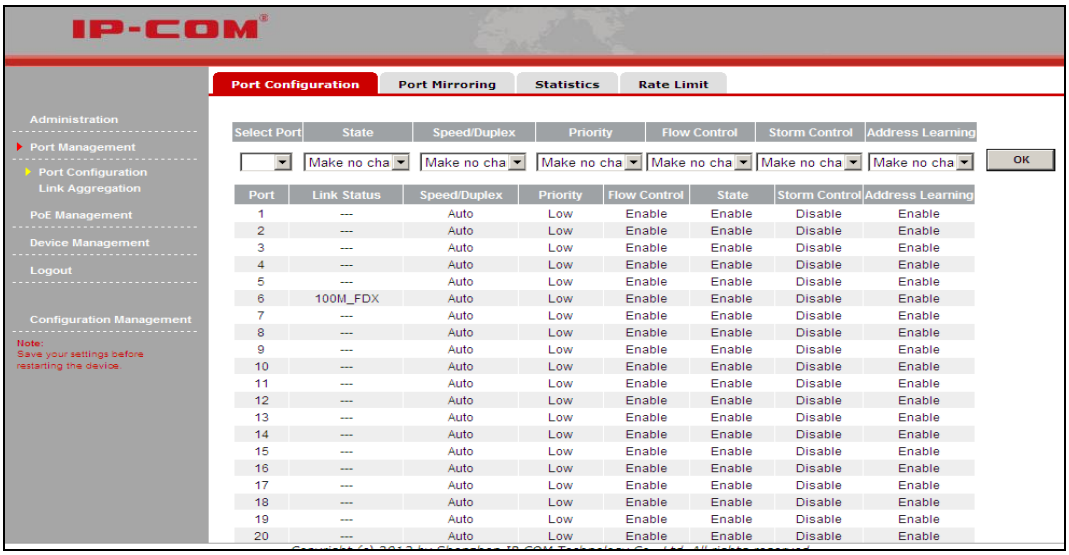
Broadcast storm control effectively prevents various broadcast storm, avoiding network congestion and ensuring a reliable network.

With MAC address learning feature, the switch identifies MAC addresses of NICs from all nodes and register them in its MAC address table so as to speed up forwarding frames by looking up destination MAC addresses of received frames in its MAC address table.

How you configure each port here will affect port mirroring, port rate limit and aggregation features, etc.

1. Config Port Settings

To enter the screen below, click **Port Management** > **Port Configuration.**



To configure a port, select a port number from the drop-down list, say, 1.

Fields on the screenshot above are described below:

Field	Description
Select Port	Select a port number from the drop-down list that you wish to configure.
State	Enable/Disable a port. If disabled, the corresponding port will be unavailable for use. By default this field is Enabled.
Speed/Duplex	Three types of modes are available on Ethernet ports: Full-duplex: Ports operating in Full-duplex mode can send and receive packets concurrently. Half-duplex: Ports operating in Half-duplex mode can either send or receive packets at a given time. Auto: Auto-negotiation, ports operating in Auto-negotiation mode determine their duplex mode by auto-negotiating with peer ports. By default, Auto (Auto-negotiation) is enabled. Available options for RJ45 ports 1-24 include 10M half-duplex, 10M full-duplex, 100M full-duplex and 100M half-duplex. Available options for RJ45 ports 25-26 include Auto (auto-negotiation) and1000M full-duplex RJ45 ports 25-26 are a part of the Gigabit combo (SFP fiber/copper) ports, where fiber ports always take priority over copper ports.
Priority	3 port priority levels are provided: **High**, **Low** and **Make no change**. The default setting is Low. For packets not carrying 802.1Q tag, the switch uses port priority as 802.1p priority to look up in local priority mapping table and mark a local priority for it. In case of congestions, the switch forwards packets based on their priority levels.
Flow Control	With flow control enabled on both the switch and its link partner, the switch, when encountering congestion, will send flow control frames to notify the link partner of

	such; upon receiving such frames, the link partner will temporarily stop sending packets to the switch, thus avoiding packets drop and ensuring a reliable network.
Storm Control	Enable/disable the broadcast storm control feature or restrict the max number of broadcast packets transmitted and received on active port(s). With broadcast storm control enabled, broadcast traffic exceeds the max value (2000pps), system will drop the excessive frames to reduce the traffic into a restricted ratio, thus effectively controlling various storms, avoiding network congestion and ensuring a reliable network.
Address Learning	Enable/disable the MAC address learning feature on a port. By default, it is enabled.
Link Status	Displays currently actual link rates and duplex modes on switch ports.

Note:

To update port settings like speed/duplex, priority, flow control, enable/disable a port, broadcast storm control and MAC address learning, first select a port and then click **OK**.

You can refresh the webpage to display updated settings on the port.

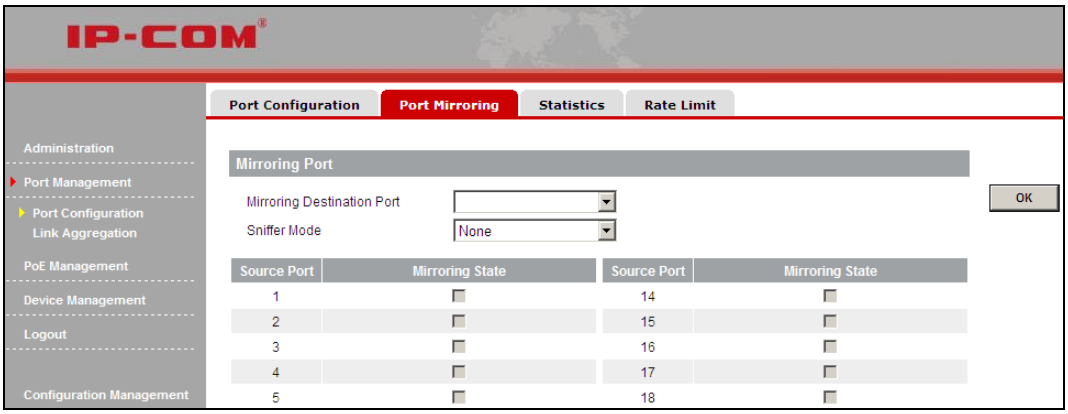
2. Port Mirroring

1. Port Mirroring Overview

Port mirroring is used on a network switch to send a copy of either inbound or outbound traffic (or both) on single or multiple mirroring source interfaces to a network monitoring connection on another mirroring destination port. This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion detection system. It can be used as a diagnostic tool as well as a debugging feature and also enables switch performance monitoring.

2. Config Port Mirroring

Click **Port Management > Port Configuration > Port Mirroring** to enter interface below.



To configure port mirroring settings, do as follows:

1) Select a mirroring destination port (only one).
2) Select a mirroring source port (you can select one or more mirroring source ports but only one mirroring destination port).
3) Select a proper Sniffer Mode (mirroring mode): None, Ingress, Egress or Egress & Ingress.
4) Click **OK** to complete your settings.

Fields on the screen are described below:

Field	Description
Mirroring Destination Port	Select the port to which port traffic is copied.
Sniffer Mode	Select a sniffer mode for a corresponding mirroring source port. Important: None: Indicates corresponding port is not mirrored. Ingress：Only incoming packets are copied to the monitor port. Egress：Only outgoing packets are copied to the monitor port. Egress & Ingress: Both inbound and outbound packets on the corresponding port are copied to the monitor port (mirroring destination port).
Source Port	Select the port from which the packets are mirrored

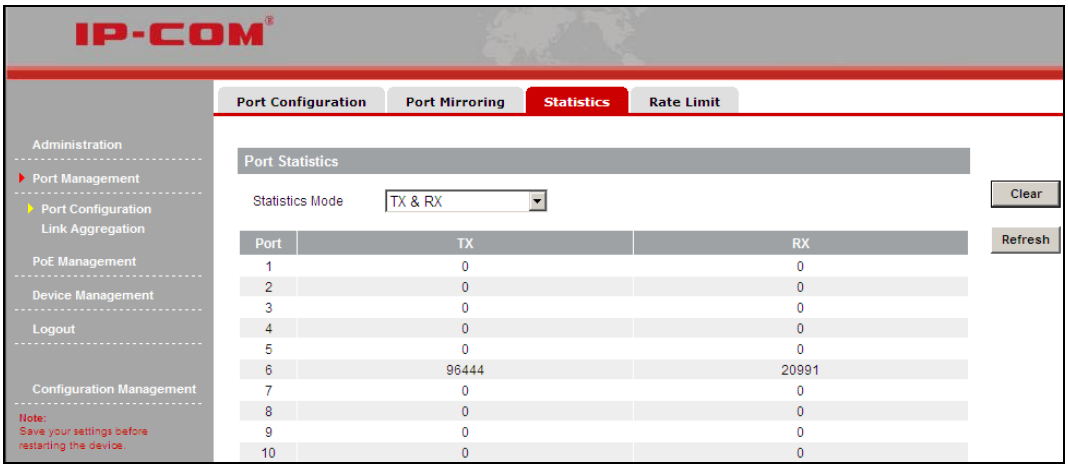
IMPORTANT:

1) A mirroring destination (monitor) port and mirroring source port should not be the same port.
2) A port in an aggregation group should not be configured as a mirroring destination (monitor) port.
3) A STP-enabled port should not be configured as a mirroring destination (monitor) port.
4) The bandwidth of the mirroring destination port should not be smaller than that of the mirroring source port(s).
5) A mirroring destination (monitor) port should be directly connected to a server that can monitor network traffic.

3. Statistics

Statistics displays the number of RX, TX, collision, drop and CRC error frame on each port.

To enter statistics interface below, click **Port Management** > **Statistics**.



You can select what type of data to count, for example RX & TX, and system will count and display the number of packets received & transmitted on each active port. Click **Refresh** to display updated statistic data or click **Clear** to clear current statistic data.

Note:

Counters will clear the current statistic data and restart counting if statistic mode is changed.

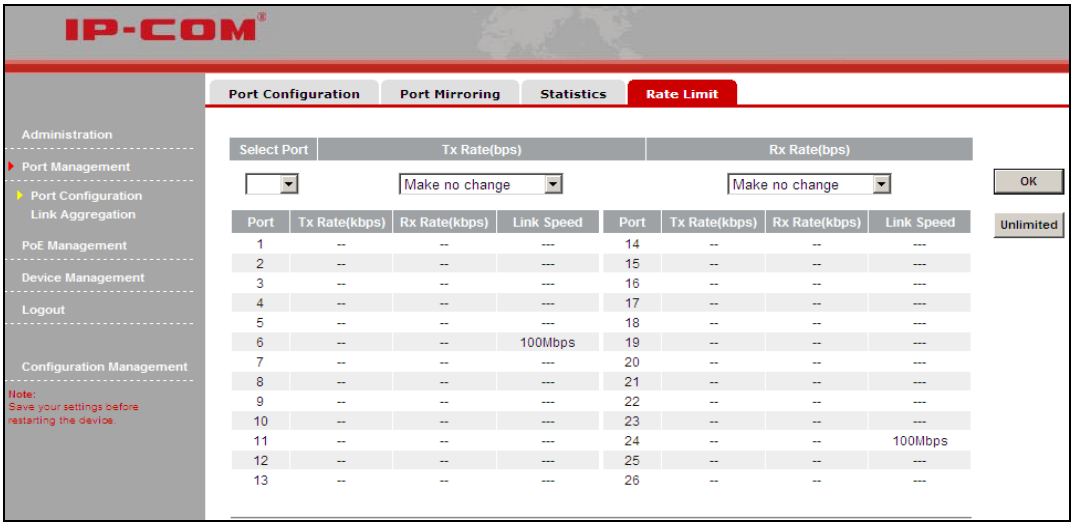
4. Rate Limiting

Rate limiting is used to control the rate of traffic sent or received on a network interface. Traffic that is less than or equal to the specified rate is sent, whereas traffic that exceeds the rate is dropped or delayed. It effectively avoids excessive bandwidth utilization by some users so that other users can have a guaranteed share of the bandwidth to enjoy a smooth network. It is useful for Internet caf és and community broadband environments.

Note that this feature is not applicable to the Gigabit ports 25-26.

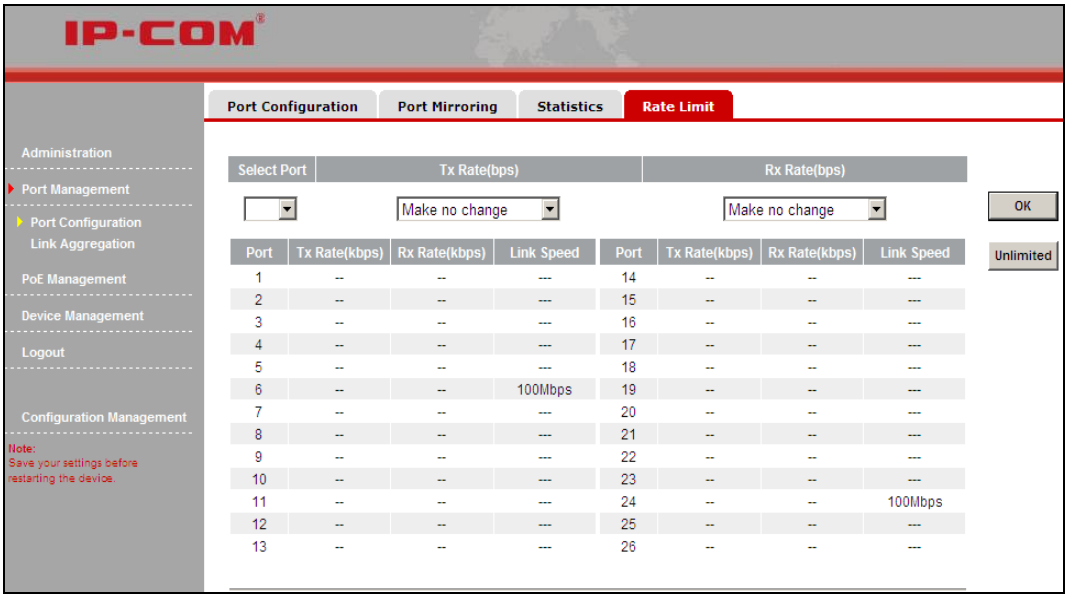
To enter the interface below, click **Port Management** > **Rate Limit**.

Unlimited: Each port transmits and receives packets at an actual link speed.



Fields on the screen are described below:

Field	Description
Port	Select a port number from the drop-down list.
Tx Rate (kbps)	Select a Tx (Tranmit) rate for a selected port. Options available are 256k, 512k, 1M, 2M, 4M, 8M, 10M, 16M, 32M, 64M and 100M. The default is "--", which means the given port transmits packets at an actual link rate.
Rx Rate (kbps)	Select an Rx (Receive) rate for a selected port. Options available are 256k, 512k, 1M, 2M, 4M, 8M, 10M, 16M, 32M, 64M and 100M. The default is "--", which means the given port receives packets at an actual link rate.



Fields on the above page are described below:

Field	Description
Port	Displays port ID
Link Speed	Displays link rate (Mbps) on each port
Tx Rate (kbps)	Displays maximum transmit rate (Kbps) on each port
Rx Rate (kbps)	Displays maximum receive rate (Kbps) on each port

Note:

The Tx/Rx (Transmit/Receive) rate should not exceed a given port's link rate, and if it does, system displays actual link rate only.

