User Manual

MS888G2
24 Port Modular SNMP Managed Switch

Version: 1.01
June, 2006

TABLE OF CONTENTS

Caution

Electronic Circuit devices are sensitive to static electricity. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electric charge.

To protect your switch, always:

- Touch the metal chassis of your computer to ground the static electrical charge before you handle the switch.
- Pick up the switch by holding it on the left and right edges only.

Electronic Emission Notices

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment.

European Community (CE) Electromagnetic Compatibility Directive

This equipment has been tested and found to comply with the protection requirements of European Emission Standard EN55022/EN60555-2 and the Generic European Immunity Standard EN50082-1.

EMC:	EN55022(1988)/CISPR-22(1985)	class A
	EN60555-2(1995)	class A
	EN60555-3	
	IEC1000-4-2(1995)	4K V CD, 8KV, AD
	IEC1000-4-3(1995)	3V/m
	IEC1000-4-4(1995)	1KV – (power line), 0.5KV – (signal line)

Australian C-Tick Compliance.

This equipment is compliant with the required Australian C-Tick standards

MS888G2 User Manual

About this User Manual

This User Manual will guide you on procedures to install, configure and monitor the Alloy MS888G2 24 port Modular SNMP Managed Switch utilising the built-in web management interface and also the CLI.

Overview of the User Manual

- Chapter 1 “Introduction” describes the features of the MS888G2 Modular SNMP Managed switch
- Chapter 2 “Installation”
- Chapter 3 “Operation of the Web-based Management”
- Chapter 4 “Operation of the CLI”

1. Introduction

1.1. Overview of MS888G2 SNMP Managed Switch

The MS888G2 Switch is a high performance web and SNMP managed switch that provides a modular solution for 100Mbps networking in Fibre and Copper termination. The MS888G2 modular 3 slot chassis design supports 24x 10/100Mbps copper or 100Mbps fibre ports with 2 built-in Gigabit paired dual media ports for Gigabit uplink. The switch facilitates high availability services through intelligent network management and support for dual redundant power supplies.

All modules for the MS888G2 are Hot Swappable allowing the switch to be configured with different port variations without having to power down your network.
All available modules are listed below:

Intelligent Network features offer a complete management solution that can enable you to scale your network from a single departmental switch right up to any Enterprise environment. STP and RSTP offer network redundancy features, IGMP snooping offers support for Streaming Video and Multicasting images, Tagged VLAN offers logical security and management of nodes within defined groups. QOS based on port priority queues and TOS bytes ensure efficient forwarding of critical network data.

All Ports support non-blocking maximum wire speed performance with Auto-negotiation and Auto-MDIX functions on all copper ports for simplified deployment.-

The SFP ports can support the following optional mini-GBIC modules for fibre optic cable connections (either single-mode or multimode terminated in LC type connectors):

- 1000Mbps multimode 1000Base-SX, 850nm, max. range 500m
- 1000Mbps single-mode 1000Base-LX, 1310nm, max. range 10Km
- 1000Mbps single-mode 1000Base-LHX, 1310nm, max. range 40Km
- 1000Mbps single-mode 1000Base-LHX, 1550nm, max. range 40Km
- 1000Mbps single-mode 1000Base-ZX, 1550nm, max. range 70Km
- 1000Mbps single-mode 1000Base-EZX, 1550nm, max. range 100Km
- 1000Mbps WDM single-mode/single-core 1310nm, max. range 20Km
- 1000Mbps WDM single-mode/single-core 1550nm, max. range 20Km

------This is not an exhaustive list of SFP modules available--------

*Notes: * The two WDM (Wave Division Multiplexing) mini-GBIC modules are designed to facilitate a link over a single core of single-mode fibre cable. The two units must be used in a paired manner, one at either end of the link.*

** Mini-GBIC modules that are designed to the relevant standards should be compatible with any make of switch with SPF ports. If you have concerns regarding compatibility, please contact the supplier of your mini-GBIC product.*

The 10/100/1000Mbps copper ports meet all IEEE 802.3/u/x/z Gigabit and Fast Ethernet specifications.

The 1000Mbps SFP fibre ports via optional mini-GBIC modules are compliant with all IEEE 802.3z and 1000Base-SX/LX/LHX/ZX/EZX standards.

1000Mbps single fibre WDM transceivers are designed with an optic Wavelength Division Multiplexing (WDM) technology that transports bi-directional full duplex signals over a single fibre core.

The MS888G2 supports the following module types:

- **M8T -** 8 Port 10/100 Base-TX module
- **M8MT -** 8 Port 100 Base-FX (MT-RJ) Multi mode module
- **M8SC** - 8 Port 100 Base-FX (ST) Multi Mode module
- **M8ST** - 8 Port 100 Base-FX (SC) Multi Mode module
- **M8SC.S05** - 8 Port 100 Base-FX (SC) Single Mode module 5km
- **M8SC.S20** - 8 Port 100 Base-FX (SC) Single Mode module 20km
- **M8SC.S60** - 8 Port 100 Base-FX (SC) Single Mode module 60km
- **M8WDM3.S20** - 8 Port 100Base-FX Single Mode/Single Fibre (SC) 1310nm Module 20Km
- **M8WDM5.S20** - 8 Port 100Base-FX Single Mode/Single Fibre (SC) 1550nm Module 20Km
- **M8WDM3.S40** - 8 Port 100Base-FX Single Mode/Single Fibre (SC) 1310nm Module 40Km
- **M8WDM5.S40** - 8 Port 100Base-FX Single Mode/Single Fibre (SC) 1550nm Module 40Km
- **M8WDM3.S60** - 8 Port 100Base-FX Single Mode/Single Fibre (SC) 1310nm Module 60Km
- **M8WDM5.S60** - 8 Port 100Base-FX Single Mode/Single Fibre (SC) 1550nm Module 60Km

• Key Features of MS888G2 SNMP Managed Switches

QoS: The MS888G2 offers powerful Quality of Service (QoS) functions. This feature adds support of TOS fields within the IP packet header (equal DSCP low 3 bits) on Layer 3 of the network framework and 6 types of network transmission events on Layer 4. QoS support is important for real-time applications based on information taken from Layer 2 to Layer 4, such as VoIP.

VLAN: Support for Port-based VLAN and IEEE802.1Q Tagged VLAN, with support for 256 active VLAN's having VLAN ID's from 1 to 4094. The VLAN feature in the switch offers the benefits of both security and performance. VLAN is used to isolate traffic between different users which provides better security. Limiting the broadcast traffic to within the same VLAN broadcast domain also enhances performance.

Port Trunking: Allows two or more links to be aggregated together to form a Link Aggregation Group (LAG). Up to 12 Gigabit ports can be set up per trunk, and a switch can support up to 8 trunking groups. Port trunks are useful for switch-to-switch cascading, providing very high full-duplex connection speeds.

Port Mirroring: Port mirroring copies traffic from a specific port to a target port. This mechanism helps track network errors or abnormal packet transmission without interrupting the flow of data.

Bandwidth Control: All models support bandwidth allocation rating on a per port basis. Ingress and egress throughput can be limited to a pre-set level appropriate to the traffic generally handled on a specific port.

SNMP/RMON: SNMP is used to remotely monitor and configure SNMP aware devices from a central SNMP management device, such as SNMP software.
RMON is the abbreviation of Remote Network Monitoring and is a branch of the SNMP MIB.
All switch models support MIB-2 (RFC 1213), Bridge MIB (RFC 1493), RMON MIB (RFC 1757)-statistics Group 1,2,3,9, VLAN MIB (802.1Q, RFC2674),

Ethernet MIB (RFC 1643) and so on.

IGMP Snooping: IGMP Snooping provides a method for intelligent forwarding of multicast packets within a Layer 2 broadcast domain. By snooping IGMP registration information, a distribution list of workstations is formed that determines which end-stations will receive packets with a specific multicast address. The MS888G2 supports IGMP version 2 (RFC 2236).

Note: ** See Appendix A "Technical Specifications" for further details*

1.2. Checklist

Before you start installing your switch, verify that the package contains the following:

- A MS888G2 Modular SNMP Managed Switch
- Mounting Accessories (for 19" Rack Shelf mounting)
- This Users Manual CD-ROM
- RS-232 Console cable
- AC Power Cord

Please notify your supplier immediately if any of the aforementioned items are missing or damaged.

