

# LUXUL

*Simply Connected*

## User Guide

### XMS-1024 Luxul Xen™ Gigabit Ethernet Smart Switch



#### Use the XMS-1024 to:

- ▶ Provide Intuitive Network Management and Optimization Capabilities
- ▶ Expand Your Home or Office 10/100/1000 Ethernet Network
- ▶ Future Proof Your Network with Gigabit Speeds (10X Performance of Fast Ethernet)
- ▶ dOptimize and Protect Your Network with Advanced VLAN, QoS and Network Security Features

[luxul.com](http://luxul.com)

## GIGABIT ETHERNET SMART SWITCH

### MODEL NUMBER: XMS-1024

#### USER GUIDE

© 2011 Luxul. All Rights Reserved.

No part of this publication may be modified or adapted in any way, for any purposes without permission in writing from Luxul. The material in this manual is subject to change without notice. Luxul reserves the right to make changes to any product to improve reliability, function, or design. No license is granted, either expressly or by implication or otherwise under any Luxul intellectual property rights. An implied license only exists for equipment, circuits and subsystems contained in this or any Luxul product.

## DOCUMENT CONVENTIONS

The following graphical alerts are used in this document to indicate notable situations:



**NOTE:** Tips, hints, or special requirements that you should take note of.



**CAUTION:** Care is required. Disregarding a caution can result in data loss or equipment malfunction.



**WARNING!:** Indicates a condition or procedure that could result in personal injury or equipment damage.

## CONTENTS

<b>1: PRODUCT OVERVIEW</b>	<b>4</b>
1.1 Product Introduction	4
1.2 Product Features	4
1.3 Product Specifications	5
1.4 Package Contents	7

<b>2: HARDWARE DESCRIPTION</b>	<b>7</b>
2.1 Front Panel	7
2.2 LED Indicators	8
2.3 Rear Panel	9
<b>3. PREPARING FOR INSTALLATION</b>	<b>9</b>
3.1 System Requirements	9
3.2 Before Connecting to the Network	9
<b>4: XMS-1024 INSTALLATION</b>	<b>10</b>
4.1 Installing the XMS-1024 in a Rack	10
4.2 Desktop Setup	10
4.3 Network Connections:	11
4.4 Default IP Address	11
<b>CHAPTER:5 CONFIGURATION</b>	<b>12</b>
5.1 Login	12
5.2 Status	13
5.3 Port Settings	14
5.4 Mirror	18
5.5 VLAN	18
5.6 Trunk	22
5.7 QoS	23
5.8 MAC Settings	24
5.9 802.1X	25
5.10 RSTP	27
5.11 IGMP Snooping	30
5.12 System	31
<b>6: REGULATORY COMPLIANCE</b>	<b>36</b>
6.1 Health and Safety Recommendations	36
6.2 FCC Statement:	37
<b>7: CONTACT LUXUL</b>	<b>37</b>
<b>APPENDIX 1: COMMON COMMANDS</b>	<b>38</b>
<b>APPENDIX 2: TCP/IP ADDRESS SETTING (WINDOWS XP)</b>	<b>38</b>
<b>GLOSSERY</b>	<b>40</b>

## 1: PRODUCT OVERVIEW

### 1.1 Product Introduction

Congratulations on your purchase of the Luxul XMS-1024 Gigabit Ethernet Smart Switch, featuring XenSmart™ network management. The XenSmart management interface provides a powerful, yet simple method for setting up and optimizing an intelligent home or office network. The XMS-1024 features powerful network optimization capabilities, including extensive support for port management, port security, Quality of Service (QoS), VLAN configuration and port trunking. Other features such as 802.1X authentication, Rapid Spanning Tree Protocol (RSTP), IGMP Snooping, static MAC address table, and port traffic statistics further enable a robust, powerful network environment. The XMS-1024 provides 24 10/100/1000 Mbps RJ-45 ports and 2 shared SFP optical module expansion ports. The SFP ports can be used as uplinks for extending the network between switches or for long range communications and extensions. Optical fiber can be used to efficiently deliver data at distances of up to 49 miles as opposed to the 300 foot limitation of standard twisted pair Ethernet.

### 1.2 Product Features

- ▶ Complies with IEEE802.3, IEEE802.3u, IEEE802.3ab and IEEE802.3z Ethernet standards.
- ▶ 24 10/100/1000 Mbps RJ-45 ports, and supports Auto MDI/ MDIX
- ▶ 2 shared SFP optical module expansion ports—automatic switchover between Gigabit electrical interface and Gigabit SFP optical interface
- ▶ IEEE802.3x full-duplex flow control and half-duplex backpressure flow control
- ▶ Store-and-forward switching
- ▶ 48Gbps backplane bandwidth, supporting non-blocking line speed transfer
- ▶ Supports up to 24 groups of port-based VLANs and up to 128 groups of tagged VLANs based on IEEE 802.1Q, with VLAN IDs ranging 1 - 4094
- ▶ IEEE 802.3ad port trunk support provides 8 trunking groups, each of which can contain up to 12 port members
- ▶ 8K MAC address table; Supports up to 128 static MAC address entries
- ▶ QoS functions: Mapping mode by port, IEEE802.1p, and TOS priorities. Automatic control for the transfer queue based on 4 priorities
- ▶ Provides control over port access security, including port MAC address filtering, binding and aging
- ▶ XenConnect “Plug and Play” Compatibility

- ▶ Intelligent control of broadcast storms, and provides options for targeting broadcast type and broadcast control
- ▶ Port mirroring
- ▶ 802.1X authentication support
- ▶ Compatible with 802.1D Spanning Tree Protocol (STP) and supports 802.1W Rapid Spanning Tree Protocol (RSTP)
- ▶ IGMP Snooping
- ▶ Set the switch IP address using a static IP address or by enabling the DHCP client mode
- ▶ XenSmart™ Web management
- ▶ SNMP management
- ▶ Support for downloadable pre-optimized configuration options
- ▶ Simple update, backup and restoration of switch configuration files
- ▶ Traffic statistics and dynamic display of packet receive/transfer statistics by port
- ▶ 1U steel chassis for standard 19-inch rack installation

### 1.3 Product Specifications

<b>Standards</b>	<ul style="list-style-type: none"> <li>▶ IEEE 802.3 10Base-T Ethernet</li> <li>▶ IEEE 802.3u 100Base-TX Fast Ethernet</li> <li>▶ IEEE 802.3 NWay Auto-negotiation</li> <li>▶ IEEE 802.3x Flow Control</li> <li>▶ TCP/IP</li> <li>▶ PPPoE</li> <li>▶ DHCP</li> <li>▶ SNMP</li> <li>▶ DNS</li> <li>▶ ICMP</li> <li>▶ NAT</li> <li>▶ HTTP</li> <li>▶ ARP</li> </ul>
<b>Features</b>	<ul style="list-style-type: none"> <li>▶ Number of Ports: 24 10/100/1000BASE-T; 2 Combo 10/100/1000BASE-T/SFP</li> <li>▶ MAC Address Table: 8K</li> <li>▶ Switch Fabric: 48Gbps</li> <li>▶ Transmission Method: Store-and-forward</li> <li>▶ Auto uplink (MDI/MDI-X) detection and configuration</li> <li>▶ IGMP Snooping</li> <li>▶ Loopback Detection: Auto disable when loop is detected</li> <li>▶ Port Mirroring: one-to-one, many-to-one, mirroring for Tx/Rx/Both</li> </ul>