3.3.2 Link Aggregation

1. Link Aggregation Overview

Link aggregation groups multiple Ethernet ports together in parallel to act as a single logical link.

Aggregation-enabled devices treat all physical links (ports) in an aggregation group entirely as a single logical link (port). Member ports in an aggregation group share egress/ingress traffic load, delivering a bandwidth that is multiple of a single physical link. Link aggregation provides redundancy in case one of the links fails, thus reliability could be maintained. For example, if any port/link within the aggregation group becomes disconnected, packets intended for such port/link will be redirected to the other linked ports of the link aggregation group.

2. Port configuration considerations in link aggregation

(1)To share egress/ingress traffic load, member ports in an aggregation group must be set to the same configurations with respect to STP, QoS, VLAN, port attributes, etc.

Consistent STP Configurations: Includes state of port-level STP (enabled or disabled), type of the link (point-to-point or otherwise) connected to the port, STP cost, STP priority, loop/root protection (enabled or disabled) and port type (whether the port is an edge port), etc.

Consistent QoS Configurations: Includes rate limit, DSCP/802.1p priority.

Consistent VLAN Configurations: Includes VLANs permitted on the port and default VLAN ID on the port.

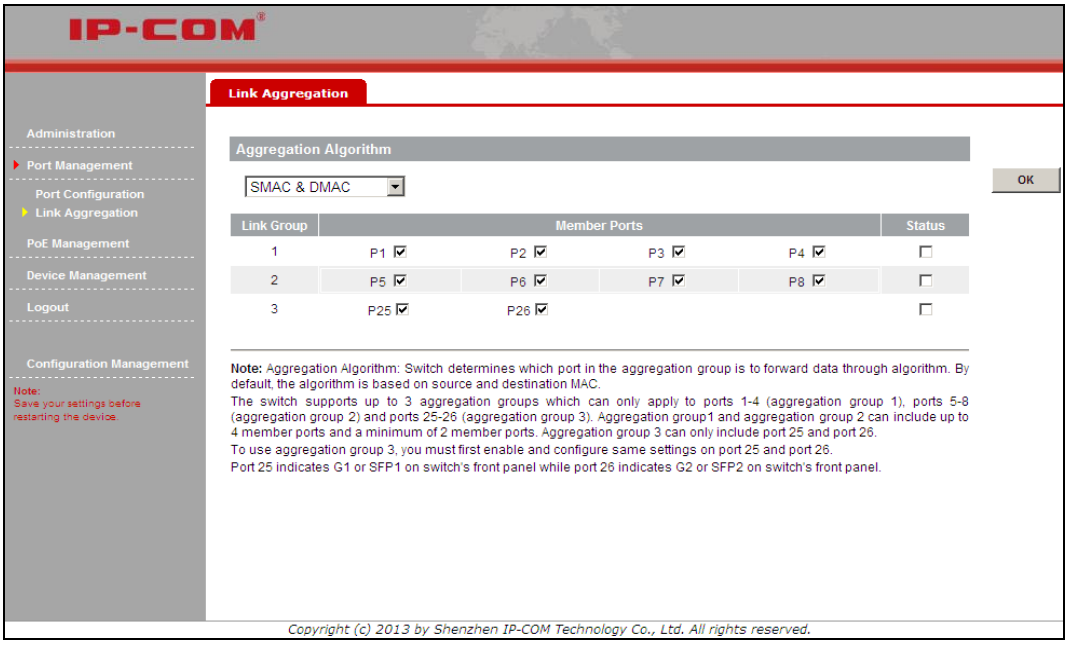
(2) When connecting switches using trunk feature, ensure uplink ports of partner switch are in an identical Trunk group. In other words, inter-switch multi-port (Trunk members) uplink must be implemented using the Trunk-to-Trunk scheme.

(3) Never connect 2 Trunk groups of a switch or uplink 2 switches through 2 groups of Trunk paths. Otherwise, it may cause network loop, broadcast storm and even collapse the whole network.

(4) The switch supports up to 3 aggregation groups which can only apply to ports 1-4, ports 5-8 and ports 25-26. Aggregation group 1 and aggregation group 2 can include up to 4 member ports and a minimum of 2 member ports. Aggregation group 3 can only include port 25 and port 26. Aggregation ports are not recommended for other configurations and use.

3. Link Aggregation Configurations

Click **Port Management > Link Aggregation** to enter the screen below.



To configure link aggregation settings, do as follows:

1) Select an aggregation algorithm from the Aggregation Algorithm drop-down list. Available options include port number Source MAC, Dest MAC and Source & Dest MAC. The default is Source & Dest MAC.
2) Select port numbers from Group Member.
3) Select Enable from Link Aggregation drop-down list box.
4) Click Save to complete your configurations.

4. Aggregation Algorithm

Member ports in a link aggregation group share traffic load according to specified aggregation algorithms.

Aggregation Algorithm	Description
Port ID	Member ports in a link aggregation group share traffic load according to the receiving port numbers.
SMAC	Member ports in a link aggregation group share traffic load according to source MAC addresses.
DMAC	Member ports in a link aggregation group share traffic load according to destination MAC addresses.
SMAC & DMAC	Member ports in a link aggregation group share traffic load according to source and destination MAC addresses.

IMPORTANT:

Below ports cannot be aggregated:

- Mirroring destination port
- Ports on which MAC address binding is enabled

3.4 PoE

PoE Overview

Power over Ethernet or PoE describes any of several standardized or ad-hoc systems which pass electrical power along with data on Ethernet cabling. This allows a single cable to provide both data connection and electrical power to devices such as network hubs, IP camera, wireless AP and closed-circuit TV cameras, etc. The IEEE standard for PoE requires category 5 cable or higher for high power levels, but can operate with category 3 cable if less power is required.

The original IEEE 802.3af PoE standard provides up to 15.4 W of DC power to each device. Only 12.95W is assured to be available at the powered device as some power is dissipated in the cable.

The updated IEEE 802.3at PoE standard also known as PoE+ or PoE plus, provides up to 25.5 W of power.

Power sourcing equipment

Power sourcing equipment (PSE) is a device such as a switch that provides ("sources") power on the Ethernet cable. The maximum allowed continuous output power per cable in IEEE 802.3af is 15.40 W. A later specification, IEEE

802.3at, offers 25.50 W.

Powered device

A powered device (PD) is a device powered by a PSE and thus consumes energy. Examples include wireless access points, IP Phones, and IP Cameras.

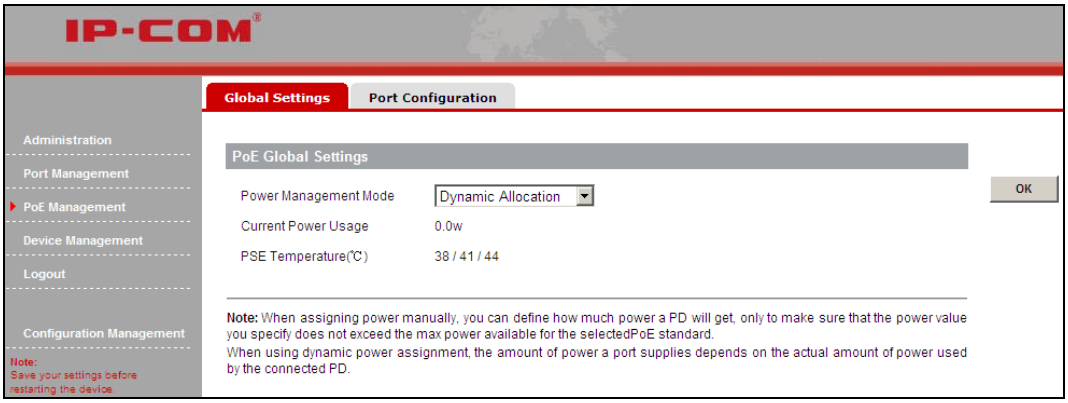
3.4.1 Global Configuration

Click **PoE Management** > **Global Settings** to enter Global Settings screen and you can

a).Configure power management mode;

b).View Current Power Utilization and PSE Temperature.

The default Power Management Mode is Dynamic Allocation. When assigning power manually, you can define how much power a PD will get, only to make sure that the power value you specify does not exceed the max power available for the selected PoE standard. When using dynamic power assignment, the amount of power a port supplies depends on the actual amount of power used by the connected PD.



Fields on the screen are described below:

Field	Description
Power Management Mode	Dynamic Allocation: If the power supply is running at 99% usage, ports prioritized as high are prioritized to receive power over ports prioritized as low. Static Allocation: If the power supply is running at 99% usage and new PDs are connected, priority is not taken in account and is not configurable, plus, no change is made on original power status.
Current Power Usage	Displays the total amount of output power.
PSE Temperature	Displays PoE module operating temperature.

3.4.2 Port Configuration

Click **PoE Management** > **Port Configuration** and you can

a). Configure PoE status, PoE standard, priority and static power allocation;

b). View the amount of power supplied to connected PDs and PD class.

If Dynamic Allocation is selected on the Global Settings screen, the Static Allocation field on the Port Configuration screen will be unconfigurable; if Static Allocation is selected, the Priority on the Port Configuration screen will gray out and become unconfigurable. Note that Port 25 and port 26 do not support PoE. In static power allocation mode, each PoE capable port is enabled with 802.3at PoE standard by default, supplying 30w of power. This 30w of power can only be supplied by the corresponding port to the connected PD and cannot be used by another port even though there is remaining power. For example, if the PD connected to the port only uses 10w, the remaining 20w will be wasted instead of being used by another port. We recommend dynamic power allocation and IEEE 802.3at PoE standard (which is the default PoE standard).

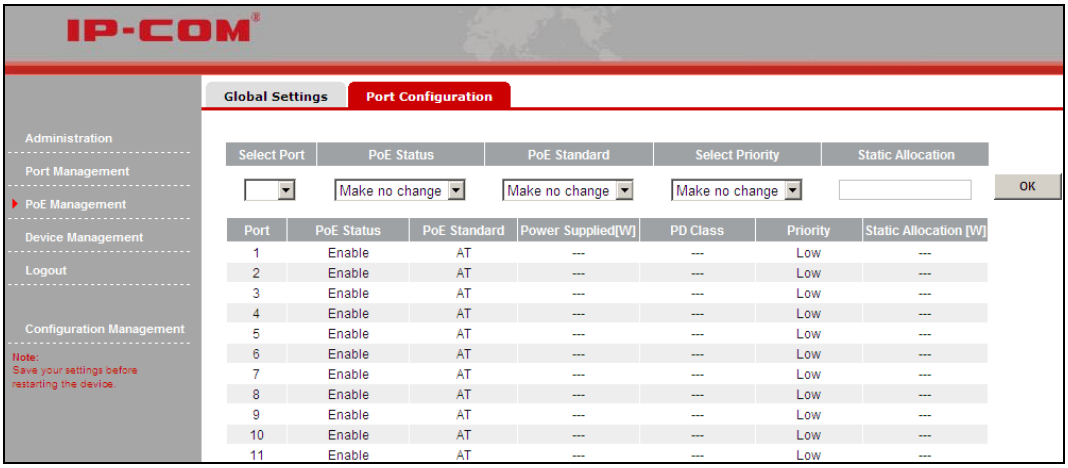


Figure 1

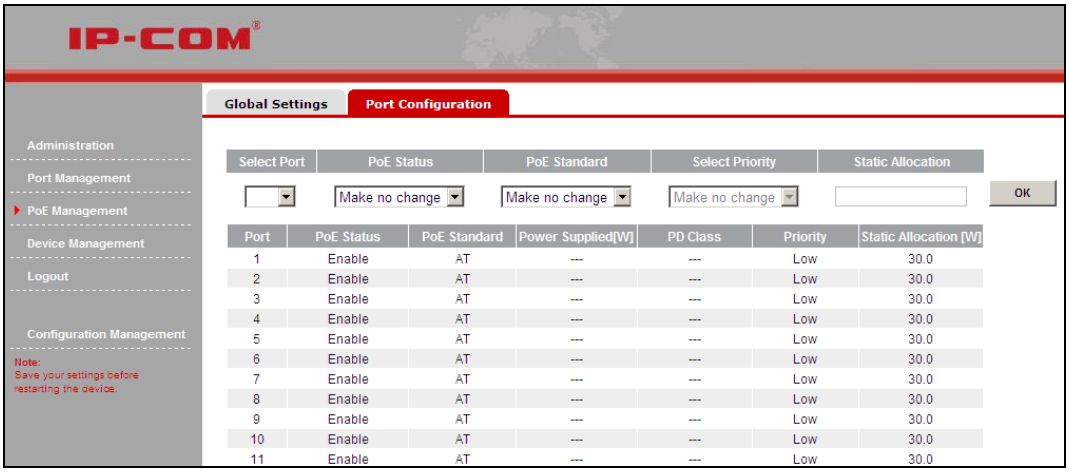


Figure 2

Fields on the screen are described below:

Field	Description
Select Port	Select a port number you wish to configure. Port numbers range from 1 to 24.
PoE Status	Enable/disable PoE. If disabled, the port will not supply power. By default, this option is enabled.
PoE Standard	The switch supports IEEE 802.3af and IEEE 802.3at PoE standards. IEEE 802.3af: The original IEEE 802.3af PoE standard provides up to 15.4 W of power to

	each device and power levels of 0, 1, 2 and 3. IEEE 802.3at: IEEE 802.3af: Compatible with IEEE 802.3af, the IEEE 802.3at PoE standard provides up to 30W of power to each device and power levels of 0, 1, 2, 3 and 4.
Priority	This field is available only if dynamic allocation is selected. Options available include High, Medium and Low. If the power supply is running at 99% usage, ports prioritized as high are prioritized to receive power over ports prioritized as medium and/or low. For example: If the power supply is running at 99% usage and port A prioritized as high connects a new PD, power supply to the PD connected to the port prioritized as low will be disconnected to ensure port A power; or in case of same port priorities, power supply to the PD connected to the port with a large logic port number will be disconnected.
Static Allocation	This field is available for configuration if Static Allocation is selected from the power management mode drop-down list. IEEE 802.3af: Enter a valid power value between 0-15.4w. If you enter a power value that is greater than 15.4w, 15.4w will be applied automatically. IEEE 802.3at: Enter a valid power value between 0-30w If you enter a power value that is greater than 30, 30w will be applied automatically.
Power Supplied	Display actual output PoE power supplied by the port. This is associated to the power consumed by the PD connected to the port.
PD Class	Classification of PDs connected to the switch. IEEE 802.3af compliant PDs are classified into classes of 0, 1, 2 and 3. IEEE 802.3at compliant PDs are classified into classes of 0, 1, 2, 3 and 4.

Note:

1. You must click **OK** to bring your configurations into effect each time you configure a port.
2. You can view your configurations on this page.

3.5 Device Management

3.5.1 VLAN

1. VLAN Overview

A Virtual Local Area Network (VLAN) is a network topology which allows to logically instead of physically segment a LAN into several net segments. A VLAN combines a group of hosts with a common set of requirements logically instead of physically relocating devices or connections. In 1999, IEEE released 802.1Q draft as a standardized VLAN implementation solution.