1.3. Features

The Alloy MS888G2 provides a comprehensive range of features:

- **Hardware**
- Supports 3x Modular 8 port 10/100Mbps Copper or 8 port 100Mb Fibre interfaces with a variety of fibre terminations.
- 2 Paired 10/100/1000Mbps or 1000Mbps SFP Mini-GBIC Ports
- Supports 256KB packet buffer and 128KB control memory
- 8K MAC address
- Maximum packet length of up to 1536 bytes
- Full-duplex flow control (IEEE 802.3x) and half-duplex backpressure
- Extensive front-panel diagnostic LED's; System: Power, Copper Ports: LINK/ACT, 10/100/1000Mbps, SFP Ports: SFP(LINK/ACT)
- **Management**
- Supports detailed port statistics and the ability to configure the speed, duplex and flow control settings of each port
- Supports per port traffic monitoring counters
- System information is displayed once logged in
- Supports port mirroring function
- Supports static trunk and LACP based Trunking
- Supports Port Based and 802.1Q VLAN's
- Supports user management via web interface and limits three users to login
- Supports broadcast storm suppression
- Trap events can be sent when certain events occur
- Configuration can be restored to factory default at the push of a button
- Hot Swappable SFP modules
- Supports Quality of Service (QoS) for real time applications based on the information taken from Layer 2 to Layer 4, such as VoIP
- Built-in web-based management and CLI management, providing a more convenient UI for the user
- Supports port mirroring function for ingress traffic
- Support for both spanning and rapid spanning tree (802.1w RSTP, 802.1d STP)
- Supports 802.1x authentication
- SNMP access can be disabled to prevent illegal SNMP access
- Supports Ingress, Non-unicast and Egress Bandwidth rating management
- The trap event and alarm message can be transferred via e-mail and mobile phone short message
- TFTP for firmware upgrade, system log upload and config file import/export

1.4. Overview of the MS888G2 Switch

Fig. 1-1: Front View of the MS888G2 Switch with modules

1.4.1. User Interfaces on the Front Panel (Button, LED's and Plugs)

There are 3 module slots for use with one of the many available modules for the MS888G2. The modules include 8 ports of 10/100Mbps copper or 8 ports of 100Mbps Fibre in a variety of fibre termination types. The LED display area, located on the right side of the panel, contains 2 Power LEDs (which indicate the power status of each of the power supplies in the switch) a CPU LED (which indicates whether the CPU is working correctly) and 6 LED's that indicate the status of each of the paired 10/100/1000Mbps Copper/1000Mbps Fibre ports on the switch.

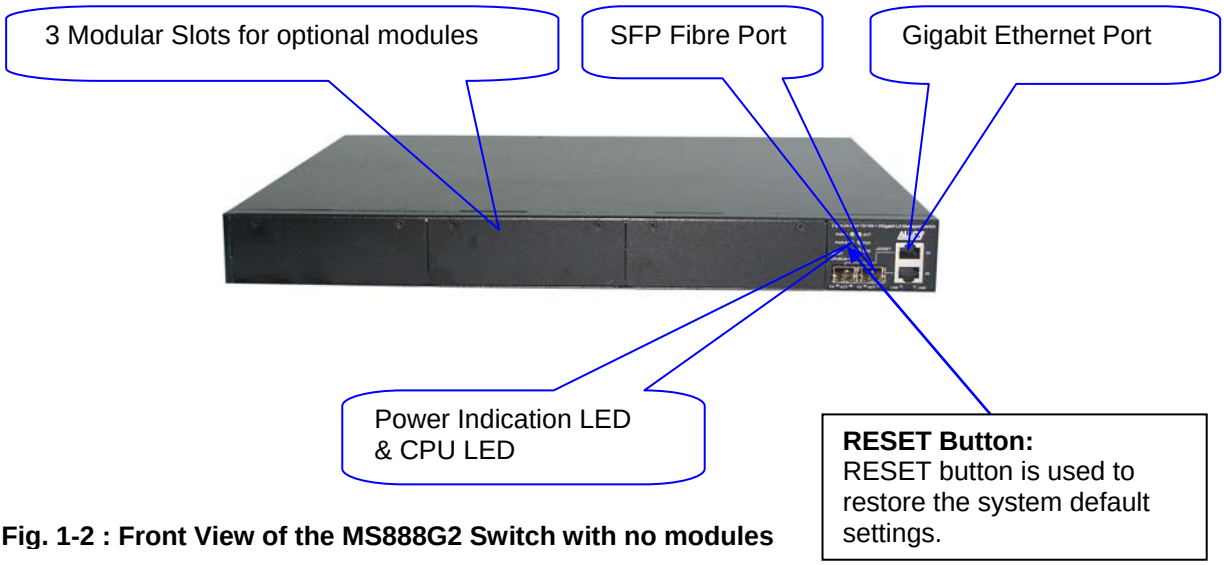

Fig. 1-2 : Front View of the MS888G2 Switch with no modules

LED Indicators

LED	Colour	Function
System LED		
CPU	Green	Blinks when CPU is active
POWER A	Green	Lit when power is active
POWER B	Green	Lit when power is active
ACT	Green	Lit when LEADSET is set to Activity mode
FDX	Green	Lit when LEADSET is set to Full Duplex mode
SPD	Green	Lit when LEADSET is set to Speed mode
LEDS for:	10/100/1000 Ethernet copper ports 25* & 26*	
LINK	Green	- On when connection with remote device is good - Off when no link is present
ACT	Green	- Blinks when any traffic is present
LEDS for:	SFP Gigabit Fibre Ports 25* & 26*	
FX	Green	- On when connection with the remote device is good - Off when no link is present
ACT	Green	- Blinks when any traffic is present

**All SFP ports are paired with one of the 10/100/1000Mbps copper RJ-45 ports. Only one of the paired ports can be used.*

1.4.2. User Interfaces on the Rear Panel

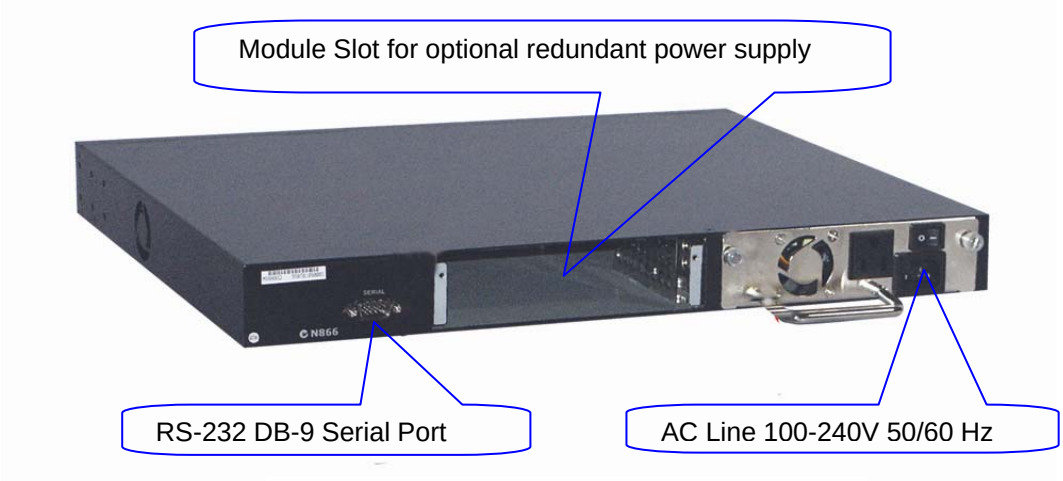

Fig. 1-3: Rear View of the MS888G2 Switch

1.5. Overview of the Optional SFP Modules

With the MS888G2, the SFP ports are paired with RJ-45 copper ports 25 and 26. Only one of any given paired port can be used. In this manner, these paired ports can be seen as 'Dual Media' ports that support 10/100/1000Mbps or 1000Mbps fibre via the SFP interfaces.
Optional 1000Mbps mini-GBIC fibre transceiver modules can be used for high-speed uplink connections to fibre backbones or servers, when installed in the SFP ports. A range of optional Alloy mini-GBIC modules are available:

Alloy Part No.	Description
MGBIC-T	1000Mbps, mini-GBIC, Copper, 100metres
MGBIC-MLC	1000Mbps multimode 1000Base-SX, 850nm, max. range 500m
MGBIC-SLC10	1000Mbps single-mode 1000Base-LX, 1310nm, max. range 10Km
MGBIC-SLC4013	1000Mbps single-mode 1000Base-LHX, 1310nm, max. range 40Km
MGBIC-SLC4015	1000Mbps single-mode 1000Base-LHX, 1550nm, max. range 40Km
MGBIC-SLC70	1000Mbps single-mode 1000Base-ZX, 1550nm, max. range 70Km
MGBIC-SLC100	1000Mbps single-mode 1000Base-EZX, 1550nm, max. range 100Km
MGBIC-WDMS3.20	1000Mbps WDM single-mode/single-fibre 1310nm, max. range 20Km
MGBIC-WDMS5.20	1000Mbps WDM single-mode/single-fibre 1550nm, max. range 20Km

Notes: * *The two WDM (Wave Division Multiplexer) mini-GBIC modules are designed to facilitate a link over a single core of single-mode fibre cable. The two units must be used in a paired manner, one at either end of the link.*

* *Mini-GBIC modules that are designed to the relevant standards should be compatible with any make of switch with SFP ports. If you have concerns regarding compatibility, please contact the supplier of your mini-GBIC product.*

* *The information given in the table above is current at time of publication; availability of individual Alloy mini-GBIC modules may vary over time.*

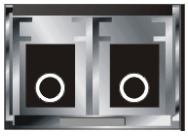

Fig. 1-4: Front View of 1000Base-SX/LX LC, SFP Fibre Transceiver

Fig. 1-5: Front View of 1000Base-LX WDM LC SFP Fibre Transceiver

2. Installation

2.1. Starting the MS888G2 Modular SNMP Managed Switch

This section provides a quick start guide for:

- Hardware and Cable Installation
- Management Station Installation
- Software booting and configuration

2.1.1. Hardware and Cable Installation

Please Note:

⇒ *Wear a grounding strap to avoid damaging the switch with an electrostatic discharge*

⇒ *Be sure that the power switch is in the 'OFF' position before you insert the power cord*

• Installing Optional SFP Mini-GBIC Modules

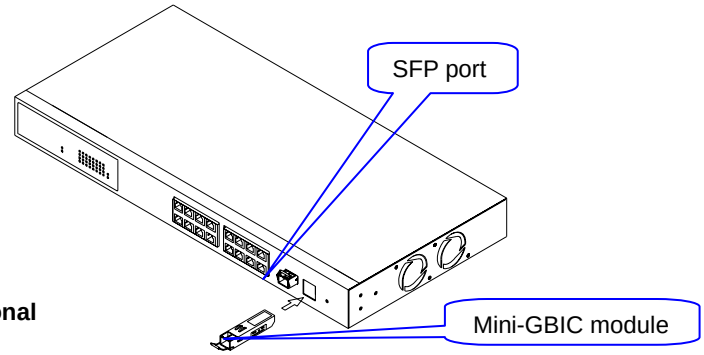

Fig. 2-1: Installation of optional SFP mini-GBIC

• Connecting the SFP Mini-GBIC Module to the Chassis:

The optional SFP Mini-GBIC modules are hot-swappable, so you can plug or unplug them while the power is applied to the switch.

1. Verify that the mini-GBIC module is compatible with the SFP port on the switch (for example, some switch manufacturer's design their mini-GBIC modules to be operable only in their branded devices).
2. Verify that the type of mini-GBIC you have selected for use will be compatible with the type of fibre optic cable that is to be used.
3. Verify that the type of mini-GBIC you have selected for use will be compatible with the fibre optic transceiver at the other end of the link (e.g. – compatible wavelength and standard).
4. Slide the module along the slot and ensure that the module is properly seated against the SFP slot socket/connector.
5. Install the media cable for network connection.
6. Repeat the above steps, as needed, for each module to be installed into the switch.

• Installing Optional 8 Port Copper or Fibre Modules

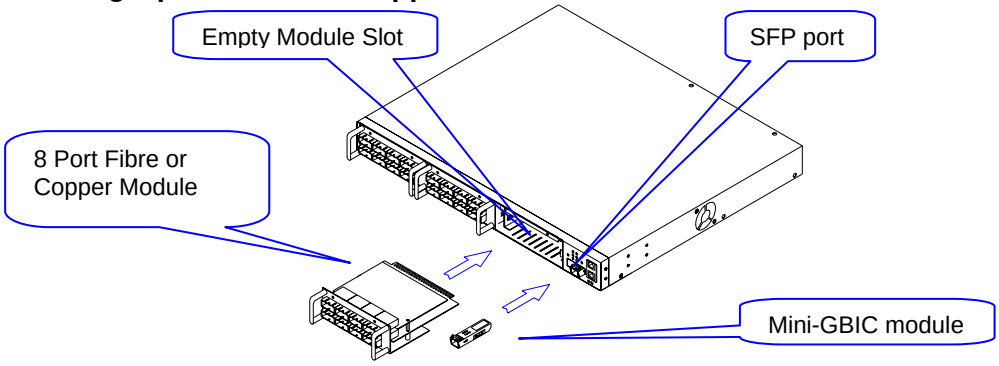

Fig. 2-2: Installation of optional Copper or Fibre Module

• Connecting the Module to the Chassis:

All modules are hot-swappable, so you can plug or unplug them while the power is applied to the switch.

1. Verify that the type of module you have selected for use will be compatible with the type of fibre optic cable that is to be used.
2. Verify that the type of module you have selected for use will be compatible with the fibre optic transceiver at the other end of the link (e.g. – compatible wavelength and standard).
3. Slide the module along the slot and ensure that the module is properly seated against the socket/connector.
4. Install the media cable for network connection.
5. Repeat the above steps, as needed, for each module to be installed into the switch.

• Copper Ports - Cable Installation

Please Note:

⇒ *The RJ-45 ports on the MS888G2 support MDI/MDI-X auto-crossover functionality. This enables use of either straight-through or crossover UTP cable types; the RJ-45 ports will automatically be configured to suit the characteristics of the device at the remote end of the link.*

⇒ *The RJ-45 ports on the MS888G2 support Nway auto-negotiation; the ports will automatically be configured to be compatible with the speed and duplex settings of the device at the remote end of the link.*

⇒ *The minimum grade of cable for use with the switch is Cat. 5 grade UTP or STP. Higher grades of UTP/STP cable may also be used to connect to the copper RJ-45 ports.*

1. Depress the clip on the RJ-45 connector and push into the RJ-45 port. Release connector and ensure that the cable connector is securely locked into the RJ-45 port.

2. Repeat the above steps, as needed, for each RJ-45 port to be connected.

• Power On

Please Note:

⇒ *The Alloy MS888G2 uses a 100-240 VAC, 50-60 Hz power supply. The power supply will automatically convert your local AC power source to DC power for use by the switch.*

1. Ensure that the power switch is turned off before connecting mains power.
2. Connect the power cord supplied with the switch to your nearest mains outlet.
3. Connect the other end of the power cord into the IEC power port on the switch.
4. Repeat above steps for each power supply module.
5. Turn the switch on.
6. When initial power is applied, all the LED indicators will light up for a brief period while the system performs its startup tests. Once the initial tests ('POST test') have completed all except the power and CPU LED should return to an off state.

• Firmware Loading

After power on, the boot-loader will load the switch firmware into the main operational memory. This process will take about 30 seconds. Once completed, the switch will flash all the LED's once and then switch to a ready state.

2.1.2. Cabling Requirements

To help ensure a successful installation and keep network performance at optimum levels, take care to use Cat.5e grade or higher cabling. Ensure that stranded core UTP cable, if used, runs for no more than 10 metres, and that solid core runs for a maximum of 100 metres. Poor cabling is the most common cause for network dropouts or poor performance.

2.1.2.1. Cabling Requirements for UTP Ports

- For Ethernet copper network connections, the UTP cable used must be Cat. 3 grade as a minimum, with a maximum length of 100 metres
- For Fast Ethernet copper network connections, the UTP cable used must be Cat. 5 grade as a minimum, with a maximum length of 100 metres
- For Gigabit Ethernet copper network connection, UTP cable used must be Cat.5 grade or higher, with a maximum length of 100 metres. Cat.5e grade UTP cable is recommended.

2.1.2.2. Cabling Requirements for 100Base-FX Modules

There are two categories of fibre optic modules - multimode (MM) and single-mode (SM). The later come in different models depending on the distance required. Modules for the MS888G2 come with a variety of fibre interfaces including SC, ST, MT-RJ and WDM SC.