<b>VLAN</b>	<ul style="list-style-type: none"> <li>▶ 802.1Q max 4094 VIDs</li> <li>▶ Port Based VLAN</li> <li>▶ Supports 1 Management VLAN</li> </ul>
<b>Quality of Service (QoS)</b>	<ul style="list-style-type: none"> <li>▶ 4 Queues per port</li> <li>▶ Queue handling: Strict, Weighted Round Robin (WRR)</li> <li>▶ CoS based on DCSP, 802.1P and Port Based Priority Queues</li> <li>▶ Port based bandwidth control</li> </ul>
<b>Access Control List</b>	<ul style="list-style-type: none"> <li>▶ Maximum profiles: 50</li> <li>▶ Maximum rules shared by profiles: 240</li> <li>▶ ACL based on MAC address, IPv4 Address, VLAN ID, 802.1p Priority, DSCP</li> <li>▶ ACL actions: permit, deny</li> </ul>
<b>Security</b>	<ul style="list-style-type: none"> <li>▶ 802.1X Port Based Access Control: Default forwarding</li> <li>▶ Port Security: Supports up to 64 MAC addresses per port</li> <li>▶ Traffic Control: Broadcast/multicast/unicast storm control</li> <li>▶ Static MAC: Supports 256 Static MAC entries</li> </ul>
<b>Management</b>	<ul style="list-style-type: none"> <li>▶ Web Based GUI</li> <li>▶ System Log: Max 500 log entries</li> </ul>
<b>Network Data Transfer Rate</b>	<ul style="list-style-type: none"> <li>▶ Ethernet: 10Mbps (Half-duplex)</li> <li>▶ Ethernet: 20Mbps (Full-duplex)</li> <li>▶ Fast Ethernet: 100Mbps (Half-duplex)</li> <li>▶ Fast Ethernet: 200Mbps (Full-duplex)</li> <li>▶ Gigabit Ethernet: 1000Mbps (Half-duplex)</li> <li>▶ Gigabit Ethernet: 2000Mbps (Full-duplex)</li> </ul>
<b>Interface Options</b>	<ul style="list-style-type: none"> <li>▶ RJ-45: <ul style="list-style-type: none"> <li>▶ 10 Base-T: Cat.5 UTP /STP</li> <li>▶ 100 Base-TX: Cat.5 UTP /STP</li> <li>▶ 1000Base-T: Cat.5, Cat.5e or Cat.6 UTP/STP</li> </ul> </li> <li>▶ Cable Recognition for Straight-through or Crossover Cables</li> </ul>
<b>Certifications</b>	FCC Class A, CE, RoHS
<b>Led</b>	<ul style="list-style-type: none"> <li>▶ Per Unit: Power</li> <li>▶ Per Port: Link/Activity</li> </ul>
<b>Power Consumption</b>	27.5 Watts Maximum
<b>Power Supply</b>	Internal Switched Power, AC100-240V, 50-60Hz input
<b>Operating Temperature</b>	32°F to 104°F (0°C to 40°C)
<b>Operating Humidity</b>	10% to 90% (Non-condensing)
<b>Dimensions</b>	W: 17.3" x D: 8.3" x H: 1.7" (W: 439.5mm x D: 211mm x H: 43.2mm)
<b>Weight</b>	<ul style="list-style-type: none"> <li>▶ Item: 6.5 lbs (2.95Kg)</li> <li>▶ Packaging: 8 lbs (3.63Kg)</li> </ul>

## 1.4 Package Contents

The following items should be included in the box:

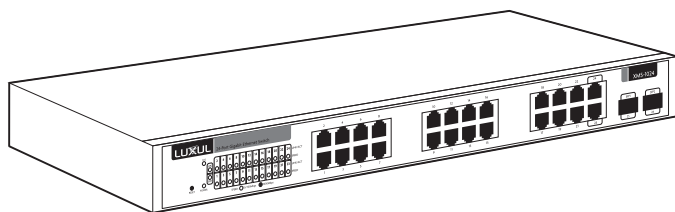
- ▶ XMS-1024 Gigabit Ethernet Smart Switch
- ▶ Power Cord
- ▶ Two L-shaped rack mounting brackets and screws
- ▶ Four rubber pads
- ▶ Quick Installation Guide
- ▶ CD-ROM with User Documentation

If any of the listed items are missing or damaged, please contact the reseller from whom you purchased for return/replacement.

## 2: HARDWARE DESCRIPTION

### 2.1 Front Panel

The front panel of the XMS-1024 switch includes 24 1000Mbps RJ45 and 2 SFP expansion ports on the right side and LED indicators on the left side. Each 1000Mbps port has one Link/Activity LED and one 1000Mbps LED, there are also two SFP LEDs, one Power LED, one System LED and a factory reset button.



#### *XMS-1024 Front Panel View*

- ▶ **Factory Reset Button:** Used to restore factory default settings.
  - ▶ **To reset to factory defaults,** press and hold the reset button until the SYS LED turns off, approx. 5 seconds. A factory reset may take approximately a minute to complete. A successful Factory Reset is indicated by the Port LED lights scrolling once from left to right. When the SYS LED turns on the unit is ready.



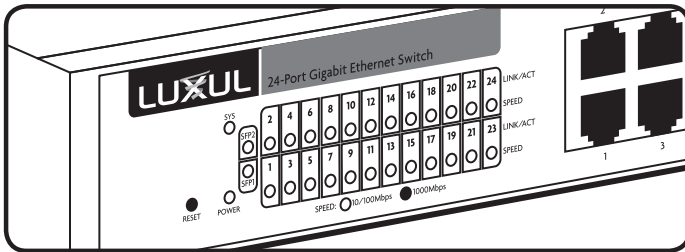
**NOTE:** To hard reset the router use the power switch. Turn the router off, wait 5 seconds and turn the unit back on.



**CAUTION:** Resetting the XMS-1024 to factory defaults will remove all custom settings.

## 2.2 LED Indicators

Each port has one numbered Link/Activity LED and one 1000 Mbps LED. The SFP interface shares the LED indicators with the corresponding Ethernet Port. In addition, there is one System LED and one Power LED, as well as a Reset button to reboot the device or restore factory default settings.



### LED Indicators

The green LED indicators show the working status of the switch. The following table describes the LED functionality:

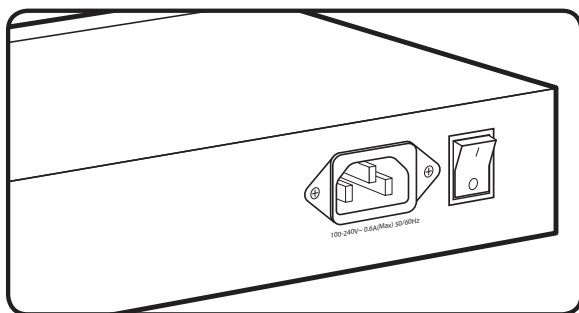
Indicator Name	Description	
Power	On	This LED indicates that there is power to the XMS-1024
	Off	If LED is off, check power & connections and on/off switch at the back of the unit.
Link/Act	On	The Link/Activity LED of the port will be on if there is a device connected to the port.
	Flashing	The Link/Activity LED flashes when a port is receiving or transmitting data.
	Off	There is nothing connected to the port.
1000 Mbps	On	The 1000 Mbps LED will come on if a device capable of 1000Mbps is connected to the port.
	Off	If a port has no device connected or it is not a 1000 Mbps capable device, the 1000 Mbps LED will be off.

SYS	On	Indicates that the XMS-1024 is running normally.
	Flashing	Indicates that the XMS-1024 is restoring default settings.
	Off	Indicates that the XMS-1024 is in startup and initialization process or is not on.

At startup, port LEDs will flash for 1 second as a self test.

When an SFP optical interface is in use, the 1000 Mbps LED and the Link/Activity LED of the corresponding Ethernet port are both on to indicate the SFP status.

## 2.3 Rear Panel



*XMS-1024 Rear Panel View*

**Power Input:** Please use the included power cable

## 3. PREPARING FOR INSTALLATION

### 3.1 System Requirements

- ▶ **Ethernet Cables** to connect the XMS-1024 to Ethernet enabled devices
- ▶ **Computer** equipped with a Web browser. Supported Web browser versions include Microsoft IE 6.0 and up, Safari 1.0 and up or Mozilla Firefox 1.0 and up. The Web browser is used to configure the XMS-1024.
- ▶ **Power** must be AC 100-240V~ 0.6A(Max) 50/60Hz.