VLANs allow a network to be logically segmented into different broadcast domains. All members in a VLAN are

treated as in the same broadcast domain and communicate as if they were on the same net segment, regardless of their physical locations. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated. Different VLANs cannot intercommunicate directly. Inter-VLAN communication can only be achieved using a router or other layer 3 devices that are able to perform Layer 3 forwarding.

2. Benefits of VLANs

Broadcast traffic and unicast traffic are confined to each VLAN, reducing bandwidth utilization and improving network performance. VLANs are used for multiple reasons.

Better management and control of broadcast activity

VLANs conserve network resources by segmenting a large broadcast domain into several smaller broadcast domains or VLAN groups and restrict all broadcast traffic to the VLAN on which the broadcast was initiated.

Reduced cost

The use of VLANs to create broadcast domains eliminates the need for routers to handle this function, permitting operation at lower latencies and cost compared to routers under heavy load and at high cost.

Ease of network administration

Members of a VLAN group can be geographically dispersed as they are logically related instead of physically on the same VLAN. Thus network administrators do not need to re-config the network when a VLAN member changes its location. For example, in order to better collaborate with staffs from home or abroad on a special project a workgroup is indispensable. Using VLAN, all workstations and servers that a particular workgroup uses can be assigned to the same VLAN.

Tighter network security

Different VLANs cannot intercommunicate directly. Inter-VLAN communication can only be achieved using a router or other layer 3 devices that are able to perform Layer 3 forwarding.

3. VLAN Mode

The switch provides 2 VLAN modes as below:

802.1Q VLAN Mode

IEEE 802.1Q is the networking standard that supports Virtual LANs (VLANs) on an Ethernet network. The standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames.

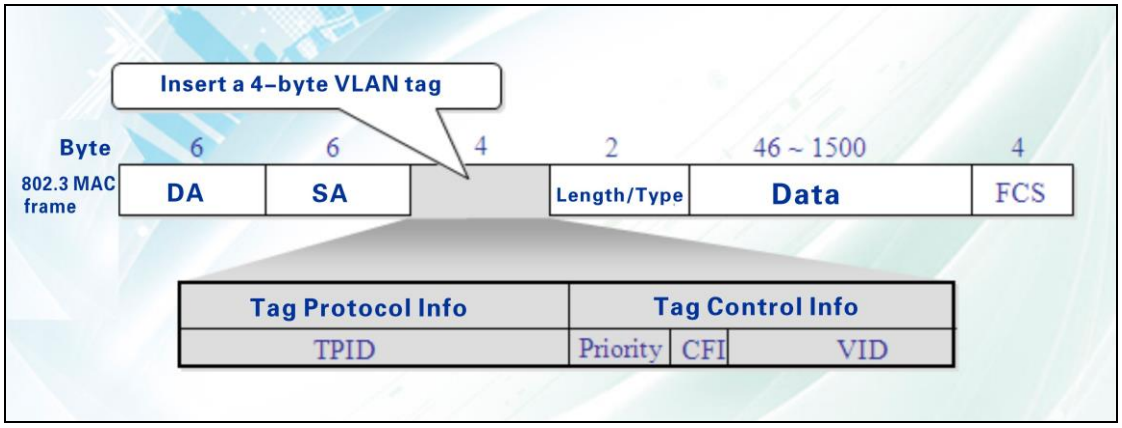
Port-based VLAN Mode (The switch operates in this mode by default)

Port-based VLANs limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department. Members of the same VLAN can intercommunicate. A user can belong to multiple VLANs simultaneously. For example, if you want both user A and user B to communicate with user C while user A and user B cannot intercommunicate, simply put user A and user C to a VLAN and user B and user C to the other VLAN.

4. 802.1Q VLAN

Tagged VLAN

As defined in IEEE 802.1Q, a four-byte VLAN tag is inserted after the DA&SA field to identify frames of different VLANs.



TPID: The 16-bit TPID field with a value of 0x8100 indicates that the frame is VLAN-tagged.

Priority: The 3-bit priority field indicates the 802.1p priority of the frame.

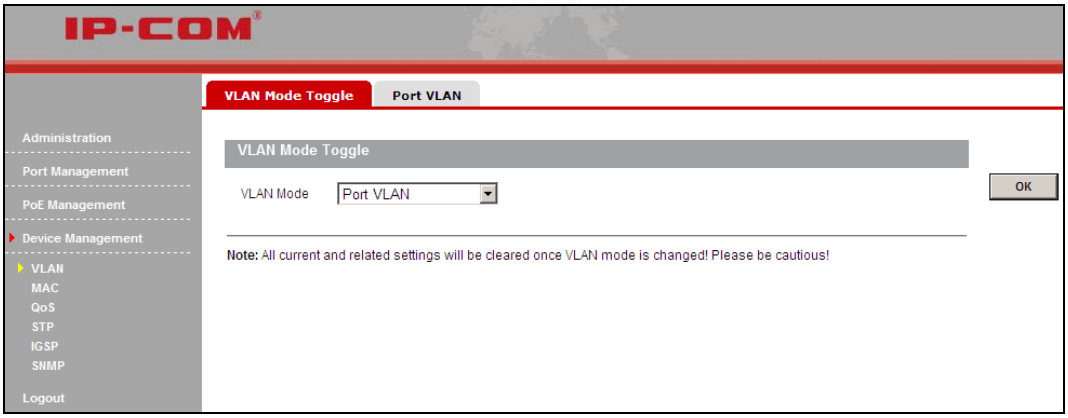
CFI: The 1-bit CFI field specifies whether the MAC addresses are encapsulated in the standard format. A value of 0 indicates that MAC addresses are encapsulated in the standard format. A value of 1 indicates that MAC addresses are encapsulated in a non-standard format. For Ethernet switches, it is advisable to set this value to 0.

VID: The 12-bit VLAN ID field identifies the VLAN that the frame belongs to. The VLAN ID range is 0 to 4095. Because 0 and 4095 are reserved, a VLAN ID actually ranges from 1 to 4094.

5. VLAN Mode Toggle

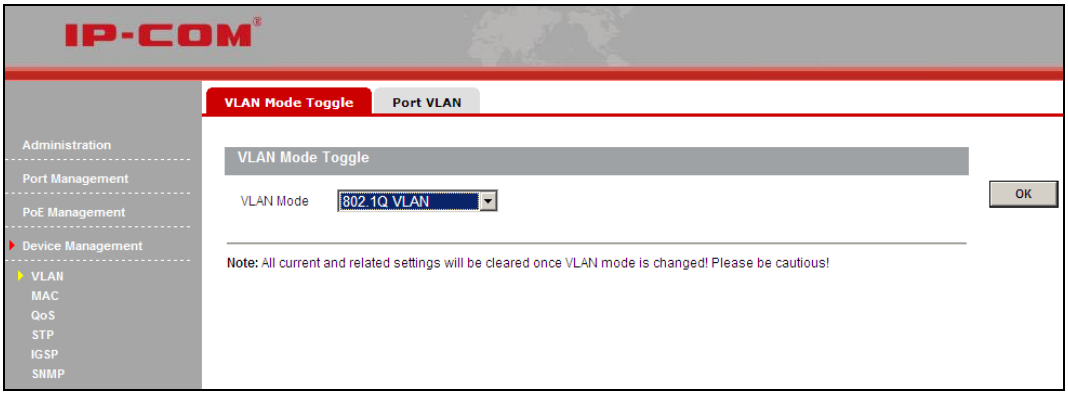
You can toggle between port VLAN and 802.1Q VLAN. Note that related settings like MAC address table entries will be removed when you change the VLAN mode.

To enter the screen below, click **Device Management** > **VLAN** > **VLAN Mode Toggle**.



To switch to 802.1Q VLAN:

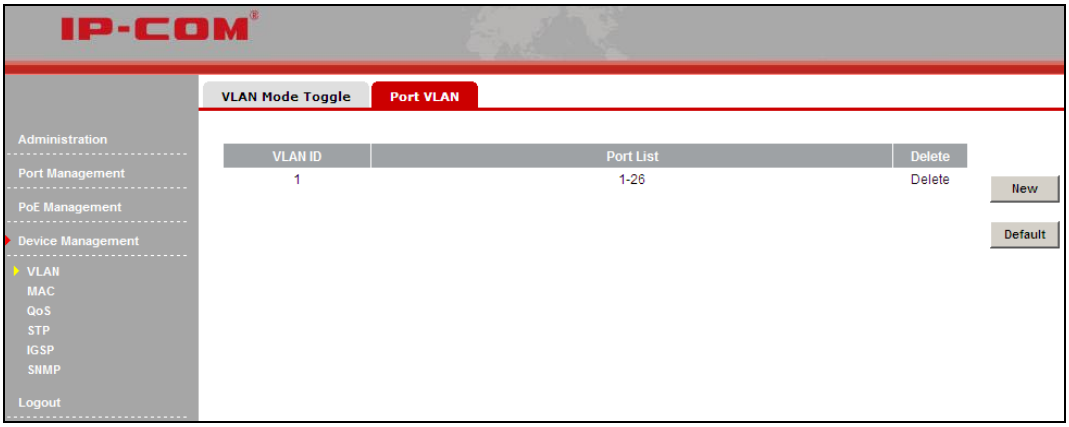
Select **802.1Q VLAN** and click **OK**. The default VLAN mode is port based VLAN.



6. Port VLAN Configuration

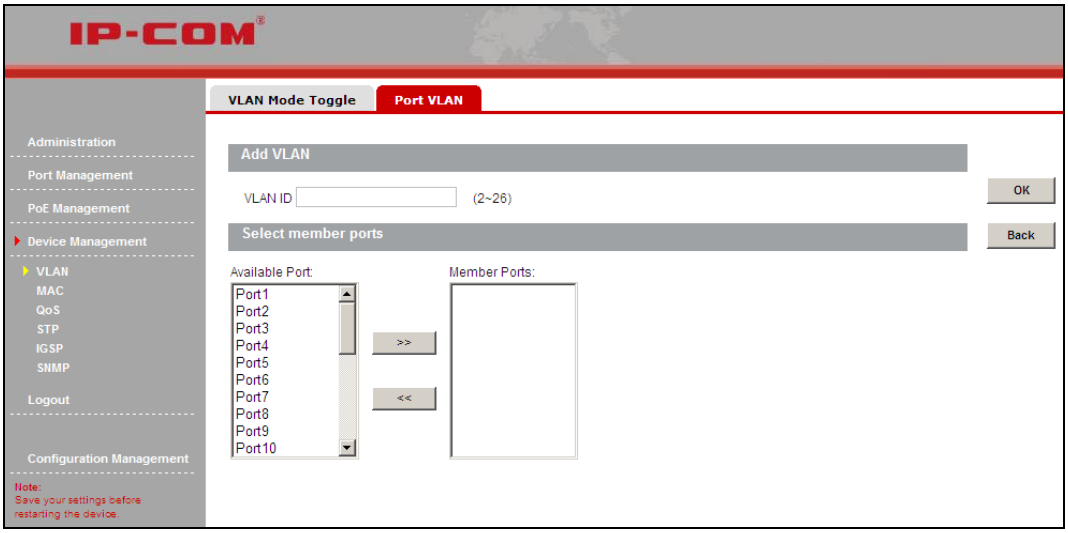
Here you can configure port VLAN settings. A port can join multiple port VLANs. Up to 26 VLANs can be configured.

In port VLAN mode, click **Device Management** > **VLAN** > **Port VLAN** to enter the Port VLAN screen below:



To add a port VLAN, do as follows:

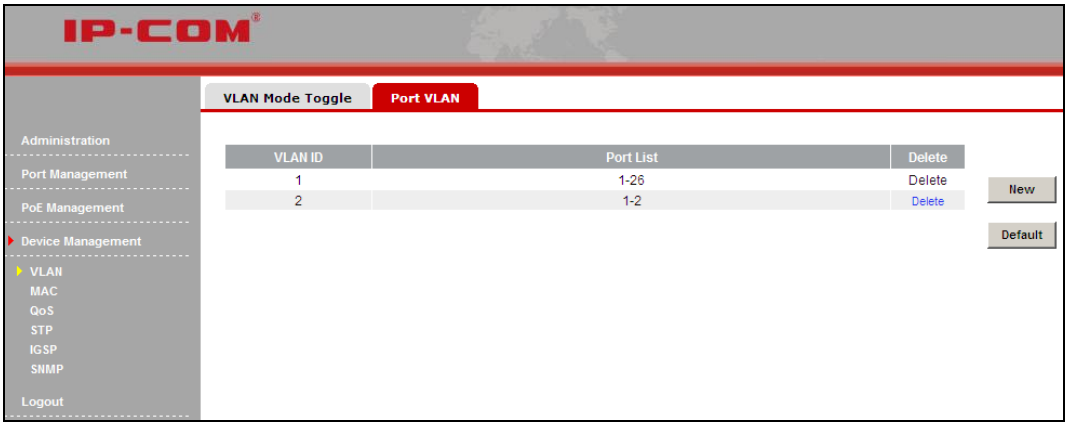
1) Click **New** to enter the screen below:



2) Specify a VLAN ID between 2~26.

3) Select the ports you wish to add to the VLAN from **Available Port** box and click >> to move them to the **Member Ports** box. You can press the **Ctrl** key or **Shift** key on your keyboard to select multiple ports

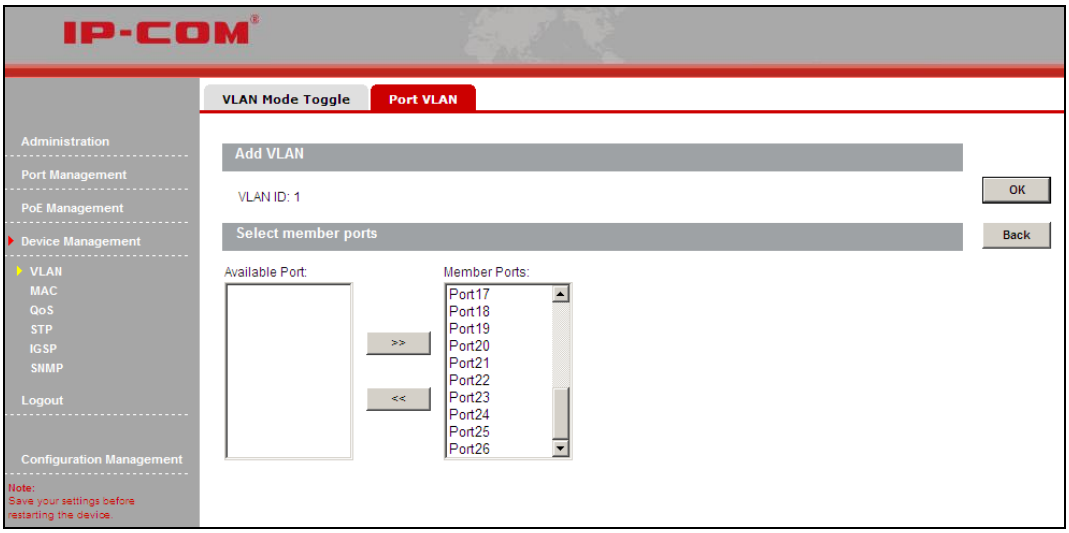
4) Click **OK** and a screen similar to the below will appear.