The following table lists the types of fibre optic cable that are supported by modules installed in the Alloy MS888G2. Other cable types not listed here may be supported; please contact the supplier of your switch for details.

<table>
<tr><td rowspan="2">100Base-FX 1310nm Fibre Module Models</td><td colspan="2">8-port Fibre module: SC SM *5/20/60Km single mode*</td></tr>
<tr><td colspan="2">ST/SC/MT-RJ multi-mode *2Km</td></tr>
<tr><td rowspan="4">100Base-FX Single Fiber WDM Module</td><td rowspan="2">Single-mode *20Km</td><td>TX(Transmit) 1310nm</td></tr>
<tr><td>RX(Receive) 1550nm</td></tr>
<tr><td rowspan="2">Single-mode *20Km</td><td>TX(Transmit) 1550nm</td></tr>
<tr><td>RX(Receive) 1310nm</td></tr>
</table>

2.1.2.3. Cabling Requirements for 1000SX/LX/ZX SFP Modules

There are two categories of fibre optic modules - multimode (MM) and single-mode (SM). The later is categorised into several classes by the distance it supports. These are SX, LX, LHX, ZX and EZX. The majority of mini-GBIC modules available use a LC type connector. The connector types used currently on Alloy mini-GBIC modules are LC and WDM SC, for the following module types:

- Gigabit Fibre with multimode LC SFP mini-GBIC modules
- Gigabit Fibre with single-mode LC mini-GBIC modules
- Gigabit Fibre with single-mode/single core WDM SC 1310nm SFP mini-GBIC modules
- Gigabit Fibre with single-mode/single core WDM SC 1550nm SFP mini-GBIC modules

The following table lists the types of fibre optic cable that are supported by SFP mini-GBIC modules installed in the Alloy MS888G2. Other cable types not listed here may be supported; please contact the supplier of your switch for details.

IEEE 802.3z Gigabit Ethernet 1000SX 850nm	**Multimode Fibre Cable and Modal Bandwidth**			
	Multimode 62.5/125μm		Multimode 50/125μm	
	Modal Bandwidth	Range	Modal Bandwidth	Range
	160MHz-Km	220m	400MHz-Km	500m
	200MHz-Km	275m	500MHz-Km	550m
1000Base-LX/LHX/XD/ZX	**Single-mode Fibre 9/125μm**			
	Single-mode transceiver 1310nm 10Km, 40Km			
	Single-mode transceiver 1550nm 40Km, 70Km, 100Km			
1000Base-LX Single Fibre (WDM SC)	Single-mode *20Km		TX(Transmit)	1310nm
			RX(Receive)	1550nm
	Single-mode *20Km		TX(Transmit)	1550nm
			RX(Receive)	1310nm

Cont. Please Note:

⇒ *Further information can be found in section 1.5 on page 7*

⇒ *All figures denoting the range a given cable type can achieve must be treated as maximum values. A number of variables can limit the actual range that can be achieved – grade of cable used, quality of cable, and presence of joins in cable runs, for example*

2.1.3. Management options available with the MS888G2

The MS888G2 supports multiple management options to allow administrators to quickly configure and monitor the switch and network performance. There are four management options available including RS-232 console, Command Line Interface (CLI), SNMP or via the built in Web Management. The following procedures will briefly describe how each method can be performed and will also be discussed in more detail later in this manual.

Section 2-1-3-1: Configuring the MS888G2 through the RS-232 serial port.

Section 2-1-3-2: Configuring the MS888G2 through the Ethernet port.

2.1.3.1. Configuring the MS888G2 through the RS-232 serial port

When configuring the MS888G2 via the RS-232 console please connect the switch via the provided serial cable to a DCE device such as a PC. Once you have connection run a terminal emulation program such as Hyper Terminal. When connecting to the switch please use the serial settings of the switch to create the connection, the default settings are below:

Baud Rate: 57600

Data Bits: 8

Parity: None

Stop Bits: 1

Flow Control: None

By pressing Enter you will now be prompted to login to the switch.

The default username and password for the switch is:

Username: admin

Password: admin

The RS-232 console port on the switch is mainly used for the initial setup of the switch including setting the IP Address, Subnet Mask and Gateway. It is recommended that all other management duties that need to be performed should be done via the Web Management or CLI.

To set or change the default IP address of the switch via the console port, please follow the steps below:

1. Log into the switch via hyper terminal using the above settings.

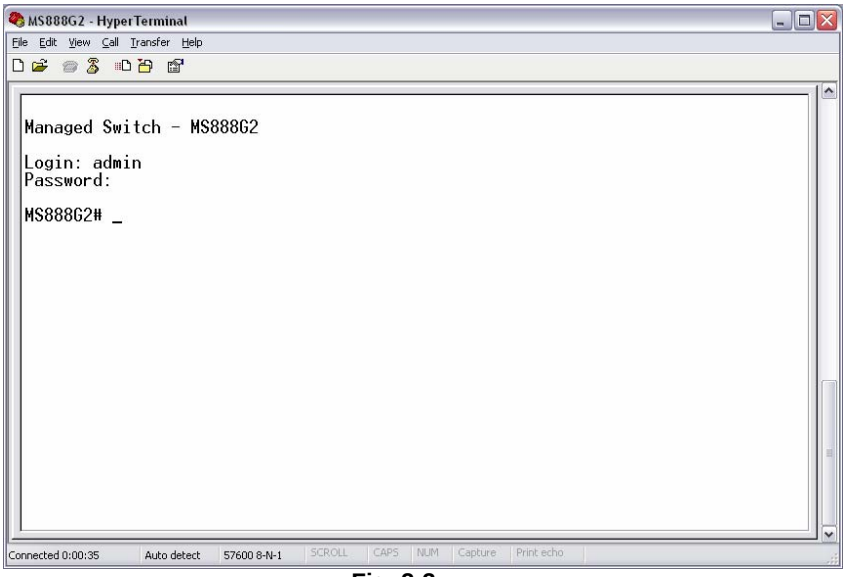

Fig. 2-3

2. Type **IP** and press **Enter** to enter the IP configuration mode.
3. Type **set ip "IP Address" "Subnet Mask" "Gateway"** where "IP Address" is the IP address of the switch, "Subnet Mask" is the subnet mask of the switch and "Gateway" is the gateway address of the switch, then press **Enter**.
4. Type **save start** to save the new switch configuration as the startup configuration for the switch.
5. Type **logout** to exit the switch's management.

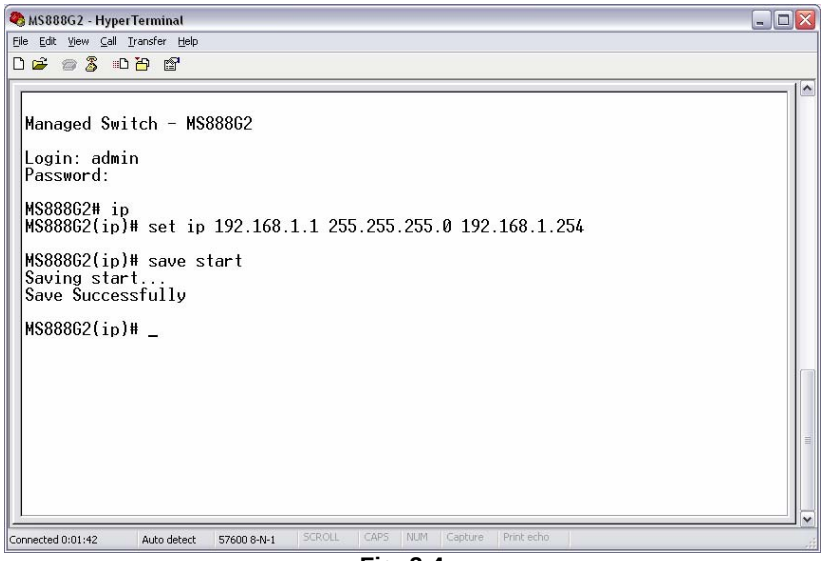

Fig. 2-4

2.1.3.2. Configuring the MS888G2 through the Ethernet Port

There are three different methods of configuring the MS888G2 through the Ethernet Port. They are CLI, Web Browser and via SNMP Management Software. We will not cover SNMP management in this manual as it will vary depending on the Network Management Software that is being used.

Note: MIB files can be located for the switch on the CD-ROM, which can then be used with your Network Management Software.