### 3.2 Before Connecting to the Network

The XMS-1024 can be rack-mounted or used as a desktop switch. Before connecting to the network, please be aware of the following requirements:

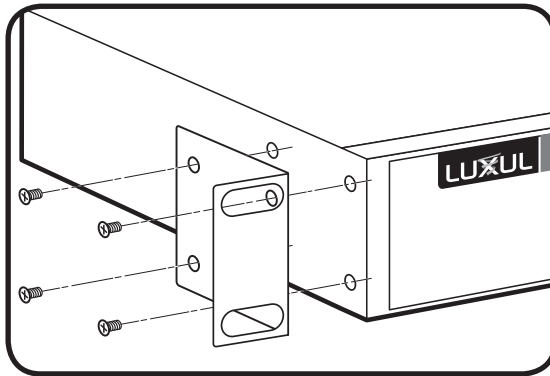
- ▶ Install the XMS-1024 in a stable/safe place to avoid any possible damage

- ▶ Make sure there is adequate space around the XMS-1024 for adequate ventilation and proper heat dissipation. It is recommended to have at least 4-6 inches around all sides.
- ▶ Do not place heavy articles on the XMS-1024.
- ▶ Power outlets should be within 5 feet of the XMS-1024.
- ▶ Verify the ground connection of the outlet is functioning properly.
- ▶ Check the power cord to confirm a secure connection.
- ▶ Avoid placement in direct sunlight.
- ▶ When installing the XMS-1024 on a flat surface, attach the rubber feet to the bottom of the device to avoid scratching the surface.

## 4: XMS-1024 INSTALLATION

### 4.1 Installing the XMS-1024 in a Rack

The XMS-1024 can easily be installed in a standard 19" rack. The XMS-1024 includes two mounting ears for installing and stabilizing the switch. For attaching the mounting ears and installing the switch within a rack, please refer to the following illustration:

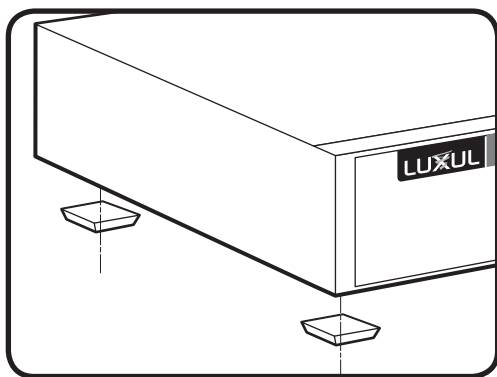


#### *Rack-Mounting the XMS-1024*

- ▶ Using the included screws, attach the mounting ears to each side of the switch.
- ▶ Mount the switch in the rack with the LEDs facing outwards. Be sure the switch is level and properly secured within the rack.

### 4.2 Desktop Setup

For use as a desktop device, position and apply the included rubber feet to the bottom of the XMS-1024.



### *Attaching the Rubber Feet to the XMS-1024*

#### **4.3 Network Connections:**

The XMS-1024 supports 10/100/1000 Mbps Ethernet; 10/100 Mbps half/full-duplex mode and 1000 Mbps full-duplex mode. All RJ-45 ports support Auto MDI/MDIX and can be used as ordinary ports or as Uplink ports. Any RJ-45 port can be used to connect the XMS-1024 to an Ethernet enabled device (including servers, routers, and other switches) without a crossover cable.

The XMS-1024 offers 2 shared SFP optical module expansion ports. Once the Gigabit SFP optical modules are inserted, these interfaces can support optical fiber cables to extend the Gigabit network up to 49 miles—enabling the network to extend beyond the 300 foot limitation of twisted pair Ethernet.

For the RJ-45 ports, Category-5, super Category-5 or Category-6 unshielded twisted pair (CAT5/CAT5e/CAT6 UTP) should be used. For best results, it is recommended that Category-6 shielded twisted pair be used to ensure stable data transmission at 1000 Mbps.

Optical fiber/cable should be selected based on the wavelength of the SFP optical module to be used.

Make sure only one Uplink channel exists between switches or between the XMS-1024 and a router. Otherwise, loops can occur and result in network failure.

#### **4.4 Default IP Address**

The XMS-1024 default IP address is 192.168.0.2. This address can be changed. However, for hassle free installation of other XenConnect™ plug and play Luxul devices, it is recommended that the default IP value be maintained.

## CHAPTER:5 CONFIGURATION

This section introduces the configuration of the XMS-1024 Gigabit Ethernet Smart Switch functions via the XenSmart™ Web-based management interface.

- ▶ **5.1 Login**
- ▶ **5.2 Status**
- ▶ **5.3 Port Settings**
- ▶ **5.4 Mirror**
- ▶ **5.5 VLAN**
- ▶ **5.6 Trunk**
- ▶ **5.7 QoS**
- ▶ **5.8 Mac Settings**
- ▶ **5.9 802.1X**
- ▶ **5.10 RSTP**
- ▶ **5.11 IGMP Snooping**
- ▶ **5.12 System**

### 5.1 Login

The XMS-1024 is not equipped with internal DHCP server. However, if your switch is connected to the the XBR-2300 Enterprise Dual-WAN Router, configuration will be automatic. Otherwise, the IP address of the computer for login and configuration will need to be manually configured. The table below lists the default parameters of the XMS-1024.

Parameter:	Default Value
Default IP address:	192.168.0.3
Default user name:	admin
Default password:	admin

#### Login to the switch with the following steps:

1. Plug an Ethernet cable into any of the ports of the switch
2. Plug the other end into the Ethernet port of your computer
3. Power on the switch
4. Check to see that the IP address of the computer is within this network segment: 192.168.0.xxx (“xxx” ranges 100-254). For example, 192.168.0.100. For IP address settings, refer to Appendix 3.
5. Open the Web browser, and enter 192.168.0.2. The switch login window appears, as shown below.
6. Enter the user name and password (default user name and default password are both set as “admin”), and then click “OK” to login to the switch configuration window.

Switch IP: 192.168.0.2

LUXUL 24-Port Gigabit Ethernet Smart Switch

Username:

Password:

## 5.2 Status

### Status

Hardware Version	V2.0
Firmware Version	V2.1
DHCP Client	Disable
VLAN Mode	802.1q Vlan
IP Address	192.168.0.2
Subnet Mask	255.255.255.0
Gateway	192.168.0.1
MAC Address	c8-3a-35-e0-00-01
ARL Aging Time	300

► **Status:** Displays the current system status of the XMS-1024

- ▷ Hardware Version: Hardware version of the switch
- ▷ Firmware Version: Software version of the switch
- ▷ DHCP Client: Status of the DHCP client, set at “Disable” by default
- ▷ IP Address: 192.168.0.2 by default

- ▶ Subnet Mask: 255.255.255.0 by default
- ▶ Gateway: 0.0.0.0 by default
- ▶ MAC Address: MAC address of the switch
- ▶ ARL Aging Time: Aging time of the MAC address table, 300 seconds by default

## 5.3 Port Settings

In this screen you can set the operating mode of each port. Six working modes are available for any port: 10 Mbps half-duplex, 10 Mbps full-duplex, 100 Mbps half-duplex, 100 Mbps full-duplex, 1000 Mbps full-duplex and auto negotiation. By default, the auto negotiation mode is enabled for all ports. In this mode, upon switch power up, each port automatically communicates and negotiates with its connected device, to determine the optimal operating mode. For other operating modes, manual setting is required and the settings should match the operating mode of the connected device; otherwise communication may fail. Port settings also affect the port mirroring and Trunk group functions.

- ▶ **5.3.1 Port**
- ▶ **5.3.2 Rate Limit**
- ▶ **5.3.3 Storm Control**
- ▶ **5.3.4 Statistics**

### 5.3.1 Port

**Port Configuration**

Port	Admin	Auto Negotiate	Speed Duplex	Flow Control
1	Enable	Enable	10Mbps Half	Disable

**Port Status**

Port	Link Status	Speed Mode	Speed Duplex	Flow Control	Port	Link Status	Speed Mode	Speed Duplex	Flow Control
1	Forwarding	Auto-Negotiate	100Mbps Full	Disable	2	Down	Auto-Negotiate	Down	Disable
3	Down	Auto-Negotiate	Down	Disable	4	Down	Auto-Negotiate	Down	Disable
5	Down	Auto-Negotiate	Down	Disable	6	Down	Auto-Negotiate	Down	Disable

- ▶ **Port Configuration:** Basic port configuration options for the XMS-1024 include port enable/disable, operating mode and flow control. The following describes the configuration functionality:
  - ▶ Port: Displays the corresponding port number for viewing or changing settings. All 24 10/100/1000 Mbps Ethernet ports are available for configuration.
  - ▶ Admin: Either enables or disables the corresponding port. If “Disable” is selected, the port is no longer operational.



**CAUTION:** Do not disable ports unless necessary.

- ▶ Auto Negotiate: If “Disable” is selected, you must manually specify the speed and duplex the port will use.