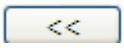


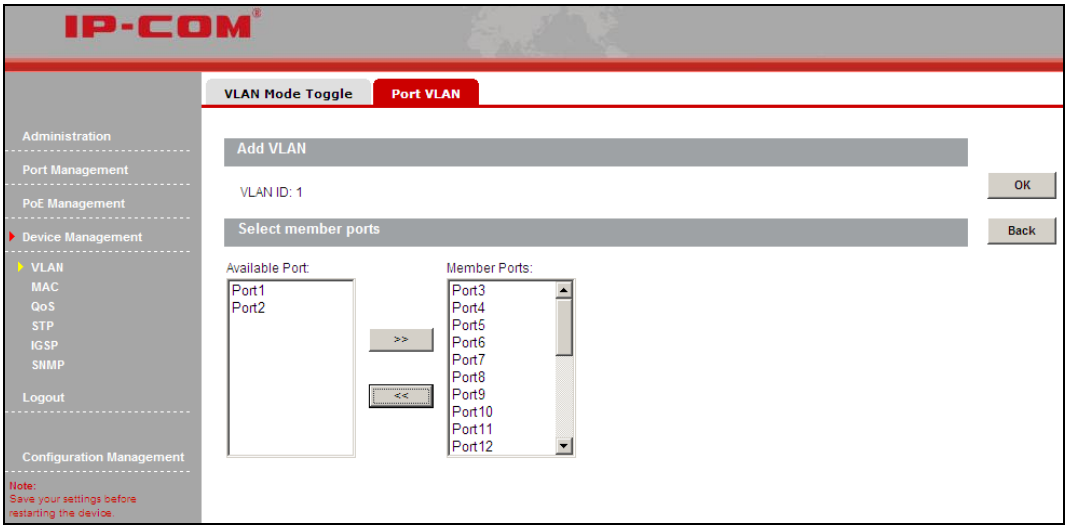
To change port VLAN members

As seen on the screen above, port 1 and port 2 are also included in VLAN1. To isolate them from other ports**,** follow instructions below to remove them from VLAN 1.

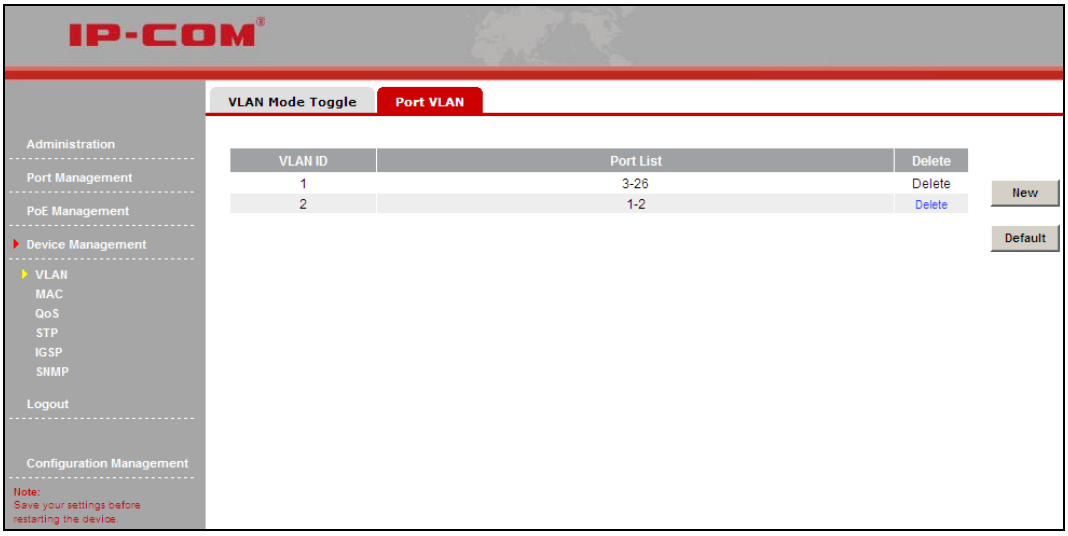
1) Click **VLAN1** to enter the screen below:



2) Click  to move them back to the **Available Port** box.



3) Click **OK** and you will see the screen below (port 1 and port 2 are no longer included in VLAN1):



To remove an existing VLAN

To remove an existing VLAN, simply click the **Delete** button next to the existing VLAN ID you wish to remove. Note that the default VLAN1 cannot be deleted.

By default, all member ports will return to VLAN1 when an existing VLAN is deleted.

Important:

Up to 26 port VLANs can be configured.

A new VLAN must include at least one member port.

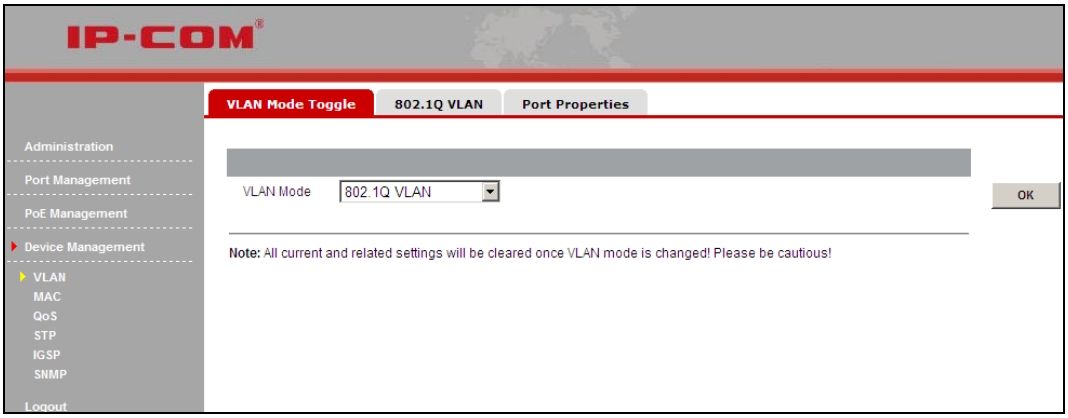
A member port must belong to at least one VLAN.

A port that no longer belongs to any VLAN after the VLAN it belonged to is removed will automatically return to the default VLAN1.

Port based VLAN cannot implement inter-switch isolation or provide segmentation services across different switches.

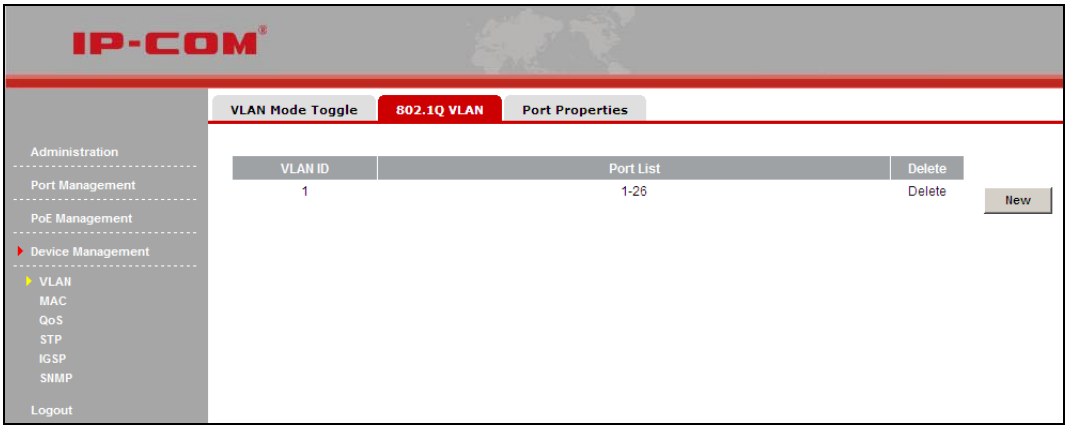
7. 802.1Q VLAN Configurations

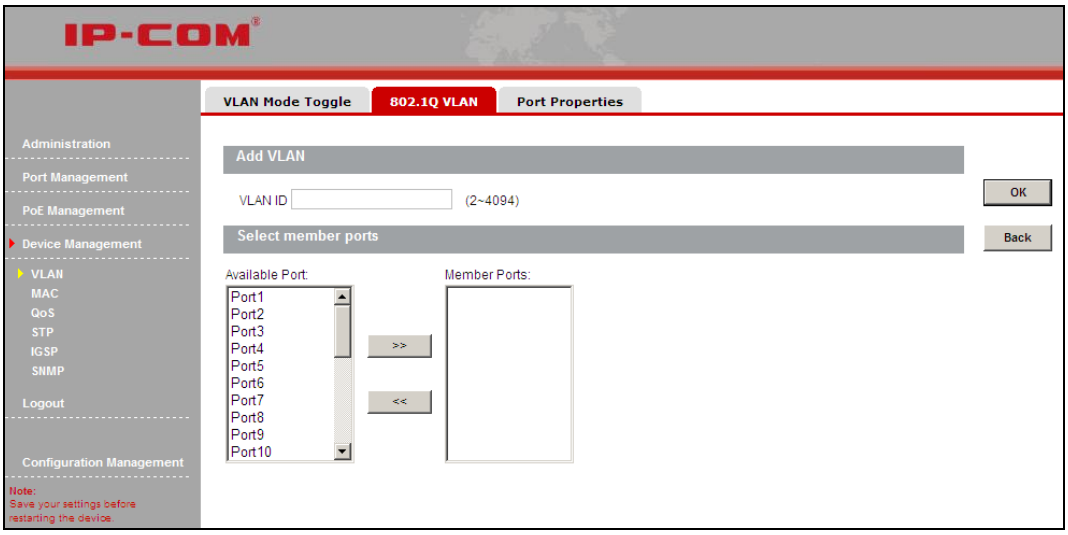
To enter the screen below, click **Device Management** > **VLAN** > **802.1Q VLAN**.



To add a QVLAN, do as follows:

1) Click **New** to enter below screen:

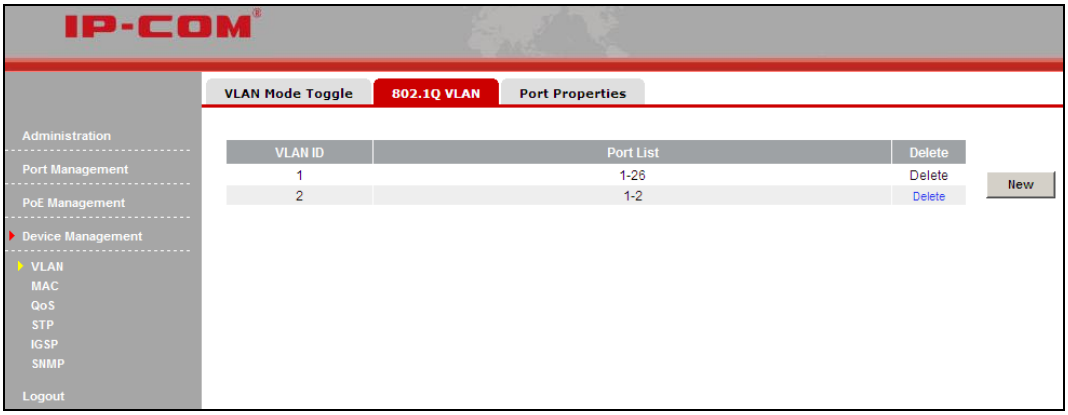




2) Specify a VLAN ID between 2~4094.

3) Select the ports you wish to add to the VLAN from **Available Port** box and click >> to move them to the **Member Ports** box. You can press the **Ctrl** key or **Shift** key on your keyboard to select multiple ports

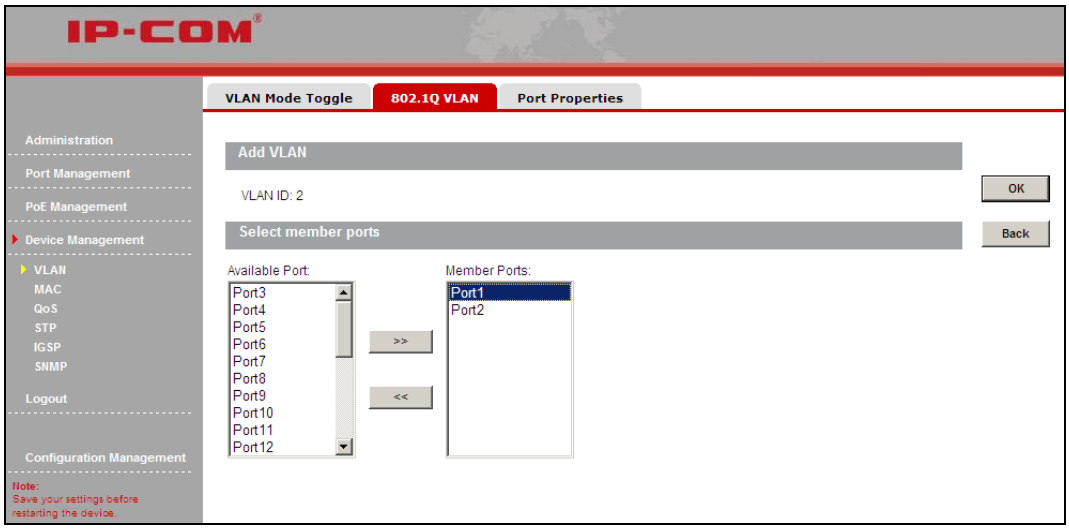
4) Click **OK** and a screen similar to the below will appear.



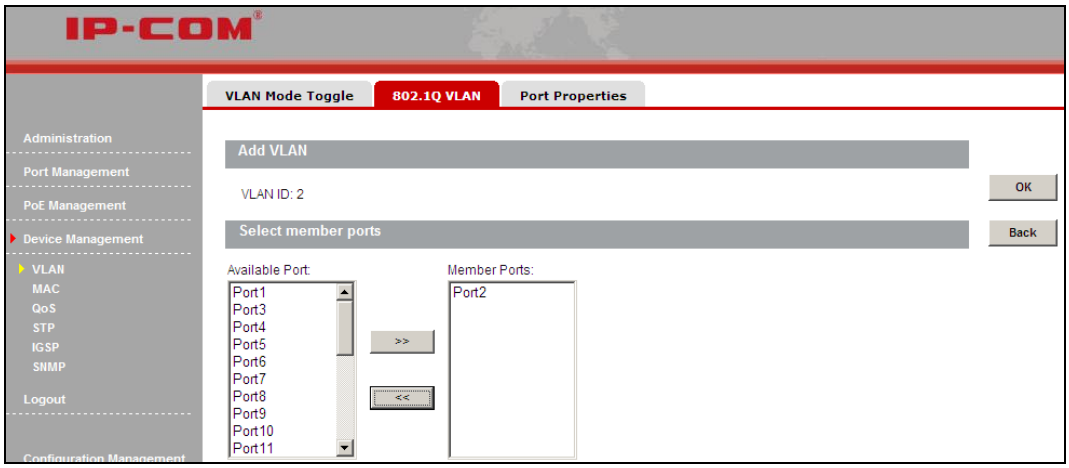
To change 802.1Q VLAN member ports

As seen on the screen above, to change member ports of the 802.1Q VLAN 2 to port 2 and port 3**,** follow instructions below.