The default IP Address, Subnet Mask and Gateway addresses are shown below:

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.254

To be able to communicate with the switch via the Ethernet port you will need to ensure that your computer has an IP Address in the same subnet range.

Eg. 192.168.1.5

If using the web management open a web browser and enter the default IP Address of the switch into the address bar.

You will now be prompted to log into the switch, the default username and password is shown below:

Username: admin

Password: admin

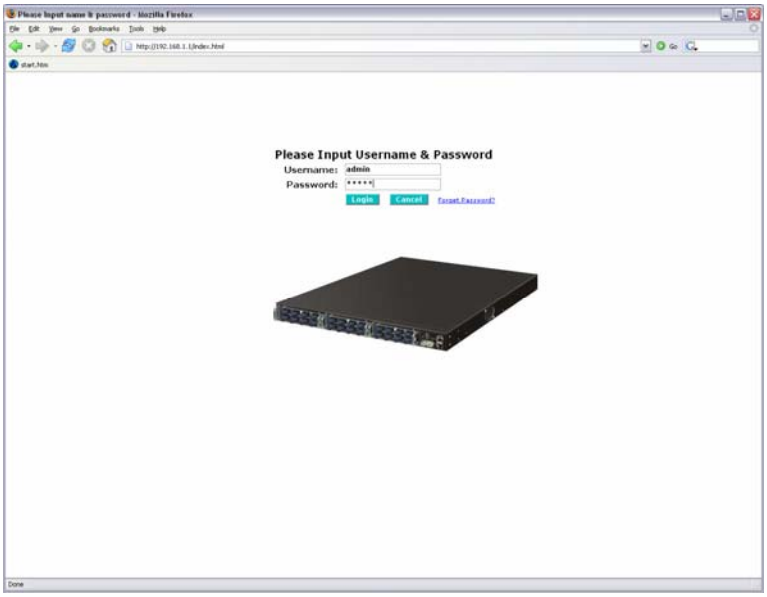

Fig. 2-5

Note: The web management configuration will be covered in detail in Chapter 3.

If using the CLI open a command prompt and create a telnet session to the default IP Address of the switch.

You will now be prompted to log into the switch, the default username and password is shown below:

Username: admin

Password: admin

Fig. 2.5

Note: The CLI configuration will be covered in detail in Chapter 4.

3. Operation of the Web Based Management

The following chapter allows the administrator to monitor and manage the MS888G2 through the web management interface. Management functionality such as Port Based and 802.1q VLAN, Port Aggregation (Trunking), QoS, Port configuration and much more can all be configured quickly and easily via any port of the MS888G2 switches.

To access the web management of the MS888G2 open a web browser such as Internet Explorer or Mozilla Firefox and enter the default IP address into the address bar.
The default network settings for the MS888G2 are shown below:

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.254

Username: admin

Password: admin

Once you have entered the IP address of the MS888G2 into a web browser you will be prompted with a login screen where you will need to enter a valid username and password to gain access to the switch. The default username and password are shown above.

The MS888G2 only allows one administrator to configure the switch at one time. If another user has logged into the switch with the administrator credentials then only the first admin logged in will be able to configure the switch, the other admin will only be able to monitor the switch. Other users can also be created to gain access to the switch for monitoring purposes only. In total only three users can have access to the web management at any one time.

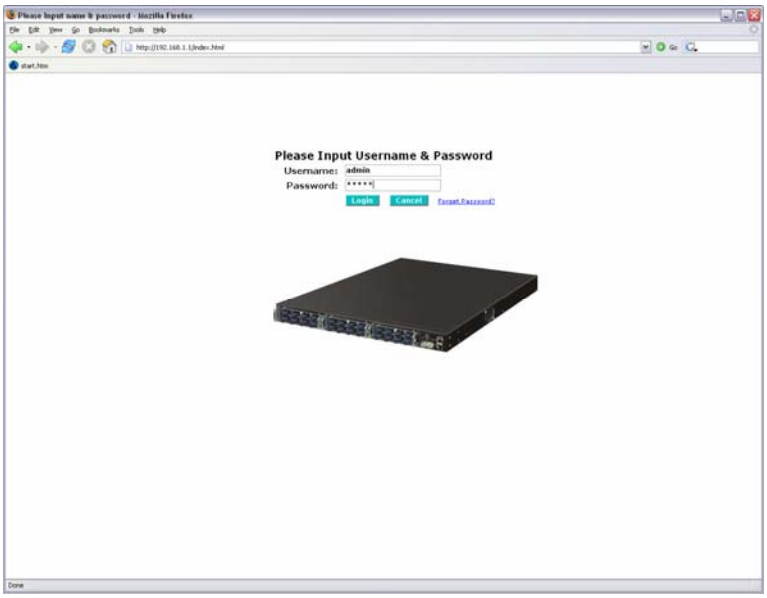

Fig. 3-1

3-1. Web Management Home Overview

Once you have entered a valid username and password and logged into the switch the System Information page will be displayed, this is the default page, it will be displayed every time that you log into the switch.

The System Information page gives you all relevant information regarding the switch including, Model Name, System Description, Location, Contact, Device Name, System Up Time, Current Time, BIOS Version, Firmware Version, Hardware-Mechanical Version, Serial Number, Host IP Address, Host MAC Address, Device Port, RAM Size and Flash Size.

Fig. 3-2

- System Information Page Layout

At the top of the page, there is a picture of the front panel of the switch. The picture displays the port status of each of the ports on the switch. If the port is green this tells us that the port has an active connection, if the port is grey then no link is present. You can then click on each of the ports to give you basic information.

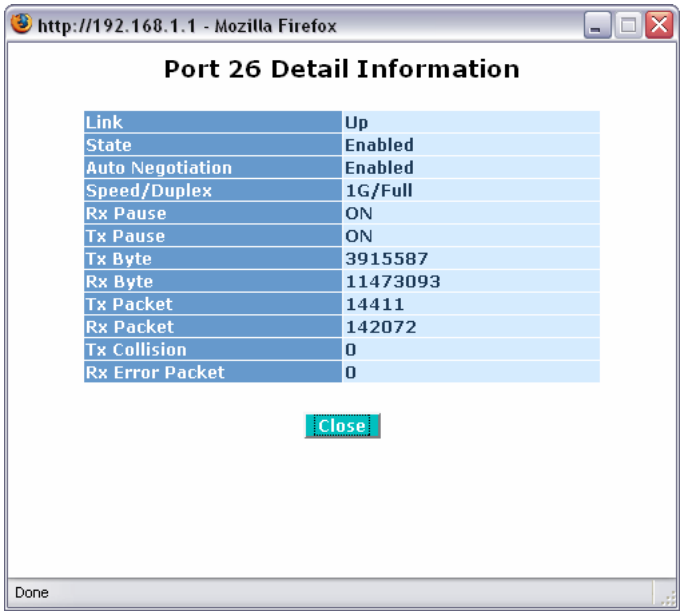

Fig. 3-3

As you can see from the image above, when you click on a particular port, basic information for that port will be displayed.

At the top left corner of the page is a drop down box that allows the administrator to enable and set the time out value for the Auto Logout function. If the switch's Auto-Logout time is set to 3 minutes, after 3 minutes of no activity the switch will automatically log the user out of the web interface. The Auto Logout function can also be turned off.

At the left hand side of the screen is the main menu tree. This menu is used to navigate your way around the switch's web interface. The image below shows the menu tree for the web interface:

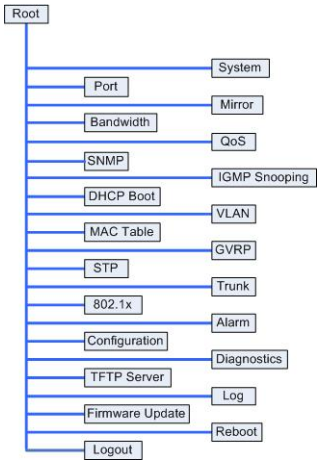

Fig. 3-4

3-1-1. System Information

Allows the Administrator to view basic system settings.