**NOTE:** In order to set or change “Speed Duplex” settings, you must “Disable” the auto-negotiation function.

- ▶ Speed Duplex: Select 10 Mbps half-duplex, 10 Mbps full-duplex, 100 Mbps half-duplex, 100 Mbps full-duplex or 1000 Mbps full-duplex mode for the port.
- ▶ Flow Control: Support for IEEE802.3x full-duplex flow control and half-duplex backpressure flow control disabled by default (if “Enabled” the XMS-1024 will automatically adjust the flow control mode depending on the duplex mode).
- ▶ **Port Status:** Lists the current settings of all ports, as shown below.

Port Status

Port	Link Status	Speed Mode	Speed Duplex	Flow Control	Port	Link Status	Speed Mode	Speed Duplex	Flow Control
1	Forwarding	Auto-Negotiate	100Mbps Full	Disable	2	Down	Auto-Negotiate	Down	Disable
3	Down	Auto-Negotiate	Down	Disable	4	Down	Auto-Negotiate	Down	Disable
5	Down	Auto-Negotiate	Down	Disable	6	Down	Auto-Negotiate	Down	Disable

## 5.3.2 Rate Limit

Rate Limit Configuration

Port	Downlink	Uplink	Port	Downlink	Uplink
1	No Limit	No Limit	2	No Limit	No Limit
3	No Limit	No Limit	4	No Limit	No Limit
5	No Limit	No Limit	6	No Limit	No Limit
7	No Limit	No Limit	8	No Limit	No Limit
9	No Limit	No Limit	10	No Limit	No Limit
11	No Limit	No Limit	12	No Limit	No Limit
13	No Limit	No Limit	14	No Limit	No Limit
15	No Limit	No Limit	16	No Limit	No Limit
17	No Limit	No Limit	18	No Limit	No Limit
19	No Limit	No Limit	20	No Limit	No Limit

- ▶ **Rate Limit Configuration:** The XMS-1024 allows the user to set limits on how much bandwidth is allocated to each port. This feature prevents a devices or user from consuming excessive bandwidth and can be used to guarantee good quality bandwidth to all client devices connected to the switch.
  - ▶ Port: Displays the corresponding port number for viewing or changing settings. All 24 10/100/1000 Mbps Ethernet ports are available for configuration.
  - ▶ Downlink/Uplink: Control the receive/transmit data rates by port. Available rates are: 128 Kbps; 256 Kbps; 384 Kbps; 512 Kbps; 640 Kbps; 768 Kbps; 896 Kbps; 1024 Kbps; 1152 Kbps; 1280 Kbps; 1408 Kbps; 1536 Kbps; 1664 Kbps; 1792 Kbps; 1920 Kbps; 2048 Kbps; 2176 Kbps; 2304 Kbps; 2432 Kbps; 2560 Kbps; 2688 Kbps; 2816 Kbps; 2944 Kbps; 3072 Kbps; 3200 Kbps; 3328 Kbps; 3456 Kbps; 3584 Kbps; 3712 Kbps; 3840 Kbps; 3968 Kbps; No Limit.



**NOTE:** If the selected rate is higher than the actual connection rate of the client device, the device will operate at its maximum data rate.

- ▶ **Rate Limit:** Displays the bandwidth control status of all ports, as shown below.

Port	Downlink	Uplink	Port	Downlink	Uplink
1	No Limit ▼	No Limit ▼	2	No Limit ▼	No Limit ▼
3	No Limit ▼	No Limit ▼	4	No Limit ▼	No Limit ▼

### 5.3.3 Storm Control

#### Storm Control

Broadcast Rate	4k ▼
Multicast Rate	4k ▼
Unknow Unicast Rate	4k ▼
Set the maximum number of frames/second before the switch blocks the traffic storm.	
<input type="button" value="Apply"/>	

- ▶ **Storm Control:** Suppresses the transfer of bandwidth limiting broadcast packets through the switch. When broadcast packets reach the set bandwidth limitation, the XMS-1024 automatically discards the packet to ensure a stable environment that is free from broadcast storms.
  - ▶ Broadcast Rate: The allowed bandwidth rate of broadcast packets. Default is 1024kb or 1mb/second.
  - ▶ Multicast Rate: The allowed bandwidth rate of multicast packets. Default is 1024kb or 1mb/second.

**i NOTE:** If multicast streaming is used in your environment you will want to raise this limit from the default.

- ▷ Unknown Unicast Rate (Flood): The allowed bandwidth rate of flood packets. Default is 1024kb or 1mb/second.

**i NOTE:** This value should not be raised without the assistance of a Network Administrator in determining if it is necessary.

**i NOTE:** The XMS-1024 does not completely suppress broadcast packets. Instead it only limits the transmission rate for broadcast packets.

### 5.3.4 Statistics

**Statistics**

Clear Refresh

Port	Tx Bytes	Tx Frames	Rx Bytes	Rx Frames	Tx Errors	Rx Errors
1	579029271	1273523	157865400	564178	0	3
2	2724135	5582	1176148	5151	0	1
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0

- ▷ **Statistics:** Displays the amount of data in bytes and frames that have been received/transmitted by all ports currently in operation, as well as the number of error frames received/transmitted by all ports in operation.
  - ▷ Clear: Clears all current port statistics data.
  - ▷ Refresh: Manually refreshes the current port statistics data.

**i NOTE:** The statistics page does not update dynamically

## 5.4 Mirror

### Mirror

Mirror Port	1 ▾											
Mirrored Port	1	2	3	4	5	6	7	8	9	10	11	12
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	13	14	15	16	17	18	19	20	21	22	23	24
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Apply"/>												
<p>Port mirroring sends a copy of all network traffic from one port to another port.</p> <p><b>REQUIREMENTS:</b></p> <p>1. The mirrored port's duplex speed must be greater than or equal to the source port.</p> <p>2. Both the source and mirrored ports must be on the same VLAN.</p>												

Port mirroring is used to transfer the packets of one or more monitored ports to another port, allowing a security department or administrator to monitor Internet access, traffic flows and packets.

The bandwidth of the monitoring port cannot be lower than that of the monitored port.

If the monitoring port is the monitored port, the system automatically ignores this monitored port and does not duplicate the traffic.

This function supports cross-VLAN monitoring. Monitoring is allowed even if the monitored port and the monitoring port belong to different VLAN groups.

#### ► **Mirror:**

- ▶ Mirror Port: Selects a port to serve as the monitoring port
- ▶ Mirrored Port: Selects one or more ports to be monitored

## 5.5 VLAN

A VLAN or Virtual Local Area Networks can be used to establish secure autonomous broadcast/multicast domains. A VLAN is used to divide a network into multiple network segments and/or to shrink broadcast domains for application or departmental optimization. Within a VLAN, all Ethernet packets, such as unicast, multicast, broadcast and unknown unicast packets will be transferred only to other devices within the VLAN group. A VLAN can be used to change the topological structure of the network without any movement of a network device or change of network connections. You can modify the VLAN settings of a device for example, to “move” a device from the VLAN of one group to that of another group. This helps create secure, optimized departmental (or function/application specific) networks that cannot be accessed by other departments, applications or functions. This also means the network nodes or devices can be moved, changed or added without having to physically move the device.

- ▶ 5.5.1 VLAN Mode
- ▶ 5.5.2 Port VLAN
- ▶ 5.5.3 802.1Q VLAN Configuration

- ▶ 5.5.4 VLAN Port Tag Configuration

## 5.5.1 VLAN Mode

### VLAN Mode

Port VLAN <input type="radio"/>	802.1Q VLAN <input checked="" type="radio"/>
Choose either Port VLAN or 802.1Q VLAN operating mode.	
<input type="button" value="Apply"/>	

Two VLAN modes are available: Port VLAN and 802.1Q VLAN

- ▶ **Port VLAN:** This option sets the XMS-1024 to operate in port VLAN mode
- ▶ **802.1Q VLAN:** This option sets the XMS-1024 to operate in 802.1Q VLAN mode



**NOTE:** When one VLAN mode is selected, the other mode will be disabled

## 5.5.2 Port VLAN

### Port VLAN

VLAN Group	1 ▾											
VLAN Member	1	2	3	4	5	6	7	8	9	10	11	12
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	13	14	15	16	17	18	19	20	21	22	23	24
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="button" value="Apply"/>												

### VLAN Group

VLAN Group	VLAN Member																							
-	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V	V
2	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

- ▶ **Port VLAN Configuration:** Port VLAN uses the physical ports of the switch to distinguish between VLANs.