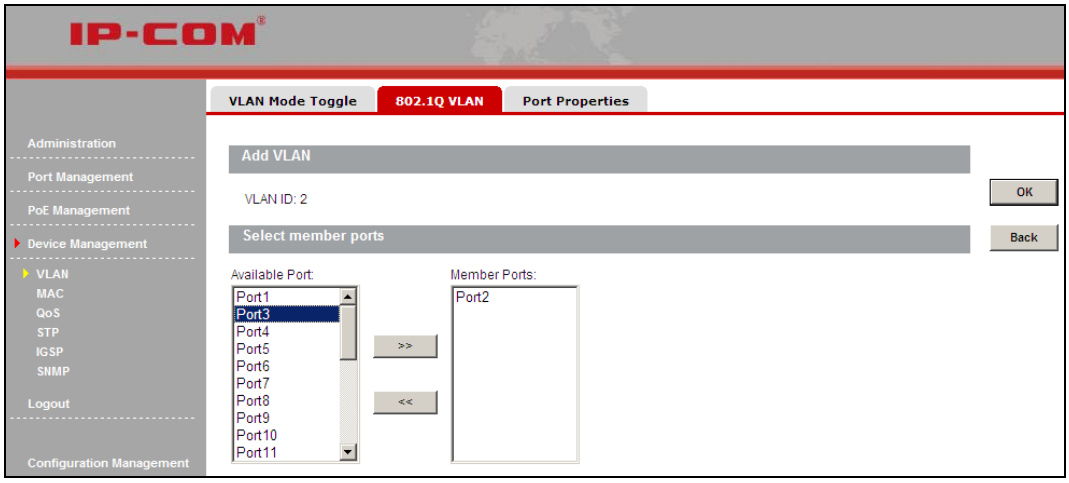
1) Click VLAN2 to enter the screen below and select port 1 from the **Member Ports** box.



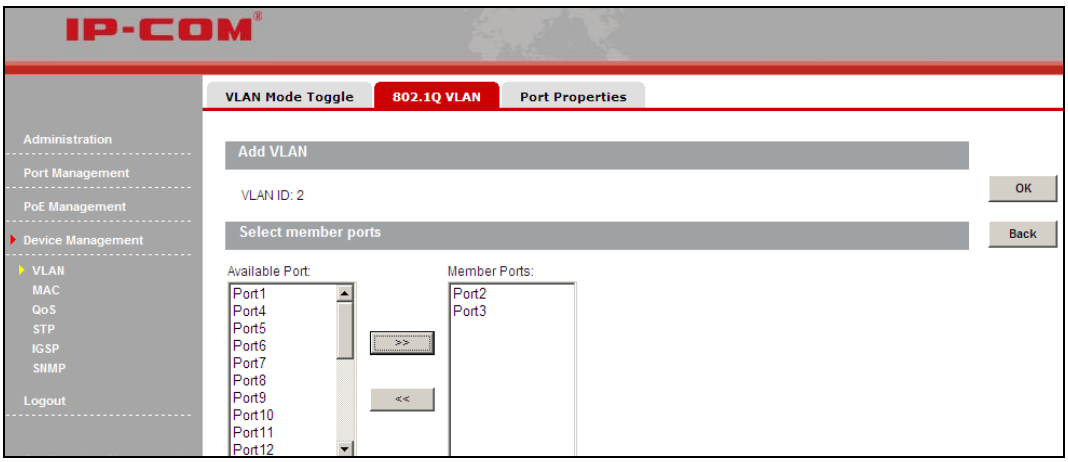
2) Click << to move it back to the **Available Port** box



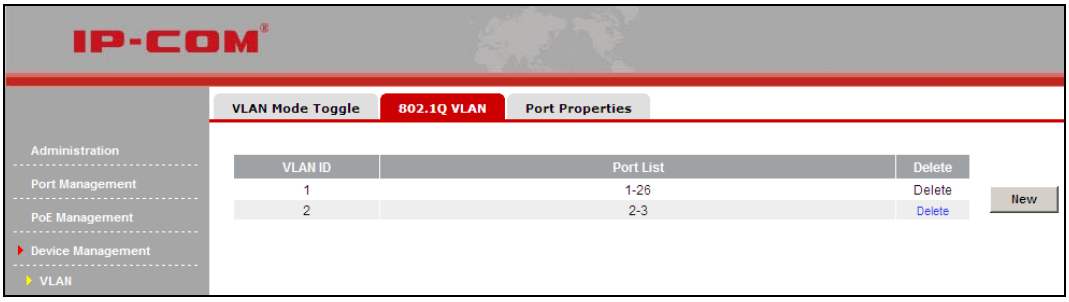
3) Select port 3 from the **Available Port** box.



4) Click >> to move it to the **Member Ports** box.



5) Click **OK** and a screen below will appear.

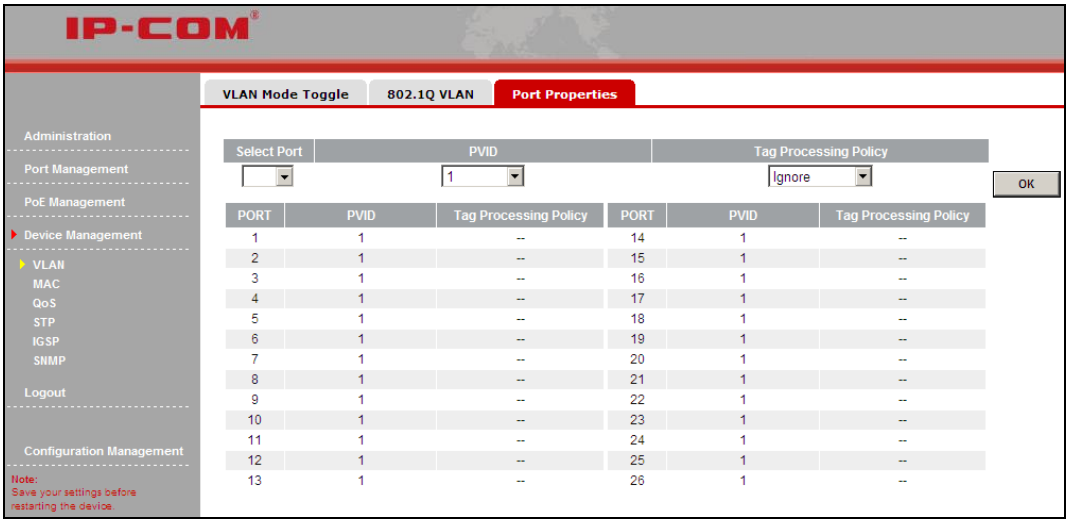


To remove an existing 802.1Q VLAN

To remove an existing 802.1Q VLAN, simply click the **Delete** button next to the existing VLAN ID you wish to remove. Note that the default VLAN1 cannot be deleted.

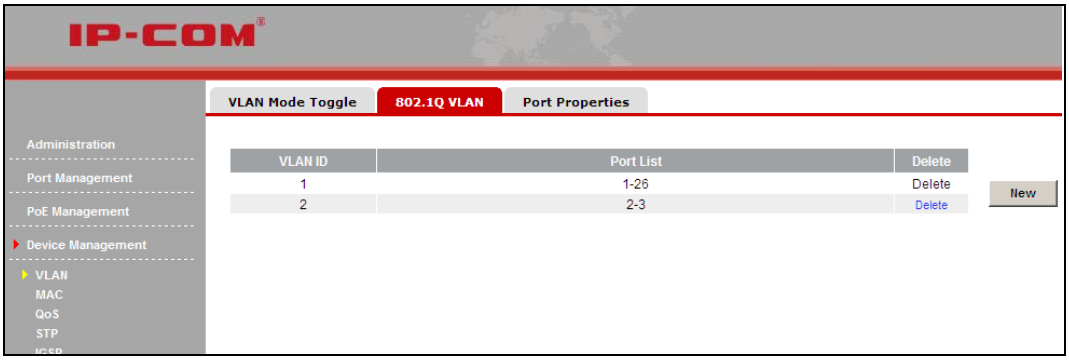
802.1Q VLAN Port Properties

To enter the screen below, click **Device Management > VLAN > Port Properties**.

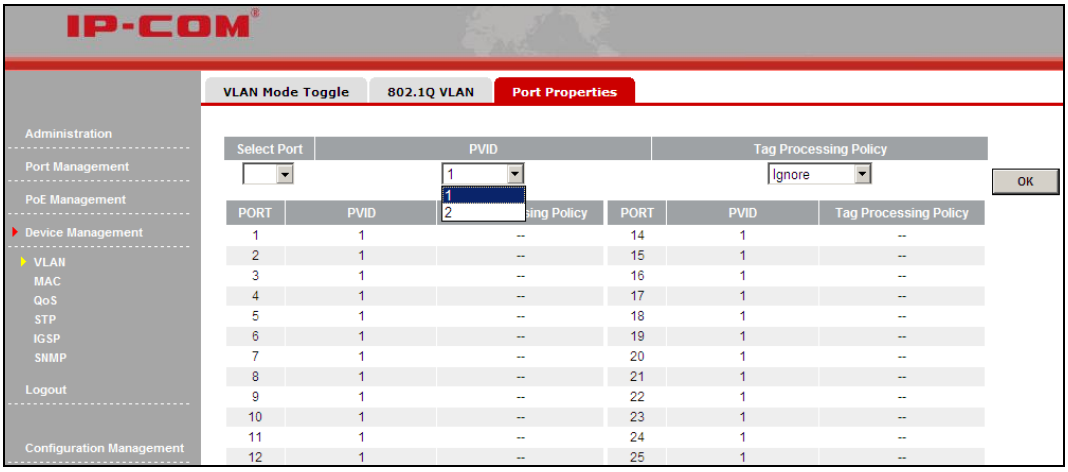


1. Port PVID

A PVID directs packets without VLAN tags to a default VLAN. PVID can be different for each port and must indicate an existing VLAN. QVLAN configurations are as seen on the screen below: there are currently two VLANs: VLAN1 and VLAN2.



As seen on the screen below, available PVIDs for port 1 are 1 and 2.



2. How port handles tag:

Ignore: Packets are forwarded as they are.

For example, if port 3 is configured to Ignore, all tagged packets received on port 3 will be forwarded with tags and all untagged packets received on port 3 will be forwarded without tags

Add Tag: Add tag to egress packets.

For example, if port 3 is configured to Add Tag, then all untagged packets received on port 3 will be tagged before they are forwarded

Remove Tag (Untag): Remove tags from egress packets.

For example, if port 3 is configured to Remove Tag, then all tagged packets received on port 3 will be removed (untagged) before they are forwarded

IMPORTANT:

- Up to 32 802.1Q VLANs can be configured.
- An 802.1Q VLAN can be empty (include no ports).
- All ports always belong to VLAN1. You can implement VLAN isolation using the QVLAN PVID.
- Operating in 802.1Q VLAN mode, MAC address learning is shared and a MAC address can only belong to one VLAN.
- 802.1Q VLAN can implement inter-switch isolation and provide segmentation services across different switches.

PVID is not affected by VLAN ID. For example, you can assign port 1 to VLAN 1, VLAN2 and VLAN3 but

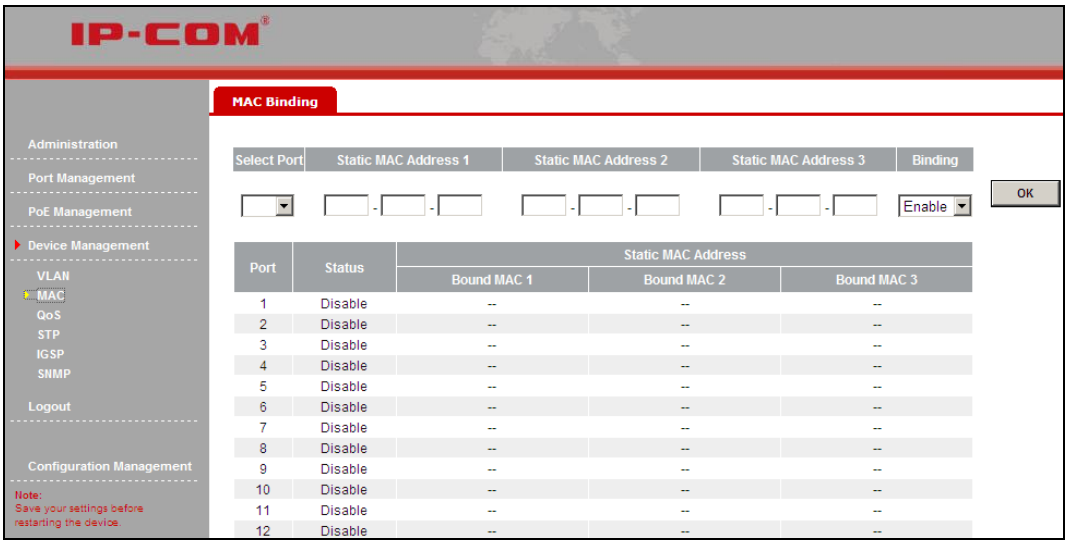
configure the port 1's PVID to any existing VLAN ID, for example, 4; however, if the existing VLAN ID 4 is deleted, port 1's PVID will be reset to the default value of 1.

3.5.2 MAC Binding

When a unicast MAC address is bound to a specific port on the switch, messages carrying this MAC as a source MAC address can only be received and forwarded by this bound port and will be directly dropped by other recipients; messages carrying this MAC as a destination MAC address will only be forwarded by switch to the specific bound port. A bound MAC address will not age out.

This feature is especially helpful to prevent any unauthorized access to your network.

Click **Device Management** > **MAC Binding** to enter the screen below:



Fields on the screen are described below:

Field	Description
Select Port	Select a port number you wish to configure.
Static MAC Address	Manually enter the MAC address (unicast address only) you wish to bind with the port on switch. Each port can bind up to 3 addresses.
Binding	Enable/disable MAC binding feature. By default, this feature is disabled.
Status	Display current port's binding status: enabled or disabled.

To enable port-MAC binding feature do as follows:

1) Select the port number you wish to bind, say, 1
2) Manually enter the MAC address (unicast address only) you wish to bind with the selected port, say, 00-B0-4C-00-00-01.
3) Select Enable from the Binding drop-down list.
4) Click OK to complete your configurations.

Note:

Ports that are enabled with MAC address binding will no longer be able to learn MAC addresses.

To disable MAC address binding feature, do as follows:

1) Select the port number that is already bound to a specific MAC address, say, 1
2) Select Disable from the Binding drop-down list
3) Click **OK** to complete your configurations

3.5.3 QoS

1. QoS Overview

Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow. For example, a required bit rate, delay, jitter, packet dropping probability and/or bit error rate may be guaranteed. Quality of service guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications such as voice over IP, online games and IP-TV, since these often require fixed bit rate and are delay sensitive, and in networks where the capacity is a limited resource, for example in cellular data communication.