Fig. 3-5

Function Name:

System Information

Function Description:

Shows the basic system information

Parameter Description:

Model Name:

The model name of the device. (Read Only)

System Description:

Gives you a description of the switch. (Read Only)

Location:

Specify a descriptive location name.
Location name can be up to 36 Alphanumeric Characters long.
Click the ***<apply>*** button to update. (Read/Write)

Contact:

Specify the System Administrator.
Contact name can be up to 36 Alphanumeric Characters long.
Click the ***<apply>*** button to update. (Read/Write)

Device Name:

Specify a descriptive device name for the switch.
Location name can be up to 36 Alphanumeric Characters long.
Click the ***<apply>*** button to update. (Read/Write)

System Up Time:

The time accumulated since last power up. Format is Day, Hour, Minute, Second. (Read Only)

Current Time:

Shows the system time of the switch. Format is Day of week, Month, Day, Hours, Minutes, Seconds, Year. Eg Mon Jan 16 3:46:49 2006 (Read Only)

BIOS Version:

The version of the BIOS in the switch. (Read Only)

Firmware Version:

The firmware version in the switch. (Read Only)

Hardware-Mechanical Version:

The hardware-mechanical version of the switch. (Read Only)

Serial Number:

The serial number assigned to the switch. (Read Only)

Host IP Address:

The IP Address of the switch. (Read Only)

Host MAC Address:

The MAC Address of the switch. (Read Only)

Device Port:

Specifies the port density and types of ports on the switch. (Read Only)

RAM Size:

The size of the DRAM in this switch. (Read Only)

Flash Size:

The size of the flash memory in the switch. (Read Only)

3-1-2. IP Configuration

The IP configuration is used to set the IP settings in the switch. The MS888G2 supports either a static IP address allocated to them via the system administrator or can be assigned an IP address dynamically from a DHCP server on your network. The IP address is used to gain access to the management functionality of the switch.

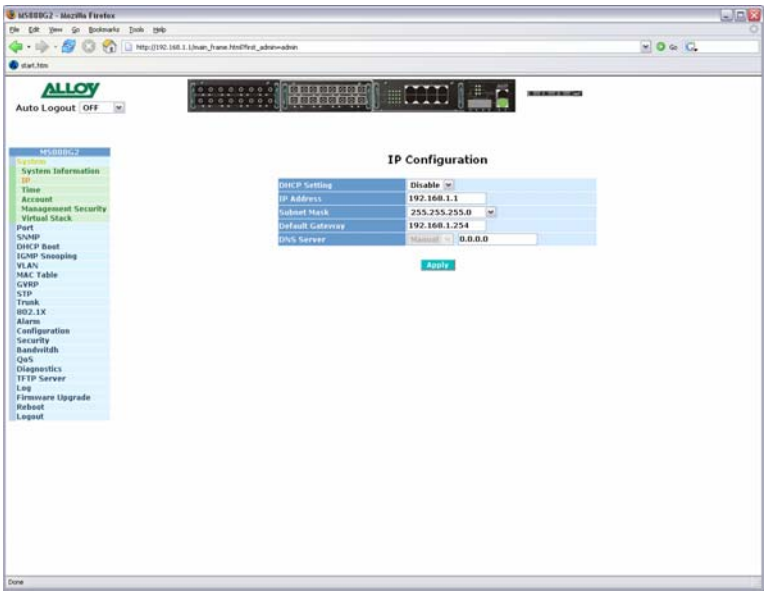

Fig. 3-6

Function Name:

IP Configuration

Function Description:

Is used to set the IP Address, Subnet Mask, Default Gateway and DNS settings for the switch

Parameter Description:

DHCP Setting:

The MS888G2 supports DHCP (Dynamic Host Configuration Protocol) Client which is used to receive an IP Address from a DHCP Server running on your network. By Default the DHCP Client is disabled and a Static IP Address has been allocated to the MS888G2. When Enabled the switch will receive an IP Address from an existing DHCP Server on your network. If Disabled you will need to allocate an IP Address in the spaces provided.
Click the ***<apply>*** button to update.

Default: Disabled

IP Address:

If the DHCP settings are set to Disabled you will need to set a manual IP Address for the switch.
Enter the required IP Address in the space provided.
Click the ***<apply>*** button to update.

Default: 192.168.1.1

Subnet Mask:

You will also need to specify a Subnet Mask to be used on your network.
Enter the required Subnet Mask in the space provided.
Click the ***<apply>*** button to update.

Default: 255.255.255.0

Default Gateway:

The Default Gateway is used in routed networks to determine the next hop for all non local destinations.
Enter the required Default Gateway in the space provided.
Click the ***<apply>*** button to update.

Default: 192.168.1.254

DNS:

DNS (Domain Name Server) is used to translate between Host Names and IP addresses. If DHCP has been enabled the switch will receive a DNS IP Address dynamically from the DHCP Server. If you are not using DHCP you will need to set a DNS address in the switch. A DNS Server address should be given to you from your ISP.
Enter the required DNS Server in the space provided.
Click the ***<apply>*** button to update.

Default: 0.0.0.0

3-1-3. Time Configuration

The MS888G2 provides two methods to keep the switch's time settings correct, they are via manual input and via a Time Server on the internet. If you are manually entering your time settings enter the "Year", "Month", "Day, "Hour", "Minute" and "Seconds" into the space provided. If you enter a number that is invalid, for instance you enter 61 in the seconds field it will be rounded down to the nearest valid number, in this case 59.

If you are using NTP (Network Time Protocol) there are four built in Internet Time Servers that you can use, or there is a space provided where you can enter a particular Time Server address. When using NTP you will also need to specify what time zone you are presently located in. The Time Zone is Greenwich-centered which uses the expression form of GMT +/- xx hours.

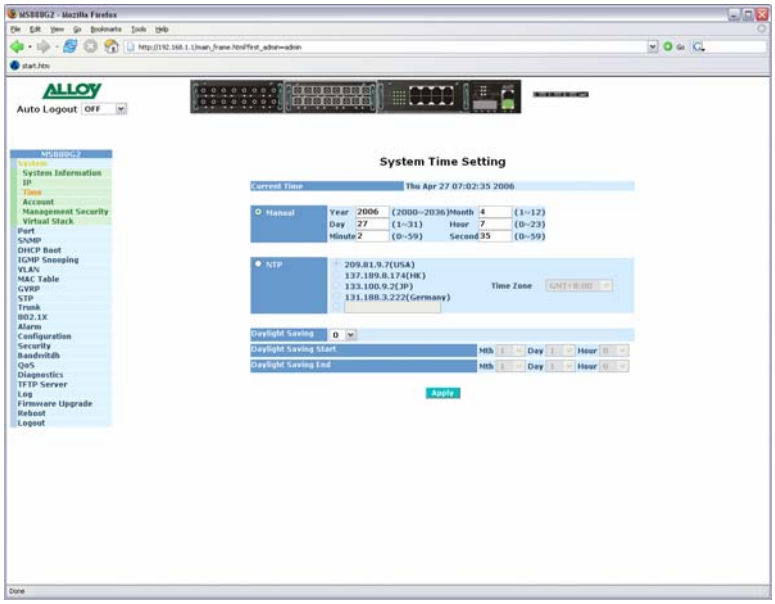

Fig. 3-7

Function Name:

Time Configuration

Function Description:

Enter a manual system time or synchronise the MS888G2's time with an available Internet Time Server. Daylight Saving time adjustment is also supported for different locations.

Parameter Description:

Current Time:

Shows the current system time.

Manual:

A manual time can be set into the switch here. Enter the Year, Month, Day, Hour, Minute and Seconds into the spaces provided. The valid figures for the parameters Year, Month, Day, Hour, Minute and Seconds are >= 2000, 1 – 12, 1 – 31, 0 – 23, 0 – 59, respectively. Once you have entered the correct time click the ***<apply>*** button to update.

Default: Year 2000, Month = 1, Day = 1, Hour = 0, Minute = 0, Second = 0

NTP:

NTP is used to sync the network time with a time server on the internet based on the Greenwich Mean Time (GMT). Once the user has selected one of the built in time servers or entered a manual time server and selected the correct time zone click the ***<apply>*** button to update. The switch will now sync with the selected time server. However this synchronisation does not occur periodically if the time does become out of sync for some unknown reason the administrator will manually have to click the apply button again to re-sync with the time server.

The Time Zone is an offset time of the GMT. The switch supports a configurable time zone from -12 to +13 hours in increments of 1 hour.

Default: +8 hours

Daylight Savings:

Daylight Savings can be configured from -5 ~ +5 hours in increments of 1 hour. If your location has adopted daylight savings please enter the appropriate value in the daylight savings drop down box. If your area does have daylight savings you will need to enter a starting and ending date of the daylight savings period. Once the date passes the starting date of the daylight savings settings the switch's time will be adjusted by the amount of hours entered in the drop down box. Click the ***<apply>*** button to update.