- ▶ **VLAN Group:** Defines the ports belonging to a specified VLAN. By default, group 1 includes all 24 ports
- ▶ **VLAN Member:** Adds the selected ports of the XMS-1024 to the specified VLAN

- ▶ **Adding a Port to VLAN:** To add a port, select the VLAN group, then mark the box to designate which ports should belong to the selected VLAN.



**NOTE:** When modifying an already configured VLAN, all ports will show up as unchecked. Any port left unchecked, will not be part of the group.



To remove a port from a specified VLAN, first select the VLAN group you wish to remove it from. Then, check the ports you wish to remain in the VLAN while leaving the ports you wish to remove unchecked.

### 5.5.3 802.1Q VLAN Configuration

802.1Q VLAN

VLAN ID:  (1-4094)

Port	1	2	3	4	5	6	7	8	9	10	11	12
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

A VLAN membership is associated to each incoming frame. The frame is forwarded to all ports that are members of the associated VLAN ID.

**RULES:**

1. Frames that are not discarded are subject to VLAN classification.
2. Untagged and priority tagged frames are classified to the default port VLAN ID (PVID).
3. Frames with existing VLAN ID tags are forwarded to the associated VLANs.

**VLAN Group**

NO.	VLAN ID	VLAN Port Member	Operation
1	1	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,	-

In 802.1Q VLAN mode (Tagged mode), the port VLAN ID (VID) is used to distinguish to which VLAN the traffic belongs. When a packet passes through the switch, the VID information in the tag header indicates to which VLAN the packet belongs. The switch then determines the destination ports according to the VID set in the packet.

- ▶ **VLAN ID:** Sets the VID identifiers associated with each port. All ports are set to one by default.



**NOTE:** Modification of the attributes of VLAN ID 1 is not allowed.

- **Port:** Adds the ports for the specified VLAN ID

## 5.5.4 VLAN Port Tag Configuration

VLAN Port Tag Configuration

Port	Port Tag	Incoming Filter	PVID
1	Untagged	<input type="checkbox"/>	1
2	Untagged	<input type="checkbox"/>	1
3	Untagged	<input type="checkbox"/>	1
4	Untagged	<input type="checkbox"/>	1
5	Untagged	<input type="checkbox"/>	1
6	Untagged	<input type="checkbox"/>	1
7	Untagged	<input type="checkbox"/>	1
8	Untagged	<input type="checkbox"/>	1
9	Untagged	<input type="checkbox"/>	1
10	Untagged	<input type="checkbox"/>	1

- **Port Tag:** Sets the Tag attribute for the corresponding port. The Port Tag rule specifies the changes to be made upon packet transmit. Available options are to either add the VID tag to the frame or to remove the VID tag from the frame (Tagged/Untagged)
- **Incoming Filter:** Specifying the Incoming Filter rule determines whether to receive or not receive the VID tagged packets that are inconsistent with the port PVID



**NOTE:** Checking the Incoming Filter box will drop all packets sent to the port that do not have the specified PVID (i.e. if the packet is tagged as one and the PVID is set to two the packet will be dropped.)

- **PVID:** Sets the VLAN ID (VID) of the specified port

## 5.6 Trunk

Trunk Configuration

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

Trunk Switching Choice  Source Address  Destination Address  Source and Destination Address

Trunking or link aggregation allows multiple ports to be grouped together as a single link between switches to increase effective bandwidth and provide link redundancy.

**RESTRICTIONS:**

1. Trunk group members must be in the same VLAN and all port configurations must be the same.
2. Trunk ports between two switches must be in the same trunk group.

Trunking is used to expand bandwidth, for failover, and/or to increase error tolerance when networking multiple switches together.

All ports that are defined as members of the trunk group can be used for trunking ONLY and cannot be used for other purposes, even when they are not being used by the trunk group.

Cross-VLAN trunk grouping is not supported. All members of a trunk group must be within the same VLAN. Otherwise the trunk will not function properly.

When the trunk group is used for inter-switch cascading (Uplinks), be sure the cascading port used for connecting with the other switch is part of the corresponding trunk group. The cascading of multiple ports (trunk members) must be done from one trunk group to a corresponding trunk group.



**CAUTION:** Never connect two trunk groups of a switch together or cascade two switches through more than one trunk channel. Such configurations will result in a network loop and will cause a broadcast storm resulting in blocking of all network traffic on the switches.

## 5.7 QoS

### QoS

Port ID	Port Priority	802.1P Tag Priority	802.1P Default Priority	ToS Priority
1	low	Disable	0	Disable

The QoS (Quality of Service) priorities are in the following order from highest to lowest:

- 1.ToS Priority
- 2.802.1P Tag Priority
- 3.802.1P Default Priority
- 4.Port Priority

### QoS Status Table

Port ID	Port Priority	802.1P Tag Priority	802.1P Default Priority	ToS Priority
1	low	Disable	0	Disable
2	high	Disable	0	Disable

QoS functions can be implemented through a combination of priority mode settings and priority control options. The XMS-1024 supports packet mapping by 4 priority levels (low, normal, medium and high) and 3 priority setting modes: Type of Service (ToS) Priority, 802.1P Tag Priority, and 802.1P Default Priority

#### ► QoS priority setting modes are in the following order from highest to lowest:

- ToS Priority: If “ToS Priority” is enabled, the switch automatically reads an 8-bit ToS tag from the IPv6/IPv4 packet. If the priority tag indicates a high priority, this packet is mapped to high priority for priority processing. When the switch becomes busy, it processes the packets marked with a high priority first.
- 802.1P Tag Priority: If “802.1Q Tag Priority” is enabled, the switch automatically reads a 3-bit priority tag from the packet with a valid VLAN tag. If the priority tag indicates a high priority, the packet is mapped to high priority. When the switch becomes busy, it processes the packets marked with a high priority first.
- 802.1P Default Priority
- Port Priority: If “Port Priority” is enabled and high priority is assigned to a physical port, all packets passing this port are mapped to high priority. As a result, the switch processes the packets received/transmitted by this port first.

#### ► Description of QoS Configuration:

- Port ID: Selects the port to be set
- Port Priority: Select “low”, “normal”, “medium” or “high” for the desired port priority



**NOTE:** Applications like Video Streaming and VoIP will work best with high priority

- ▶ 802.1P Tag Priority: Enables or disables 802.1P priority functions
- ▶ ToS priority: Enables or disables ToS priority functions
- ▶ **QoS Status Table:** Displays the QoS status of all ports

Port ID	Port Priority	802.1P Tag Priority	802.1P Default Priority	ToS Priority
1	low	Disable	0	Disable
2	high	Disable	0	Disable

## 5.8 MAC Settings

### ▶ 5.8.1 MAC Filter

### ▶ 5.8.2 Static MAC

### 5.8.1 MAC Filter

#### MAC Filter

MAC Address	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>
<input type="button" value="Add Address"/>	
To block a device's network access from all ports, add the MAC address to the MAC Filter Blacklist.	

#### MAC Filter Table

NO.	Source MAC	Operation
<input type="button" value="Delete All"/>		

- ▶ **MAC Filter:** This allows a MAC address to be added to a list that blocks that particular address from connecting to the network. When the specified MAC address tries to connect on any port of the XMS-1024, network communication will be blocked.
- ▶ **MAC Address:** Enter the MAC address to be filtered



**NOTE:** Any MAC address that has been added to the MAC filter will not be allowed to pass any traffic until it is removed from the list

- ▶ **MAC Filter Table:** Lists the MAC addresses to be filtered, as shown below. To remove A MAC address from the filter table and allow access to the network, click "Delete" on the right column next to the corresponding MAC address.

NO.	Source MAC	Operation
1	00-01-1c-3f-2e-01	<input type="button" value="Delete"/>
<input type="button" value="Delete All"/>		

## 5.8.2 Static MAC

### Static MAC Address

MAC Address	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>
Port ID	1 <input type="button" value="Add Address"/>
To only allow network access on the specified port to authorized devices, add the MAC address to the Static MAC Address Whitelist.	