QoS addresses network latency and congestion issues. Non-critical (elastic) applications like web browsing or emailing do not rely on QoS as they function however much or little bandwidth is available. However, for critical (inelastic) services or applications that require a certain minimum level of bandwidth and a certain maximum latency to function, QoS is indispensable. QoS can prevent critical traffic flow from being discarded or delayed on a congested and overloaded network, thus ensuring a mix of real-time/interoperative and non-real-time/non-interoperative traffic without meltdown.

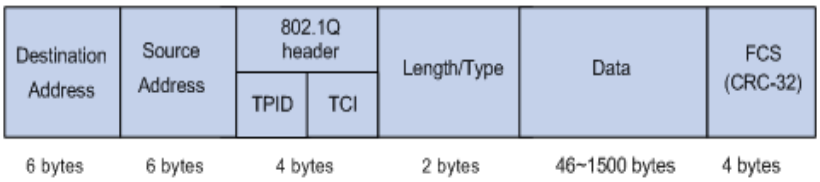
2. Widely used priority types

Port Priority

The port priority is based on switch's physical ports. To config it, click Port Management→ Port Configuration. Note that available values range from 0 to 7. It is used to determine the forwarding sequence of packets not carrying priority identifiers.

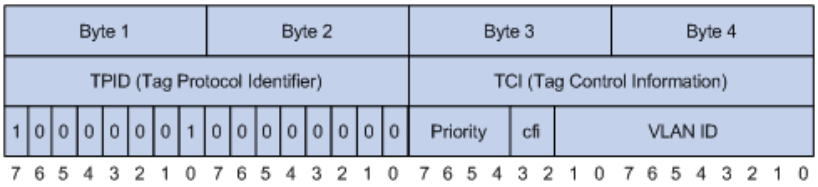
802.1p Priority

The 802.1p priority, contained in the Ethernet header, is used by QoS disciplines to differentiate traffic on layer 2 where analyzing IP header is not necessary. 802.1p priority is available only in an IEEE 802.1Q tagged frame. As seen below, the 4-byte 802.1Q tag contains a 2-byte TPID（Tag Protocol Identifier, value: 0x8100）and a 2-byte TCI（Tag Control Information).



802.1Qtagged Ethernet frame

Below displays a detailed view of an 802.1Q tag. 802.1p priority, also known as class of service (CoS), is contained in the priority field of the TCI. It is made up of 3 bits and with available values ranging from 0 to 7.



802.1QTag

The 802.1P priority tags are mapped to the Switch's priority queues as follows:

802.1P priority	Queue
1, 2	1
0, 3	2
4, 5	3
6, 7	4

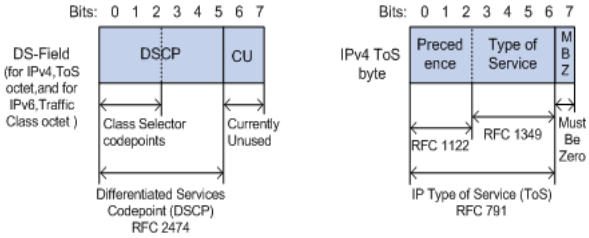
DSCP Priority

The DSCP priority resides in the IP header. The ToS field includes 8 bits, among which:

The first 3 bits denotes the IP priority, with available values ranging from 0 to 7.

Bits 3-6 denotes the ToS priority, with available values ranging from 0 to 15.

The RFC 2474 redefined the IPv4 TOS field as the DS field. The DSCP priority is denoted by the first 6 bits (bits 0～5), with available values ranging from 0 to 63, while the last 2 bits (bits 6-7) are reserved.



DS-field and ToS byte

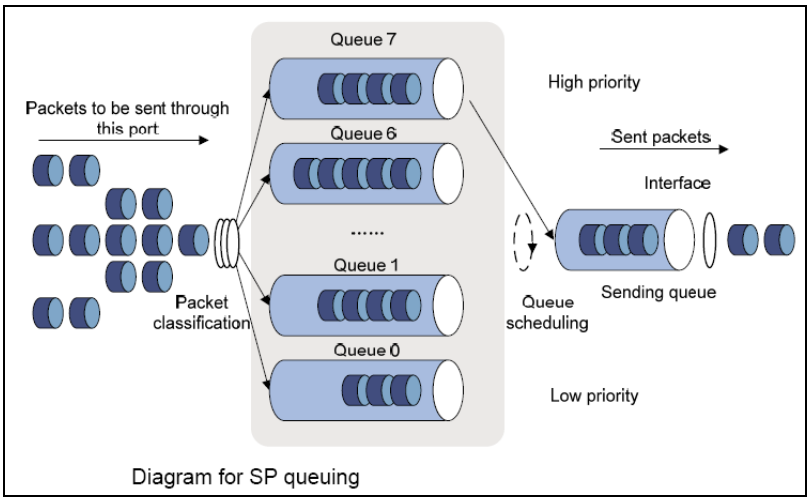
The 802.1P priority tags are mapped to the switch's priority queues as follows:

DSCP Priority	Queue
0～15	1
16～31	2
32～47	3
48～63	4

3. Scheduling Scheme Overview

QoS provides a queue scheduling policy to determine the packet forwarding sequence when congestion occurs. The switch provides two common scheduling techniques to achieve Quality-of-Service (QoS) while using shared resources: SP(Strict-Priority）and WRR (Weighted Round Robin).

Strict Priority Queuing



Strict Priority Queuing is specially designed to meet the demands of critical services or applications. Critical services or applications such as voice are delay-sensitive and thus require to be dequeued and sent first before packets in other queues are dequeued on a congested network. For example, assume that 4 egress queues 3, 2, 1 and 0 with descending priority are configured on a port.

Then under SP algorithm, the port strictly prioritizes packets from higher priority queue over those from lower priority queue. Namely, only after packets in highest priority queue are emptied, can packets in lower priority queue be forwarded. Thus High-priority packets are always processed before those of less priority. Medium-priority packets are always processed before low-priority packets. The lowest priority queue would be serviced only when highest priority queues had no packets buffered.

Disadvantages of SP: The SP queuing gives absolute priority to high-priority packets over low-priority traffic; it should be used with care. The moment a higher priority packet arrived in its queue, however, servicing of the lower priority packets would be interrupted in favor of the higher priority queue or packets will be dropped if the amount of high-priority traffic is too great to be emptied within a short time.

WRR

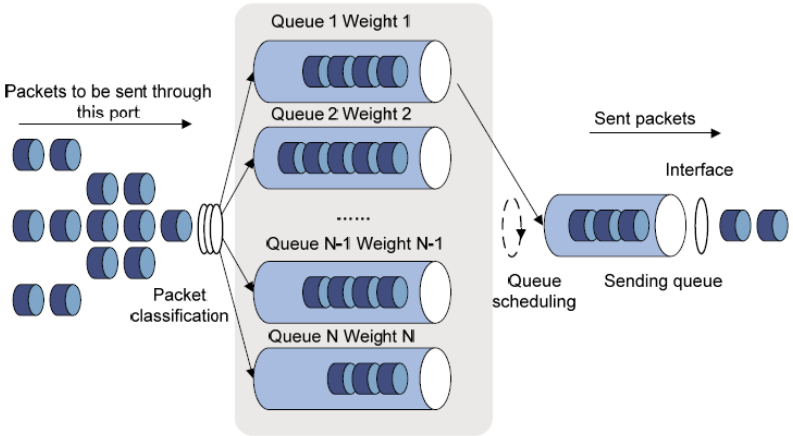


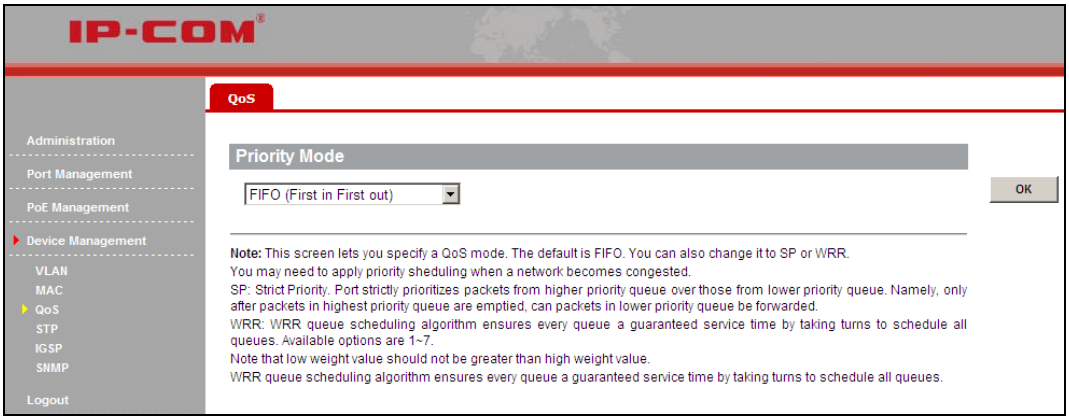
Diagram for WRR Queuing

WRR queue scheduling algorithm ensures every queue a guaranteed service time by taking turns to schedule all queues. Assume there are 4 egress queues on the port. The four weight values (namely, w3, w2, w1, and w0) indicate the proportion of resources assigned to the four queues respectively. On a 100M port, if you set the weight

values of WRR queue-scheduling algorithm to 50, 30, 10 and 10(corresponding to w3, w2, w1, and w0 respectively). Then the queue with the lowest priority can be ensured of, at least, 10 Mbps bandwidth, thus avoiding the disadvantage of SP queue-scheduling algorithm that packets in low-priority queues may not be served during a long time. Another advantage of WRR queue-scheduling algorithm is that though the queues are scheduled in turn, the service time for each queue is not fixed, that is to say, when a queue is emptied, the next queue will be scheduled immediately. Thus, bandwidth resources are fully utilized.

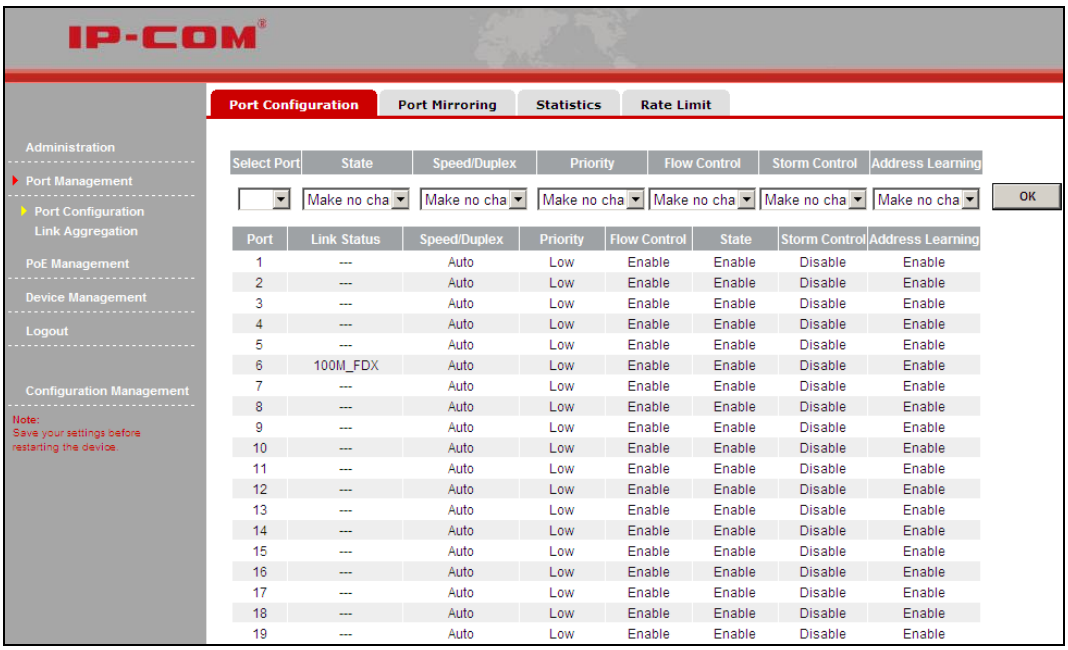
4. QoS Configurations

Click **Device Management** > **QoS** to enter the screen below**.** Here you can select strict priority or FIFO (first in first out). When configuring weight priority values, note that the value indicated by High weight should not be smaller than that indicated by Low weight. Values available for the weight rage from 1 to 7.



Click **OK** to complete the QoS configurations.

Click **Port Management** > **Port Configuration** to enter the port Configuration screen, select a port number and select **High** from the priority drop-down list. The selected port will then be in the high priority queue.



For example: In Strict Priority QoS mode, if you select “high” priority level for port1 and “low” for port2 and the 2 ports transmit packets concurrently to one port, then the receiving port will first forward packets from port1 and

then port2. Depending on configured priority levels, packets from ports with lower priority level are always forwarded only after packets from ports with higher priority level have all been forwarded; However in WRR QoS mode, if you specify weight values: High=7; Low=1, then when the 2 ports simultaneously transmit packets to one port, the receiving port will forward packets according to traffic ratio of 7:1.

3.5.4 STP

1. STP Overview

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. On Ethernet, only a single active path at a time can be maintained between any two network nodes to avoid broadcast storm. However, spare (redundant) links are indispensable to ensure reliability. Spanning tree allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, and disable those that are not part of the spanning tree, leaving a single active path between any two network nodes. This is accomplished in the STP. A STP-enabled switch can perform the following teaks:

Discover and generate an optimum STP topology

Discover and repair failures on the network; automatically update the network topology for future use. Local topology is generated by computing bridge configurations made by a network administrator. Thus, if configured properly, an optimum topology tree can be generated.

2. RSTP Overview

RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this. RSTP was designed to be backwards-compatible with standard STP. RSTP is typically able to respond to changes within 3 × Hello times (default: 3 times 2 seconds) or within a few milliseconds of a physical link failure while STP can take 30 to 50 seconds to respond to a topology change.

RSTP delivers fast transition to forwarding status without relying on timer settings. A RSTP bridge is responsive to other RSTP bridge's link status. The port does not need to wait for the topology to become stable. Edge port and P2P port are introduced to the protocol for faster transition. Below explains what an Edge port and a P2P port is and does.