Default: 0

Default values for starting and ending date:

Start: Month = 1, Day = 1, Hour = 0

End: Month = 1, Day = 1, Hour = 0

3-1-4. Account Configuration

The account configuration is used to create or modify guest and administrator accounts. The MS888G2 allows the administrator to create up to 5 guest accounts. Accounts can only be created by the administrator. When a Guest user logs into the switch they will not be able to modify any parameters, they only have read only rights to the switch. A Guest user can log into the switch and change there own password, but will not be able to modify any other accounts. The Guest account is purely created for monitoring purposes only. Administrators have the ability to delete accounts and also change the username and passwords of each account. The Administrator account can not be deleted.

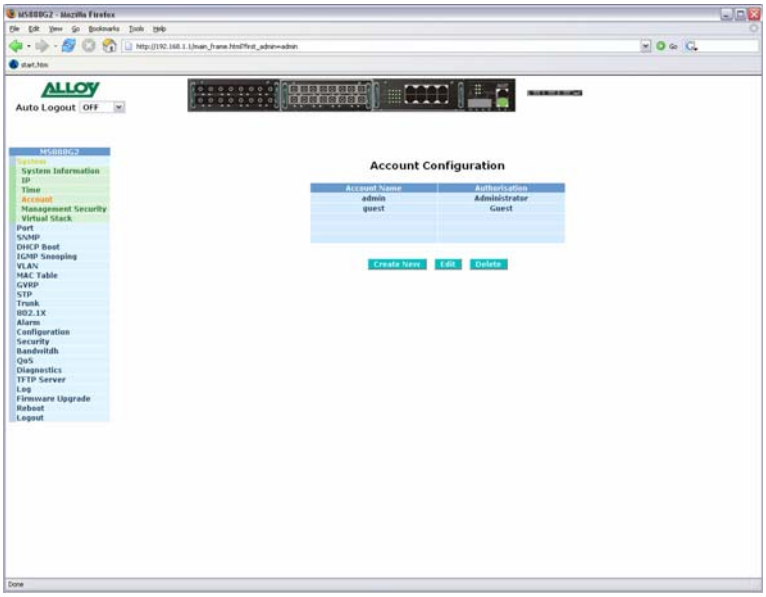

Fig. 3-8

Function Name:

Account Configuration

Function Description:

Create and Modify Administrator and Guest accounts.

Parameter Description:

Create New:

Click the Create New button to create a new guest account.

Edit:

Click the Edit button to edit an existing account, please ensure that you click on an account before clicking the Edit button.

Delete:

Select the account that you want to delete and click the Delete button.

Authorisation:

Specifies what rights the user has. Only Administrator and Guest accounts can be created.

Username:

Please enter a username for the administrator or guest account, a maximum of 15 alphanumeric characters only.

Password:

Please enter a password for the administrator or guest account, a maximum of 15 alphanumeric characters only.

Confirm Password:

Please confirm the password.

3-1-5. Management Security Configuration

The Management Security Configuration is used to implement security rules based on what type of management access a certain user has. The user management can be locked down so that only users that belong to a certain VLAN group or have a valid IP address in a predetermined range can access the switch's management interfaces. Rules can also be created to allow access to management from certain switch ports only. Eg only port 5 has access to the switch's management. Rules can then be broken down even further to allow particular management access to these VLAN groups, IP Ranges or Ports. We can specify whether we want to allow or deny access to the Web Management, Telnet or SNMP access.

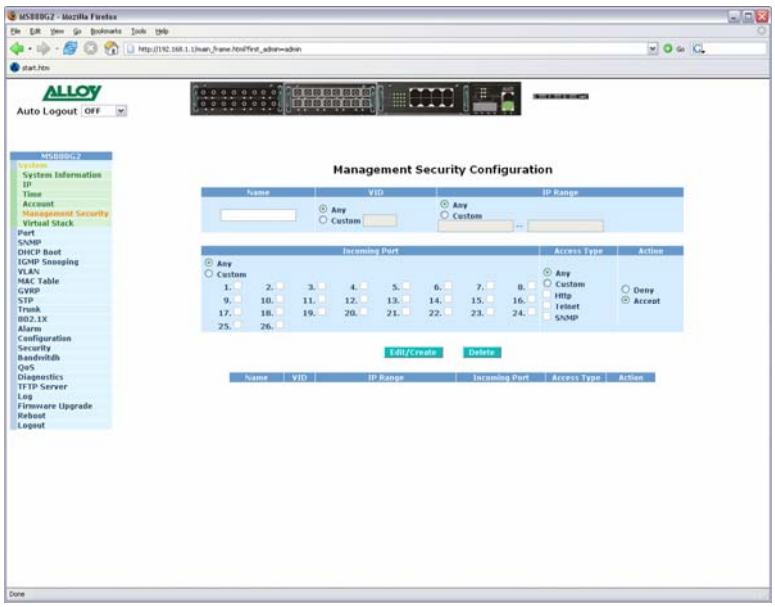

Fig. 3-9

Function Name:

Management Security Configuration

Function Description:

Create rules based access to the management features of the MS888G2.

Parameter Description:

Name:

Please enter a descriptive name for the Rule.

VID:

If you wish to lock the management down to a particular VLAN group please highlight the Custom radio button and enter the VID. Otherwise select the Any radio button.

IP Range:

If you wish to lock the management down to a particular IP range please select the Custom radio button and enter the IP range in the space provided. Otherwise select the Any radio button.

Incoming Port:

If you want to lock the management interface access down to certain ports on your switch please select the Custom radio button and tick the required ports which will allow/deny access to the management. Otherwise select the Any radio button.

Access Type:

After you have determined what physical access has been granted or denied to the management you now need to specify what management access is allowed. If you wish to allow/deny a particular type of access, select the Custom radio button and select the type of access required, HTTP, Telnet or SNMP. Otherwise select the Any radio button.

Action:

Now that you have created your management access rule you now need to specify whether the rule is going to be used to allow or deny access to the management. Select the desired radio button.

Edit/Create:

Once you have configured your management access rule click the Edit/Create button to add the rule.
If you have an existing rule that you want to edit select the rule from the list, make your changes and click on the edit button.

Delete:

Select a rule from the list and click the Delete button to remove that rule.

3-1-6. Virtual Stack Configuration

The Virtual Stack function allows multiple MS888G2 switches to be managed from a single IP Address. One MS888G2 will be configured as a Master and all other MS888G2 switches will be configured as Slaves. You can then apply a group name to the virtual stack, only one master switch can exist within the same group name. Administrators will only need to know the IP address of the master switch to gain access to all MS888G2 switches on the network.

An additional table will appear above the web management screen showing all switches that belong to the virtual stacking group. Each switches web interface can be accessed from the push of a button.

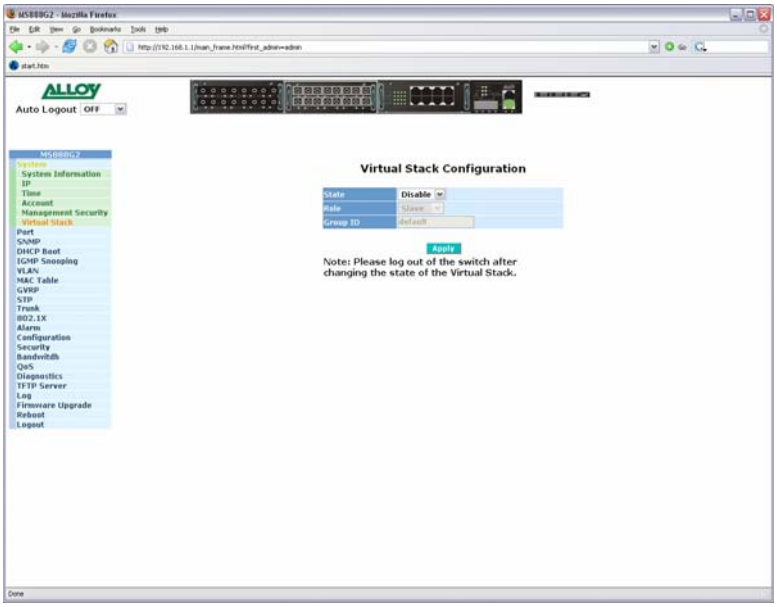

Fig. 3-10

Function Name:

Virtual Stack Configuration

Function Description:

This function is used to allow Administrators a way of configuring multiple MS888G2 switches from a single IP/Web Management interface.