### Static MAC Address Table

NO.	Source MAC	Port ID	Operation
<input type="button" value="Delete All"/>			

A Static MAC Address assigns and binds a particular MAC address to a specified port. Data transmission of that MAC address can then only be forwarded through the corresponding port.

- ▶ MAC Address: Enter the MAC address to be assigned
- ▶ Port ID: Select the port to which the MAC address will be bound
- ▶ **Static MAC Address Table:** Lists bound MAC addresses and the ports to which they have been assigned, as shown below. You can click “Delete” on the right to delete the corresponding MAC address assignment or click “Delete All” to remove all MAC address bindings.

NO.	Source MAC	Port ID	Operation
1	00-1c-3f-23-45-02	5	<input type="button" value="Delete"/>
<input type="button" value="Delete All"/>			

## 5.9 802.1X

802.1X provides methods and policies for authenticating network users and allow for network access. It is a port-based authentication policy, for the purpose of controlling access to a particular port. It “enables” the port upon successful authentication to allow transmission of all data or “disables” this port upon failed authentication.

### ▶ 5.9.1 802.1X Configuration

### ▶ 5.9.2 802.1X Port Configuration

## 5.9.1 802.1X Configuration

### 802.1X Configuration

802.1X Enabled	Enable <input type="checkbox"/>
RADIUS Server IP	<input type="text" value="0.0.0.0"/>
RADIUS UDP Port	<input type="text" value="1812"/>
RADIUS Secret	<input type="text"/>
Reauthentication Enabled	Enable <input type="checkbox"/>
Reauthentication Period	<input type="text" value="3600"/> (1 - 3600 Seconds)
EAP timeout	<input type="text" value="30"/> (1 - 255 Seconds)
<input type="button" value="Apply"/>	

- ▶ **802.1X Enabled:** Mark the box to enable or leave it unmarked to disable the 802.1X authentication function
- ▶ **RADIUS Server IP:** Sets the IP address of the RADIUS server
- ▶ **RADIUS UDP Port:** Sets the RADIUS UDP port of the XMS-1024. It is set to 1812 by default
- ▶ **RADIUS Secret:** Sets the value of the secret key the XMS-1024 sends to the corresponding RADIUS server. If there is a mismatch, the server will drop all authentication requests.
- ▶ **Reauthentication Enabled:** Enables or disables the reauthentication function. This setting, in tandem with the “Reauthentication Period” setting will force authenticated devices to reauthenticate after the period expires
- ▶ **Reauthentication Period:** Sets the time period interval for required reauthentication. This period is 3600 seconds by default (i.e. reauthentication is performed each hour).
- ▶ **EAP Timeout:** Sets the timeout interval of Extensible Authentication Protocol (EAP) authentication response. This is set to 30 seconds by default



**NOTE:** The EAP Timeout value may need to be increased in large or busy networks to prevent authentication timeout.

## 5.9.2 802.1X Port Configuration

802.1X Port Configuration

Port	Admin State	Port State	Force Re-authenticate
1	Force Authorized	802.1X disabled	<a href="#">Force Re-authenticate</a>
2	Force Authorized	802.1X disabled	<a href="#">Force Re-authenticate</a>
3	Force Authorized	802.1X disabled	<a href="#">Force Re-authenticate</a>
4	Force Authorized	802.1X disabled	<a href="#">Force Re-authenticate</a>
5	Force Authorized	802.1X disabled	<a href="#">Force Re-authenticate</a>
6	Force Authorized	802.1X disabled	<a href="#">Force Re-authenticate</a>
7	Force Authorized	802.1X disabled	<a href="#">Force Re-authenticate</a>
8	Force Authorized	802.1X disabled	<a href="#">Force Re-authenticate</a>
9	Force Authorized	802.1X disabled	<a href="#">Force Re-authenticate</a>
10	Force Authorized	802.1X disabled	<a href="#">Force Re-authenticate</a>

- ▶ **Admin State:** There are 3 options: Force Authorized, Force Unauthorized and Auto. In “Forced Authorized” state, the port allows transmission of any message. In “Forced Unauthorized” state, the port only allows transmission of authenticated messages. In “Auto” state the port allows transmission of certain messages according to the authentication result



**NOTE:** If using a RADIUS server, it is recommended to use the “Auto” state setting.

- ▶ **Port State:** Displays the 802.1X status of each port. Options include: 802.1X disabled, Link Interrupted, Authorized or Unauthorized
- ▶ **Force Re-authenticate:** Clicking the link forces the corresponding port to perform reauthentication

## 5.10 RSTP

Rapid Spanning Tree Protocol (RSTP) can be used to create connection links for redundancy and failover. To avoid loops, RSTP automatically assigns a root bridge or root port and parameters are changed at the bridge level.

### ▶ 5.10.1 RSTP Configuration

### ▶ 5.10.2 RSTP Port Configuration



**NOTE:** Because the RSTP algorithm is complex, it is recommended to use default values. If modification to RSTP parameters is necessary, consult a networking expert and/or carefully read and understand RSTP definitions and procedures.

## 5.10.1 RSTP Configuration

### RSTP Configuration

System Priority	<input type="text" value="32768"/>
Hello Time	<input type="text" value="2"/> (1 - 10 Seconds)
Max Age	<input type="text" value="20"/> (6 - 40 Seconds)
Forward Delay	<input type="text" value="15"/> (4 - 30 Seconds)
Version	<input type="text" value="RSTP"/>
<input type="button" value="Apply"/>	

- ▶ **System Priority:** Sets the system priority of each switch within the network. The switch with the lowest system priority will become the root bridge. If the switch is used in a large-scale enterprise network, it is recommended to skip this setting.
- ▶ **Hello Time:** Sets a value ranging 1 second to 10 seconds. This sets the time interval for the root bridge transmission of BPDU packets to all of other switches, so it is known which switch is serving as the root bridge. When a switch not serving as the root bridge is set with a specific value, the value does not take effect. Only when the switch becomes the root bridge is the setting active.
- ▶ **Max Age:** Sets a value ranging 6 seconds to 40 seconds. If a switch does not receive the BPDU packet transmitted by the root bridge when the maximum aging time is up, the switch will take over as the root bridge and transmit the BPDU packets to all other switches. If the switch has the lowest priority level, it will continue to function as the root bridge. This setting should be set to a large value, to avoid unnecessary resetting of the root bridge.
- ▶ **Forward Delay:** Sets a value ranging 4 seconds to 30 seconds. This is the monitoring time for a switch port to change from blocking status into forwarding status (i.e. how long it will take for a port to become active after another port has failed). A higher value means greater delay in response.
- ▶ **Version:** Selects the version of Spanning Tree to use: RSTP based on 802.1W (default value) or STP based on 802.1D (Note: RSTP is the current industry standard.)

## 5.10.2 RSTP Port Configuration

RSTP Port Configuration

Port	Protocol Enabled	Edge	Path Cost
1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	auto
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	auto
3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	auto
4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	auto
5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	auto
6	<input checked="" type="checkbox"/>	<input type="checkbox"/>	auto
7	<input checked="" type="checkbox"/>	<input type="checkbox"/>	auto
8	<input checked="" type="checkbox"/>	<input type="checkbox"/>	auto
9	<input checked="" type="checkbox"/>	<input type="checkbox"/>	auto
10	<input checked="" type="checkbox"/>	<input type="checkbox"/>	auto

- ▶ **Protocol Enabled:** Enables or disables the RSTP function by port. By default this function is disabled for all ports
- ▶ **Edge:** If a port is directly connected with a device, the port should be set as an edge port. Edge ports feature faster status transition, taking a shorter time to change from blocking state into forwarding state.
- ▶ **Path Cost:** Sets a value ranging 0 to 200000000. “Auto” indicates that the XMS-1024 will automatically determine the lowest port path cost depending on the port rate.

## 5.10.3 RSTP Status

RSTP Bridge Overview

Bridge ID	Hello Time	Max Age	Forward Delay	Topology	Root ID
32768:c8-3a-35-e0-00-01	2	20	15	Steady	This switch is Root!