Edge Port

The edge port is a configurable designation used for a port that is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

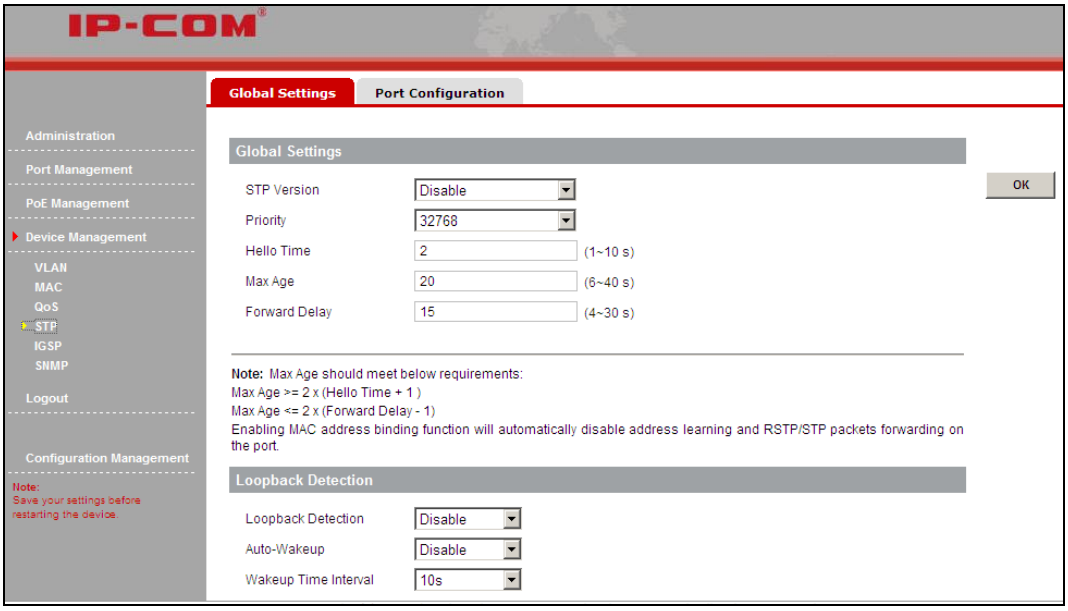
P2P Port

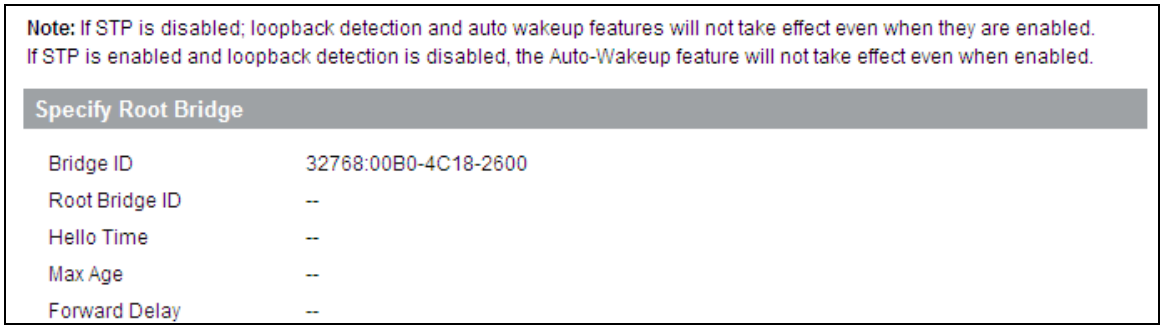
A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP/MSTP, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden

through configuration. The three protocols are mutually compatible and no conflicts or network collapse will be caused in spanning tree application.

3. STP Global Configurations

Click **Device Management** > **STP** > **Global Settings** to enter the screen below where you can configure STP settings and enable/disable loopback detection feature.





Fields on the global setup section are described below:

Field	Description
STP Version	Select the desired version of STP version: RSTP STP to eliminate loops on data link layer. The default RSTP mode is recommended. By default, this option is disabled.
Priority	Bridge priority. Select a bridge priority value from 0～61440. The smaller the number, the higher the priority.
Max Age	The Max Age may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. You may choose a time between 6 and 40 seconds.

Hello time	Configure the Hello Time. The Hello Time indicates the time interval in seconds a STP-enabled port waits to send BPDU messages.
Forward Delay	The Forward Delay Time is the amount of time in seconds a bridge remains in a listening and learning state before forwarding packets. Valid values range from 4 to 30 seconds.

Fields on the Loopback Detection section are described below:

Field	Description
Loopback Detection	With this feature enabled, the switch will be able to detect loops from downlinked devices and put the ports in a status of Active. Loops are confirmed when the port receives BPDU messages it sent. If no loop is detected, port status will not be changed.
Auto-Wakeup	Enable/disable it to allow/disallow blocked ports to forward packets when loop disappears. If enabled, blocked ports will re-enter "Forward" state, meaning that such ports regain the ability to forward packets when the switch detects no current loop during a specified Wakeup Time Interval. However if loop still exists, then such blocked ports will remain in "Blocked" state, meaning that they are still not able to forward packets. If disabled, when the port becomes "Active", you will need to manually enable the port on the port setup screen.
Wakeup Time Interval	When enabled, port in "Discard" status will enter Forwarding status and re-detect network.

Fields displayed on the bridge status section are described below:

Field	Description
Bridge ID	Displays the Bridge ID. The bridge ID consists of priority and MAC Address of the bridge
Root Bridge ID	The ID of the Bridge that is selected as root bridge in spanning tree
Hello Time	Displays the Root Bridge Hello Time
Max Age	Displays the Root Bridge Maximum Age Time
Forward Delay	Displays the Root Bridge Forward Delay Time

Note:

If STP is disabled; loopback detection and Auto-Wakeup features will not take effect even when they are enabled.

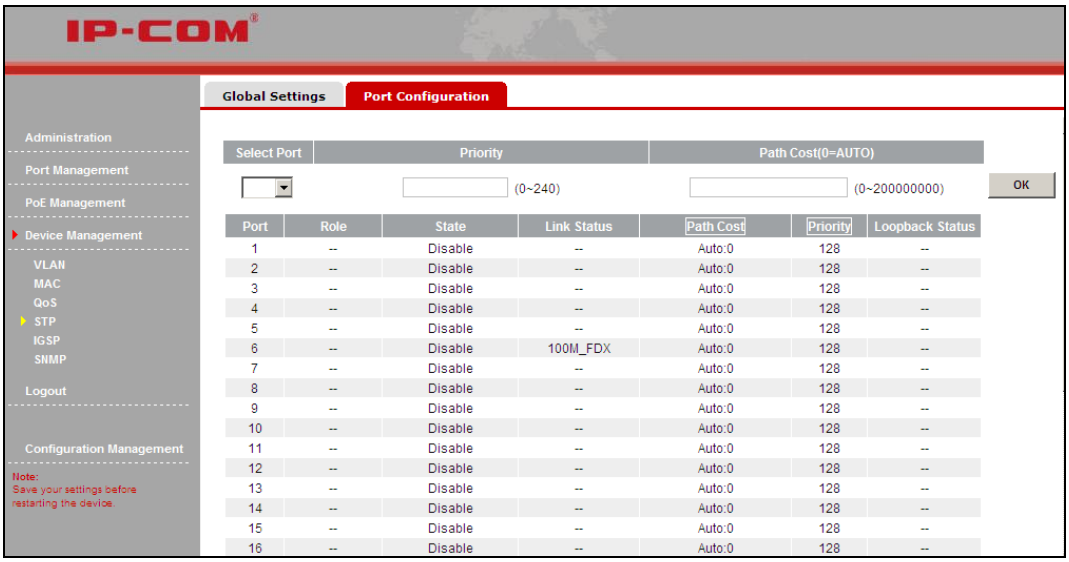
If STP is enabled and loopback detection is disabled, the Auto-Wakeup feature will not take effect even when enabled.

2 x (Forward delay - 1) ≤ Max Age≥ 2 x (Hello Time + 1)

4. STP Port Configurations

Select a port number from corresponding drop-down list and specify priority and path cost for it.

By default, all ports' priority values are set to 128 and path cost complies with 802.1T standard as seen below.



Fields on the screen are described below:

Field	Description
Select Port	Select a port number from 1-26.
Priority	The priority of a port, for differentiating ports with identical path cost. The smaller the value, the higher the priority.
Path Cost	A configurable parameter that can be defined by STP algorithm. The path cost is 2000000 for a 10M net segment and 200000 for a 100M net segment. Valid values range from 0 to 200000000. If 0 is entered, system will automatically negotiate an optimum cost.
Role	Display the role that a port plays in spanning tree: Designated, Backup, --, Root
State	Display port status: Blocking, Disable, Learning, Forwarding
Link Status	Display port link status: --, speed+ duplex mode
Downlink Loopback Status	Display "Active" when detecting loopback from downlinked devices otherwise display "--".

3.5.5 IGMP Snooping

1. IGMP Snooping Overview

IGMP snooping is the process of listening to Internet Group Management Protocol (IGMP) network traffic. IGMP snooping, as implied by the name, is a feature that allows a network switch to listen in on the IGMP conversation between hosts and routers.

Principle of IGMP snooping

By listening to the conversations between hosts and routers, the switch maintains a map of which links need which IP multicast streams. Multicast streams may be filtered from the links which do not solicit them. An IGMP-Snooping-disabled layer-2 device will flood multicast traffic to all the ports in a broadcast domain (or the VLAN equivalent). With IGMP snooping enabled, known multicast traffic will be forwarded to hosts that have explicitly joined the group. It provides switches with a mechanism to prune multicast traffic from links that do not contain a multicast listener (an IGMP client).

How IGMP Snooping Works

A switch that runs IGMP snooping performs different actions when receiving different IGMP messages.

When receiving a general query

The IGMP querier periodically sends IGMP general queries to all hosts and routers on the local subnet to determine which active multicast group members exist on the subnet. After receiving an IGMP general query, the switch forwards it through all ports in the VLAN (except the port that received the query) and performs corresponding actions on the receiving port (resets/enables the age timer).

When receiving a membership report

A host sends an IGMP membership report to the multicast router in the following circumstances:

After receiving an IGMP query, a multicast group member host responds with an IGMP membership report.

When intended to join a multicast group, a host sends an IGMP membership report to the multicast router to announce that it wants to join the multicast group. After receiving an IGMP membership report, the switch forwards it through all the router ports in the VLAN, resolves the address of the reported multicast group and performs corresponding actions on the receiving port (resets/enables the age timer). A switch does not forward an IGMP membership report through a non-router port.

When receiving a leave message

When an IGMPv1 host leaves a multicast group, the host does not send an IGMP leave message, so the switch cannot know immediately that the host has left the multicast group. However, as the aging timer on the member port that corresponds to the host expires, the the switch immediately deletes its forwarding entry from the forwarding table.

When an IGMPv2 or IGMPv3 host leaves a multicast group, it sends an IGMP leave message to the multicast router to inform of such leave.

When receiving an IGMP leave message from the last member port, the switch forwards it through all router ports in the VLAN and resets the aging timer on the receiving port (the port that received the IGMP leave message) instead of immediately deleting its corresponding forwarding entry from the forwarding table as it cannot know whether there are still other members of that multicast group attached to such port.

After receiving the IGMP leave message from a host, the IGMP querier resolves the multicast group address in the message and sends an IGMP group-specific query to that multicast group through the port that received the leave message. After receiving the IGMP group-specific query, the switch forwards it through all its router ports in the VLAN and all member ports for that multicast group.

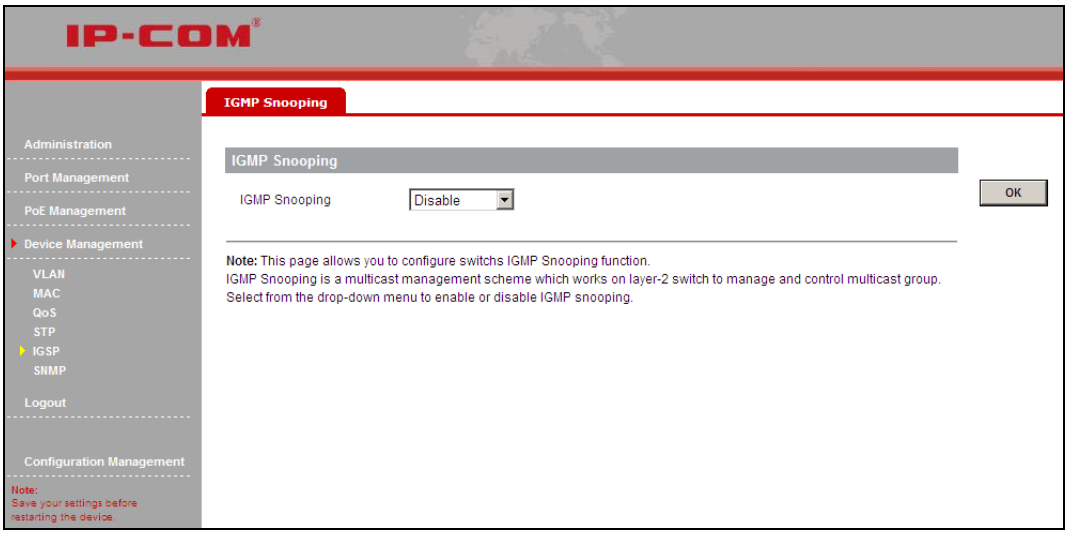
The switch also performs the following actions on the port that received the IGMP leave message: If the port receives any IGMP membership report in response to the group-specific query before the aging timer expires, the switch considers that some host attached to the port is receiving or expecting to receive multicast data from that multicast group and will reset the aging timer on the port.

If the port receives no IGMP membership report in response to the group-specific query before its aging timer expires, the switch considers that no hosts attached to the port are still members of that multicast group address and thus removes the multicast forwarding entry that the port corresponds to from the forwarding table when the aging timer expires.

2. IGMP Snooping Configurations

Click **Device Management >IGMP > IGMP Snooping** to enter the screen below.

To enable the IGMP Snooping feature, simply select **Enable** and then click **OK**.



3.5.6 SNMP

1. SNMP Overview

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the switch, switch group or network.

SNMP, using polling scheme, is suitable for use in small sized network environment demanding high speed and low cost. SNMP, implemented through the connectionless UDP, can seamlessly interoperate with multiple devices.

SNMP Work Mechanism

The SNMP framework comprises NMS and Agent:

NMS—Network Management Station NMS, is a station that runs the SNMP client software to monitor and manage the SNMP-capable devices in the network.

SNMP agent—Works on a managed network device (such a switch) to receive and handle requests from the NMS, and send traps to the NMS when some events occur.

Upon receiving GetRequest, GetNextRequest and SetRequest packets from NMS, the SNMP agent will perform Read or Write operations on managed objects depending on the type of packets received and generate Response packets to return to NMS.

2. SNMP Version

The switch supports SNMPv1 and SNMPv2c, both of which use community names for authentication. SNMP packets with community names that did not pass the authentication on the device will simply be discarded. The SNMP community name defines the relationship between an SNMP NMS and an SNMP Agent. A community name plays a similar role as a key/password and can be used to regulate access from NMS to Agent.

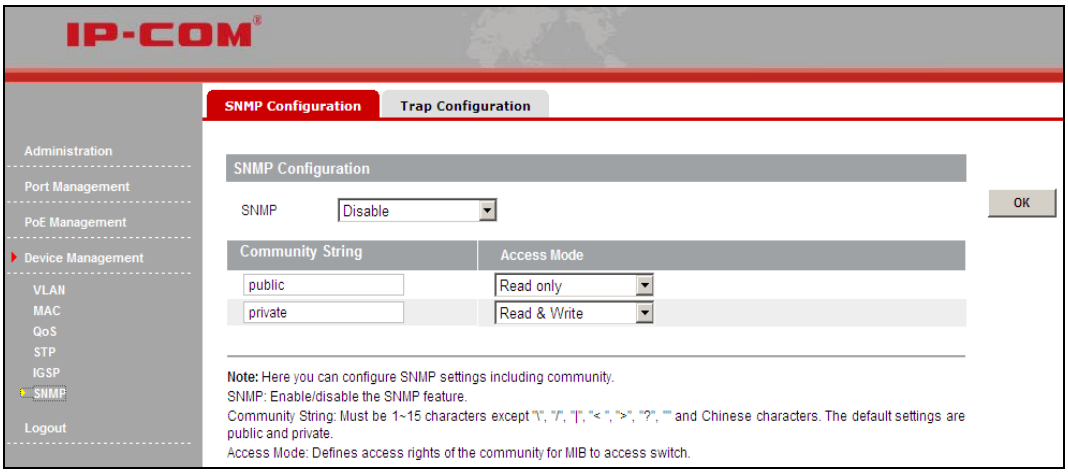
Trap

Traps are messages that alert network personnel of events that occur on the switch. The events can be as serious as a reboot (someone accidentally turned OFF the switch), or less serious like a port status change. The switch generates traps and sends them to the trap recipient (or network manager).