RSTP Port Status

Port	Path Cost	Edge Port	P2P Port	Protocol	Port State
1	200000	no	yes	RSTP	forwarding
2					Disabled
3					Disabled
4					Disabled
5					Disabled

- ▶ **RSTP Bridge Overview:** Displays the Bridge ID, Hello time, Maximum Aging Time, Forwarding Delay, Topology, and Root Bridge ID specified by the system
- ▶ **RSTP Port Status:** Displays the Path Cost, Edge Port setting, P2P Port, Protocol, and Port State specified by the system.

## 5.11 IGMP Snooping

IGMP Snooping is used to implement dynamic registration of L2 multicast on the switch. To accommodate L2 multicast with IGMP Snooping, IGMP must be activated on the client device and router as the XMS-1024 only snoops the IGMP messages transmitted by the client device and router to dynamically maintain the L2 multicast group. Multicast registration on this switch does not affect the settings of other switches in the environment. The switch transmits an IGMP query message and receives the IGMP response from the client device. Based on the receiving port, VLAN ID, and multicast of the IGMP packets, the XMS-1024 creates and maintains a multicast group. After creating a group, it forwards the IGMP packets to other switches and routers in the network. Only the ports included in a multicast group can receive the multicast data stream. This reduces network traffic and saves network bandwidth.

### ► 5.11.1 Snooping Configuration

### ► 5.11.2 Snooping Status

## 5.11.1 Snooping Configuration

### IGMP Configuration

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

### IGMP Configuration List

VLAN ID	IGMP Snooping Enabled	IGMP Querying Enabled
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Apply

### ► IGMP Configuration:

- IGMP: Enables or disables L2 multicast. By default, this option is disabled
- Router Ports: Selects the IGMP ports for multicast snooping

### ► IGMP Configuration List:

- IGMP Snooping Enabled: Enables or disables the L2 multicast snooping function
- IGMP Query Enabled: Enables or disables the IGMP query function. Once this function is enabled, the multicast snooping status can be viewed

## 5.11.2 Snooping Status

### IGMP Status

VLAN ID	Querier	Queries transmitted	Queries received	v1 Reports	v2 Reports	v3 Reports	v2 Leaves
1	Active	2516	0	0	8405	134	106

IGMP Status: Displays the multicast snooping options configured by VLAN. When the multicast table is not established, “Querier” displays “Idle”. When the XMS-1024 snoops into a multicast message, “Querier” displays “Active” and the values in “Queries transmitted” and “Queries received” will begin to be displayed. The values in “V1 Reports”, “V2 Reports” and “V3 Reports” shows the version of the multicast messages received. If a message is of V2 and a device in the multicast table wants to leave the multicast group, the leave message is transmitted in V2 format.

► **Refresh:** Manually refreshes the current port status



**NOTE:** This page does not dynamically refresh itself

## 5.12 System

- **5.12.1 SNMP**
- **5.12.2 Change Password**
- **5.12.3 Power Save**
- **5.12.4 Upgrade**
- **5.12.5 IP Configuration**
- **5.12.6 MAC Aging Configuration**
- **5.12.7 Restore Factory Defaults**
- **5.12.8 Backup**
- **5.12.9 Restore**
- **5.12.10 Logout**

### 5.12.1 SNMP

#### SNMP Configuration

SNMP	Enable <input checked="" type="checkbox"/>
SNMP Trap Destination	<input type="text" value="192.168.0.100"/>
SNMP Read Community	<input type="text" value="public"/>
SNMP Write Community	<input type="text" value="private"/>
SNMP Trap Community	<input type="text" value="public"/>

All management information and counters are stored in the Management

Information Base (MIB) of the switch. The XMS-1024 adopts standard MIB-II modules that support read function from any SNMP-based NMS software. MIB data may be set to either read-only or read-write mode.

The default SNMP community names of the switch can be user modified.

Traps are messages generated by the XMS-1024 and used for notification of certain events. Such events may be serious (i.e. switch reboot) or ordinary (i.e. the status changes of a switch port). The XMS-1024 can generate traps and send them to the NMS.

#### ► **SNMP Configuration:**

- ▶ **SNMP:** Enables or disables the SNMP management function. SNMP is enabled by default
- ▶ **SNMP Trap Destination:** Sets the destination IP address of the Trap messages generated by the XMS-1024
- ▶ **SNMP Read Community:** Sets the read-only community name. For a device to read the SNMP information of the XMS-1024, the SNMP management software must contain the read-only community name
- ▶ **SNMP Write Community:** Sets the read/write community name. For a device to modify the SNMP information on the XMS-1024, the SNMP management software must contain the read/write community name
- ▶ **SNMP Trap Community:** Used by the SNMP management software to identify the switch sending the Trap message

## 5.12.2 Change Password

### Change Password

Old Password	<input type="text"/>	(Max 15 Characters)
New Password	<input type="text"/>	(Max 15 Characters)
Confirm New Password	<input type="text"/>	
<input type="button" value="Apply"/>		

#### ► **Change Password:** Modifies the password for switch login

- ▶ **Old Password:** Enter the old password (Default password is “admin”)
- ▶ **New Password:** Enter the new password
- ▶ **Confirm New Password:** Re-enter the new password



**NOTE:** A password can consist of up to 15 alpha numeric characters.

### 5.12.3 Power Save

#### Power Save

Power Save	<input type="checkbox"/> Enable
<input type="button" value="Apply"/>	

- ▶ **Power Save:** Check to enable or uncheck to disable the power save mode
- ▶ **Apply:** Enables or disables the power save mode

### 5.12.4 Upgrade

#### Firmware Upgrade

Current Firmware Version	V2.1
Choose File	<input type="button" value="Choose File"/> No file chosen
<input type="button" value="Upgrade"/>	
<small>Turning off switch power during upgrade may result in damage. Switch will restart automatically when upgrade is complete. Please wait as it will take a few minutes to upgrade.</small>	

Please visit the Luxul website to check for firmware upgrades and obtain upgrade instructions.

#### Firmware Upgrade:

1. Go to the Luxul website and download the new version of firmware
2. Click “Browse” to locate the firmware file
3. Click “Upgrade” to perform the update



**CAUTION:** Do not power off the switch or computer being used during the upgrade or the switch may be damaged. During upgrade, it is recommended to disable all network connections except the network connection of the computer used for the upgrade.

## 5.12.5 IP Configuration

### Configure IP Address

DHCP Client	Enable <input type="checkbox"/>
IP Address	192 . 168 . 0 . 2
Subnet Mask	255 . 255 . 255 . 0
Gateway	192 . 168 . 0 . 1
Management VLAN	1
If "DHCP Client" is enabled, the web management interface is only accessible through the IP address assigned by the DHCP server.	
<input type="button" value="Apply"/>	

DHCP Client: Enables or disables the DHCP client. It is disabled by default.

- ▶ **IP Address:** Sets the login IP address of the switch (192.168.0.2 by default)
- ▶ **Subnet Mask:** Sets the subnet mask of the switch (255.255.255.0 by default)
- ▶ **Gateway:** Sets the gateway of the switch (0.0.0.0 by default)
- ▶ **Management VLAN:** Selects the VLAN of the management computer



**NOTE:** If the Management VLAN is not setup properly, you will not be able to manage the switch.



**CAUTION:** After enabling the DHCP client, you must check for the IP address obtained from the DHCP server (usually a router or sever in the network) and then re-connect to the switch. It is not recommended to use this function.

## 5.12.6 MAC Aging Configuration

### MAC Aging Configuration

ARL Aging	<input checked="" type="checkbox"/> Enable
Aging Time	300 (10 - 65535 Seconds)
<input type="button" value="Apply"/>	
If "ARL Aging" is disabled, MAC addresses will never be removed from the ARL table. It is recommended to leave ARL Aging enabled.	

The default MAC address aging time is 300 seconds. The set value should be between 10 seconds and 65535 seconds. Otherwise, the system will report an error. If "ARL Aging" is left unchecked, the system terminates MAC address aging (not recommended).

- ▶ **ARL Aging:** Check to enable this function or uncheck to disable. It is enabled by default



**NOTE:** It is not recommended to disable ARL Aging

- ▶ **Aging Time:** Sets the aging time. 300 seconds by default.



**NOTE:** It is not recommended to have an Aging Time setting greater than 3600 seconds.



**CAUTION:** If “ARL Aging” is unchecked, the switch stops learning new MAC addresses and the addresses in the MAC address table turn into static MAC entries and are free from aging. This is not recommended.