2. SNMP Configuration

To enter the screen below, click **Device Management** > **SNMP**.

Here you can enable/disable the SNMP feature, configure community name and access mode: read or write.



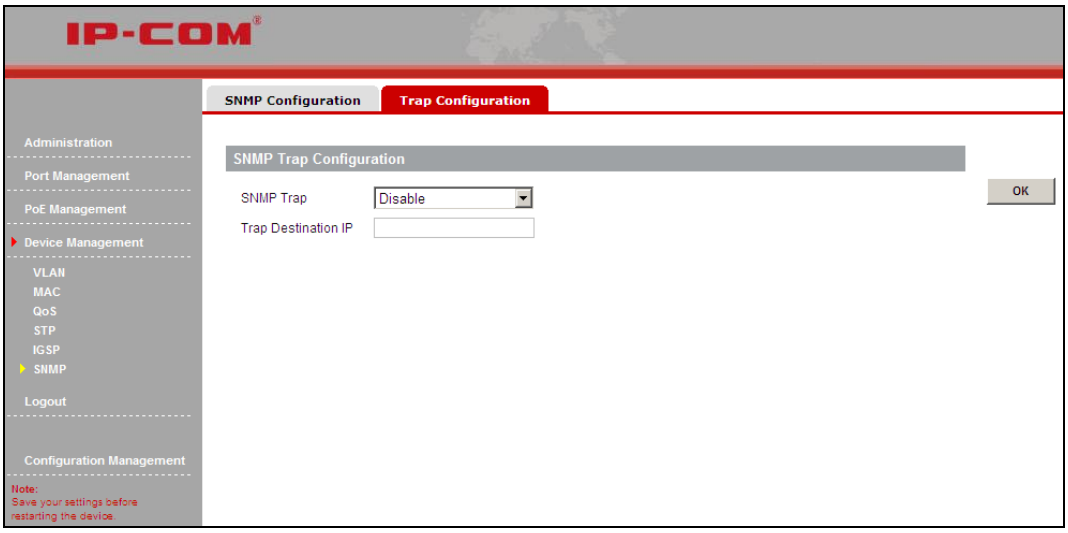
Fields on the screen are described below:

Field	Description
SNMP	Enable/disable the SNMP feature. By default it is disabled.
Community String	Used to define the relationship between SNMP manager and SNMP Agent, similarly to the function of a password, granting the SNMP manager access to SNMP Agent on the switch. By default, there are 2 community strings: public and private. Note: Up to 15 characters are allowed for each community string.
Access Mode	Defines Read/Write or Read Only right for MIB to access switch through community name.

3. Trap Configuration

Click **Device Management** > **SNMP** > **Trap Configuration** to enter the screen below.

Here you can specify the destination IP address that trap messages are to be sent.

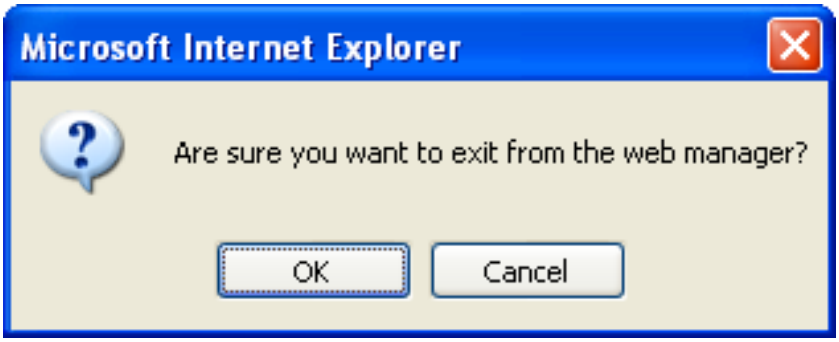


Fields on the screen are described below:

Field	Description
SNMP Trap	Trap is used to report urgent and important events (for example, a managed device is rebooted.). This option is disabled by default
Trap Destination IP	Enter a destination IP address to which switch's trap message is to be sent. Trap message will not be sent if the Trap destination IP address is invalid. The trap destination IP address should only indicate a single host.

3.6 Logout

This section allows you to exit from the switch's web manager safely.



3.7 Configuration Management

Configurations on switch will be lost if they are not saved before switch reboots. So do save them on this screen before you reboot the switch.

1. Save current settings

Use this feature to save device current configurations to ensure you will still have them on the switch even after device restarts.

Note:

It takes about 10 seconds to save device current configurations. Do NOT operate or interrupt the switch during this period. Otherwise parts of the configurations may be lost. When the page refreshes, the action of saving configurations is completed.

2. Backup settings

Once you have configured the device the way you want, you can save all settings to your local hard drive, which can later be imported to the device in case that it is restored to factory default settings.

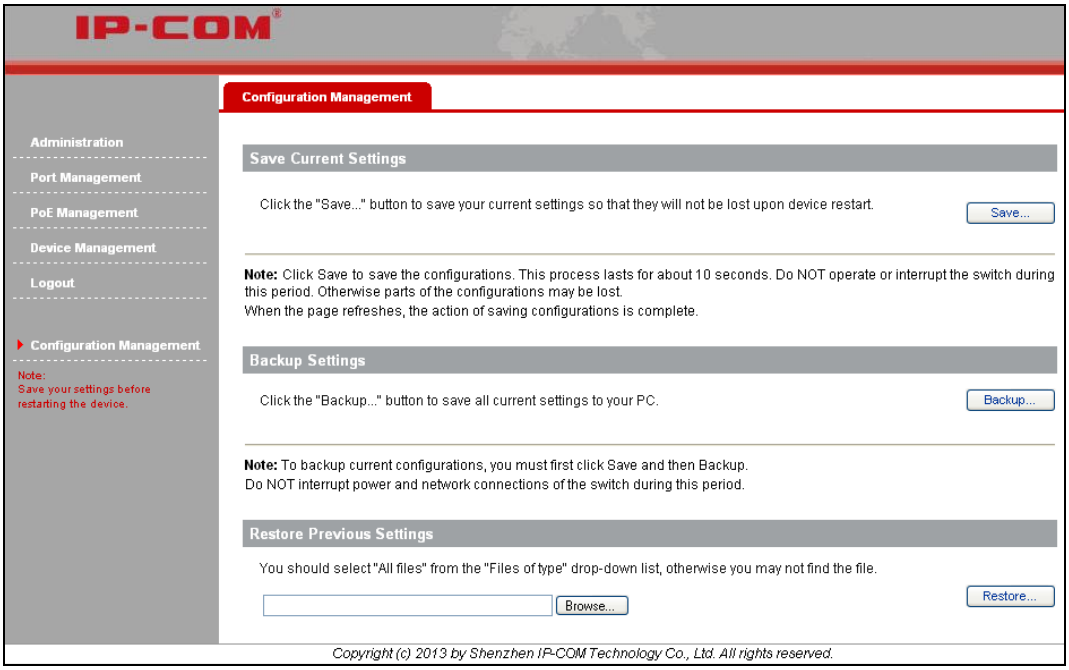
To back up current settings, click the Backup button.

Note:

To backup current settings, you must first click Save to save them. Do NOT disconnect the device from power supply and the management PC during this process.

3. Restore previous settings from local hard drive

To restore settings that are previously saved on your local hard drive, click the Browse button to locate and select the file and then click the Restore button.



Chapter 4 Useful Commands

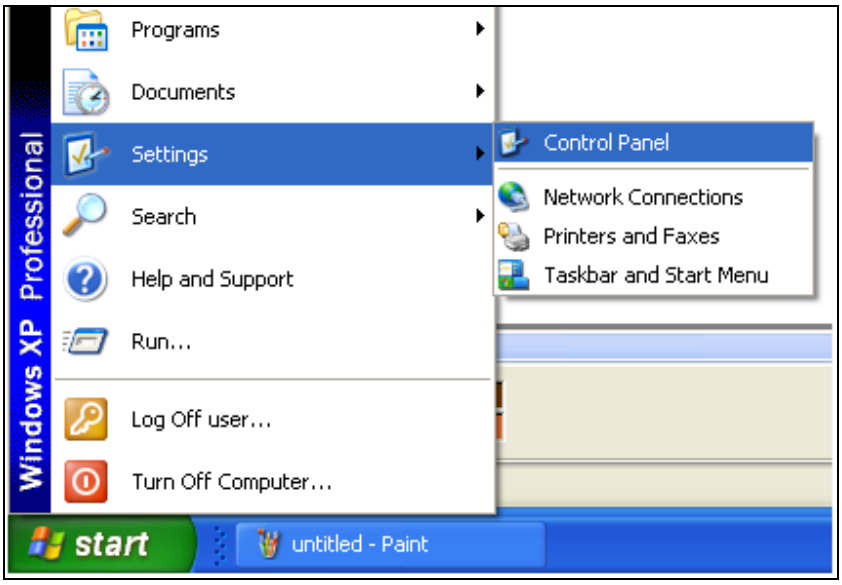
Command	Description
cmd	In computing, a command is a directive to a computer program acting as an interpreter of some kind, in order to perform a specific task.
Ipconfig/all	Ipconfig/all (internet protocol configuration) in Microsoft Windows is a console application that displays all current TCP/IP network configuration values and NIC MAC addresses.
ping	Ping is a computer network administration utility used to test the reachability of a host on an Internet Protocol (IP) network and to measure the round-trip time for messages sent from the originating host to a destination computer.
arp –d	Removes arp information from network devices
arp -a	Displays arp information from network devices

Chapter 5 TCP/IP Setup

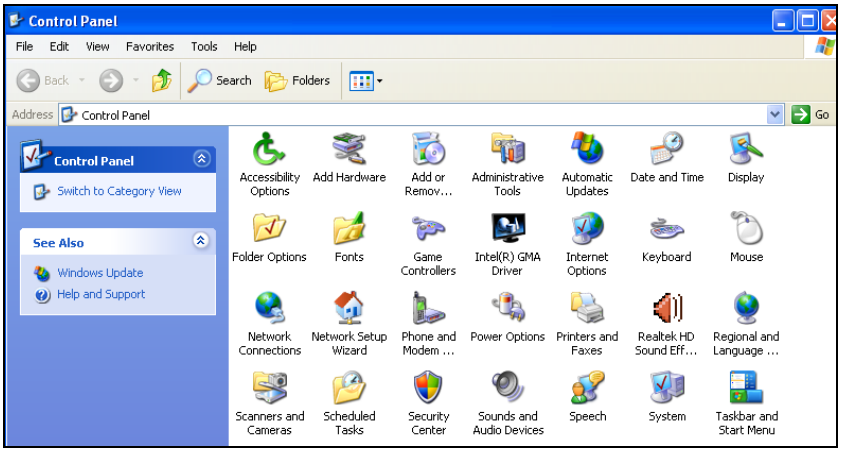
This section presents you how to configure your PC's TCP/IP settings in Windows XP. Before you start, make sure your PC has an installed NIC. If not, please install one first.

Follow steps below:

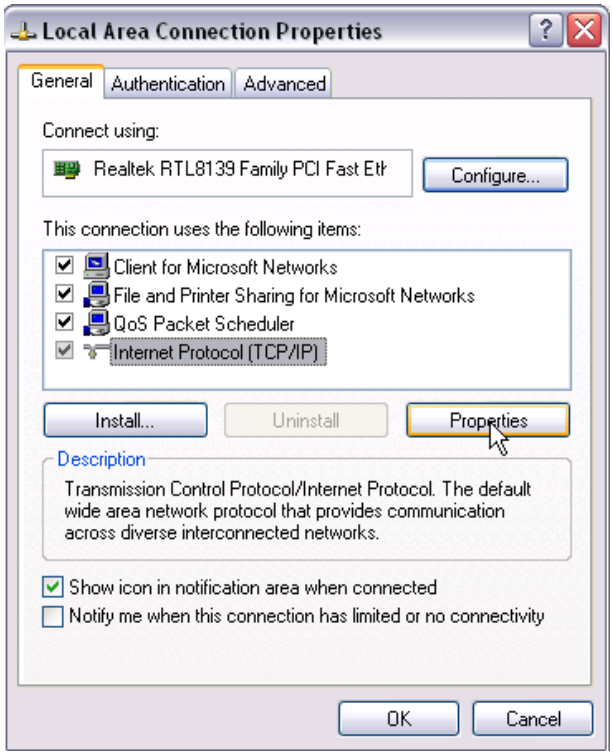
1. Click **Start** > **Settings** > **Control Panel**.



2. Click **Network Connections**.



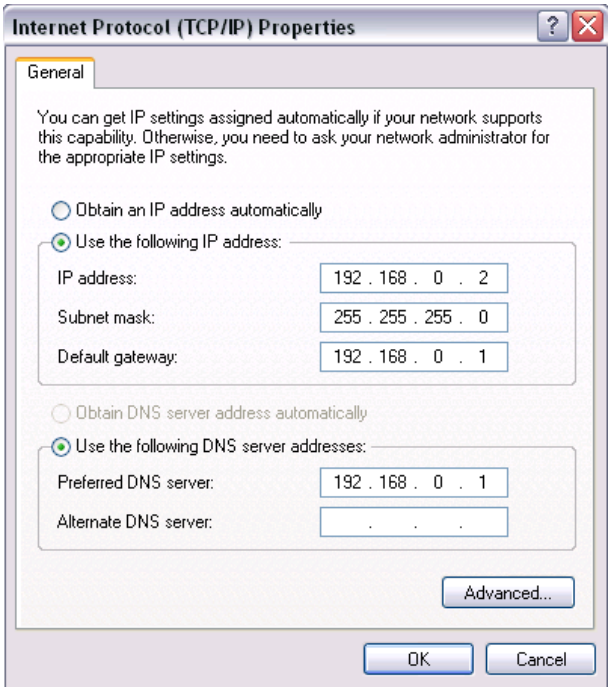
3. Right click **Local Area Connection**, click **Properties**, select **Internet Protocol (TCP/IP)** on the appearing window and then click **Properties**.



4. Select **Use the following IP address** and configure as below:

IP address: 192.168.0.x (where x can be any number between 2~254)

Subnet Mask: 255.255.255.0.



5. Click **OK** twice to exit.

Appendix Regulatory Compliance Information

CE Mark Warning

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures. This device complies with EU 1999/5/EC.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable.

FCC Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment.

Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

NOTE: (1) The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. (2) To avoid unnecessary radiation interference, it is recommended to use a shielded RJ45 cable

Disclaimer: This equipment is an industry class product instead of an end-user device. It may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio communications, which can be determined by turning the equipment off and on, the user may need to take some measures to correct the interference.