## 5.12.7 Restore Factory Defaults

### Restore Factory Defaults

Press Apply to restore to factory defaults.

- ▶ **Restore Factory Defaults:** Click “Apply” to restore the factory default configuration



**CAUTION:** Restoring default configuration will re-set all of your settings to factory defaults. The switch will now have the default IP address 192.168.0.2. For login, both default user name and default password are “admin.”

## 5.12.8 Backup

### Backup Current Settings

Press Backup to backup a copy of the current settings to a file.

- ▶ **Backup Current Settings:** Click “Backup” to backup the current switch configuration settings to a file

### 5.12.9 Restore

Restore Settings from a File

Select File	<input type="button" value="Choose File"/> No file chosen
<input type="button" value="Restore"/>	
<p><b>Note:</b> Turning off switch power during restore may result in damage. Switch will restart automatically when restore is complete. Please wait as it will take a few minutes to upgrade.</p>	

- ▶ **Restore Settings from a File:** Restores the backup switch configuration. Click “Browse” and select the backup file on your computer, and then click “Restore”.



**CAUTION:** It takes about 30 seconds to complete the restoration. To avoid errors during the restoration, do not power off the switch or computer being used. At the end of restoration, you will need to restart the switch.

### 5.12.10 Logout

This function is used to exit the switch configuration.

## 6: REGULATORY COMPLIANCE

This device is approved under the Luxul brand and designed to comply for use specifically with other approved Luxul devices. This device is designed to be compliant with rules and regulations in locations where they are sold and will be labeled as required. Any changes or modifications to Luxul equipment, not expressly approved by Luxul, could void the user’s authority to operate the equipment. This Luxul device when used in conjunction with the approved Luxul Models should be professionally installed and the Radio Frequency Output Power will not exceed the maximum allowable limit for those countries that have regulatory approval.

### 6.1 Health and Safety Recommendations

Warnings for the use of Wireless Devices: Please observe all warning notices with regard to the usage of wireless devices

Potentially Hazardous Atmospheres: You are reminded of the need to observe restrictions on the use of radio devices in fuel depots, chemical plants etc. and areas where the air contains chemicals or particles (such as grain, dust, or metal powders).

Safety in Hospitals: Wireless devices transmit radio frequency energy and may affect medical electrical equipment. When installed adjacent to other equipment, it is advised to verify that the adjacent equipment is not adversely affected.

Power Supply: Use only a Luxul approved power supply output rated at 100-240VDC and minimum 0.6A. The power supply shall be Listed to UL/CSA 60950-1; and certified to IEC60950-1 and EN60950-1 with SELV outputs. The device can also be powered from a compliant POE source. Use of alternative power supply will invalidate any approval given to this device and may be dangerous.

## 6.2 FCC Statement:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment 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 or more 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.

## 7: CONTACT LUXUL

For sales questions  
please contact our  
Sales Department

P: (801) 822-5450  
E: sales@luxul.com

If you experience any  
problems, please contact  
Technical Support

P: (801) 822-5450  
E: support@luxul.com

To check for firmware updates or download pre-configured application modules, visit [luxul.com](http://luxul.com).

## APPENDIX 1: COMMON COMMANDS

Common Commands	Description
cmd	Enter the command line mode of a Windows system (applicable to Windows2000 and higher).
ipconfig	Displays the IP address of the computer. (i.e. ipconfig/all) Must be run from the command line.
ping	Used to test for network availability and device/system recognition. Device sends a packet to the target host and asks for a response. If the device receives a response from the target host, it can then see the network response time and connection status between the local device and target host. Must be run from the command line.
netstat	Displays details of current active network connections including routing table and network interface information. Can also be used to count the active network connections. Must be run from the command line.
tracert	Displays the path taken by a packet before reaching the target host and the specific time when it reached each node. Similar to the Ping command but provides more detailed information. Displays the entire path and IP address of each node in the path and total elapsed tim. Must be run from the command line.

## APPENDIX 2: TCP/IP ADDRESS SETTING (WINDOWS XP)

Select “Start Control Panel (see Figure 1). Select “Classic View” if you do not see the options below.

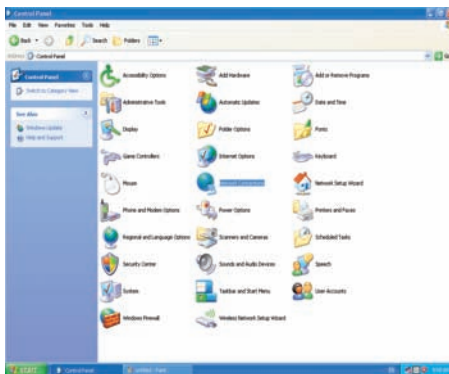


Figure 1

Double click “Network Connection” (see Figure 2).

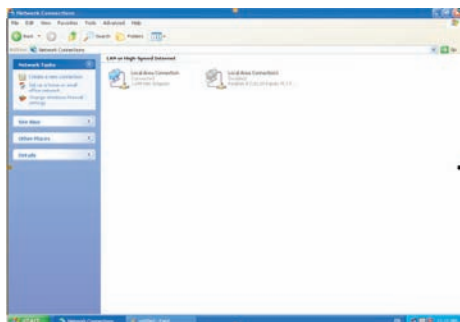


Figure 2

Right-click “Local Area Connection” and then select “Properties” in the shortcut menu. Select “Internet Protocol (TCP/IP)” then click “Properties” (see Figure 3).

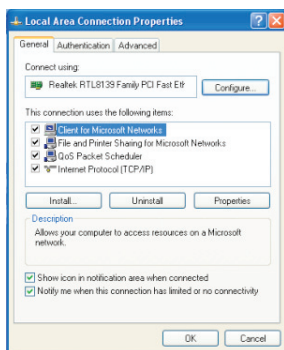


Figure 3

Select “Use the following IP address,” enter “192.168.0.xxx” (“xxx” ranges 2-254) for IP address and 255.255.255.0 for subnet mask (see Figure 4) Note: do not use 192.168.0.2 as this is the address of the switch.

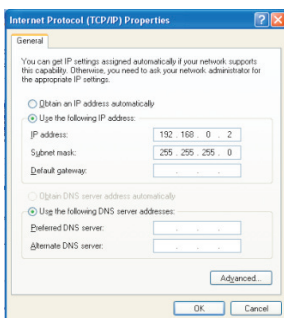


Figure 4

Click “OK” to return to the “Local Area Connection Properties” dialog box.

Click “OK” to exit the setting window. Note: the address change will not take place until you close the Local Area Connection Properties window.

## GLOSSERY

- ▶ **ARP (Address Resolution Protocol):** Converts an Internet Protocol (IP) address to its corresponding physical network address.
- ▶ **Broadcast:** The transmission of packets to all hosts in the network.
- ▶ **Broadcast Storm:** An infinite loop of ARP requests, usually associated with a physical wiring loop.
- ▶ **MAC address (Media Access Control address):** A unique identifier assigned to network interfaces for communications on the physical network segment.
- ▶ **Multicast:** Transmission of packets to a host group within the network.
- ▶ **QoS (Quality of Service):** A suite of protocols and hardware management that prioritizes data packets. Very useful in latency sensitive applications, i.e. VoIP, Control Systems, Video, Streaming
- ▶ **RSTP (Rapid Spanning Tree Protocol):** A protocol that helps to reduce broadcast storms by managing multiple connections to the same destination.
- ▶ **SNMP: (Simple Network Management Protocol):** is an “Internet-standard protocol for managing devices on IP networks.
- ▶ **IGMP Snooping:** Used to implement dynamic registration of L2 multicast on the switch.
- ▶ **TCP/IP:** Named from two of the most important protocols in it: the Transmission Control Protocol (TCP) and the Internet Protocol (IP), which are the first two networking protocols defined in this standard.
- ▶ **Unicast:** Transmission of packets to a specific host in the network.
- ▶ **Unknown Unicast (flood):** The transmission of unicast packets with an unknown destination MAC address (this does not occur under normal network operation).
- ▶ **VLAN (Virtual Local Area Network):** used to establish secure autonomous broadcast/multicast domains.

**Information on this document supersedes all previous versions.**

**Products and documents subject to change without notice.**

**Products may be discontinued without notice.**