Parameter Description:

State:

This is where you will Enable or Disable the Virtual stacking function. Select the required value and click the ***<apply>*** button to update.

Role:

Select whether the switch will be a Master or a Slave and click the ***<apply>*** button to update.

Group ID:

Enter a value for the group ID; this ID must match all other switches in your virtual stack. A maximum of 15 alphanumeric characters can be used.
Click the ***<apply>*** button to update.

3-2. Port Configuration

The Port Configuration section consists of four sub sections Status, Configuration, Simple Counter and Detail Counter. These four sections are used to control and monitor all ports on the MS888G2.

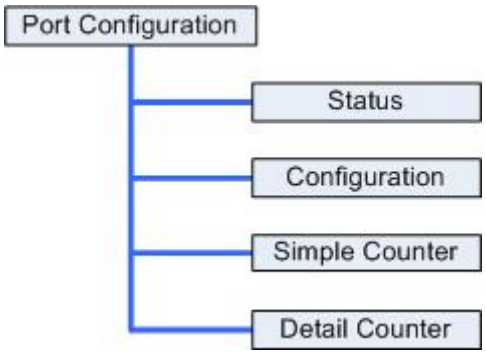

Fig. 3-11

3-2-1. Port Status

The Port Status section allows the administrator to view the current status of each port. The port status screen tells us the type of media being used, whether the link is active or not, whether the port is active or not, if it is using auto negotiation, what speed the port is running at and whether flow control is enabled. Additional Information is also available for ports 25 and 26 when running SFP modules.

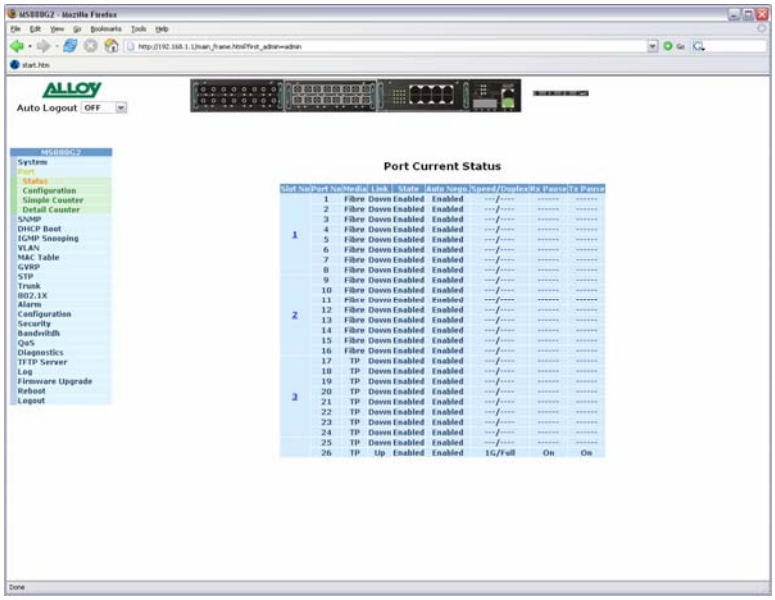

Fig. 3-12

Function Name:

Port Status

Function Description:

Reports the current Status of each port; if the state of a port changes the status screen will refresh every 5 seconds.

Parameter Description:

Slot No:

Displays each module slot available on the switch.

Port No:

Displays every port on the switch.

Media:

Displays what type of media the port is using. Media will be either TP (Twisted Pair) or Fibre.

Link:

Tells you whether the ports link state is Up or Down, Up being active and Down being inactive.

State:

Shows whether the port is enabled or disabled. If Enabled, traffic can be transmitted and received from that port, if Disabled, no traffic can be passed through this port.

Default: Enabled

Auto Negotiation:

Shows whether the port is running in auto-negotiation or forced mode. If running in auto-negotiation mode Enabled will be displayed, if running in forced mode, Disabled will be displayed. Auto-negotiation is used to automatically detect what speed and duplex settings the connecting device is using.

Default: Enabled

Speed / Duplex Mode:

Displays the Speed and Duplex settings of each port. Speed settings can either be 10Mbps, 100Mbps or 1000Mbps for Copper supporting both Half and Full Duplex or 1000Mbps Full Duplex for Fibre. If running in Auto-negotiation mode the speed and duplex settings will be determined by the connecting device. If you have forced the speed and duplex settings for a port, these settings will be displayed here. If the port does not have an active link and is configured to run in auto-negotiation mode then Auto will be displayed.

Flow Control:

Shows the port's flow control status. The MS888G2 supports both Backpressure flow control for Half Duplex and Pause flow control for Full Duplex.

Default: Enabled

If you have a valid link on a Fibre port you will be able to see some detailed information for that port by clicking on the port number in the Port Status screen.

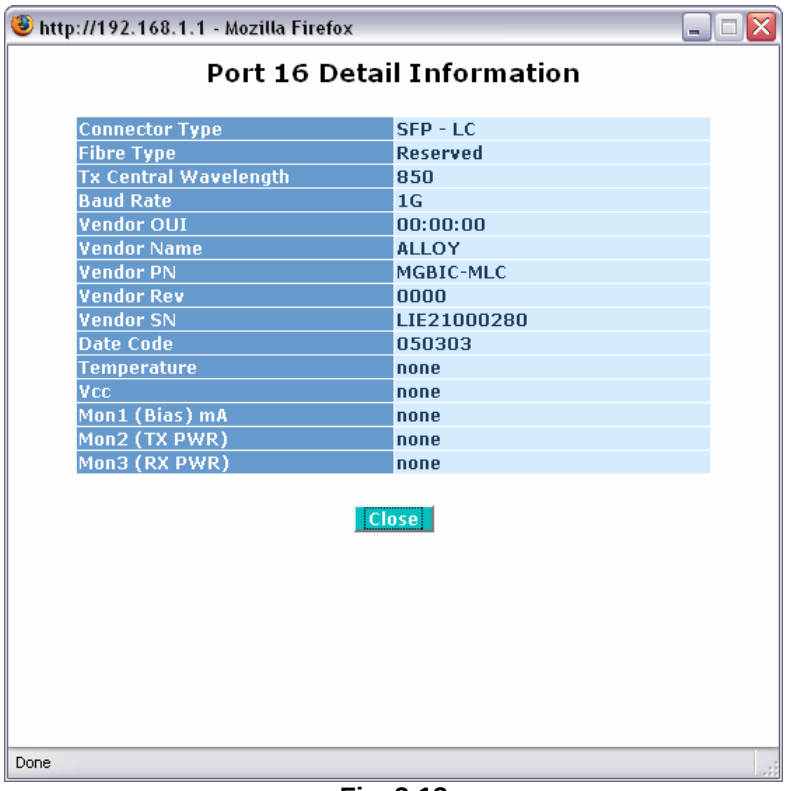

Fig. 3-13

Parameter Description for all Fibre Ports:

Connector Type:

Displays the connector type for that port, for instance, UTP, SC, ST, LC and so on.

Fibre Type:

Displays the type of fibre being used, for instance, Multimode or Single-Mode.

TX Central Wavelength:

Displays the fibre optical transmitting central wavelength, for instance, 850nm, 1310nm, 1550nm and so on.

Baud Rate:

Displays the maximum speed the SFP module supports.

Vendor OUI:

Displays the manufacturers OUI code which is assigned by the IEEE.

Vendor Name:

Displays the company name of the SFP module manufacturer.

Vendor PN:

Displays the part number of the SFP module.

Vendor Rev:

Displays the revision number of the SFP module.

Vendor SN:

Displays the serial number of the SFP module.

Date Code:

Displays the date the SFP module was manufactured.

Temperature:

Displays the current temperature of the SFP module.

Vcc:

Shows the current working voltage of the SFP module.

Mon1(Bias) mA:

Shows the Bias current of the SFP module.

Mon2(TX PWR):

Shows the transmit power of the SFP Module.

Mon3(RX PWR):

Shows the receive power of the SFP Module.

3-2-2. Port Configuration

The Port Configuration section allows the administrator to Enable or Disable a port, turn auto negotiation on or off for a particular port and also force the speed and duplex settings of each port. The administrator can also Enable or Disable the flow control settings for each port.

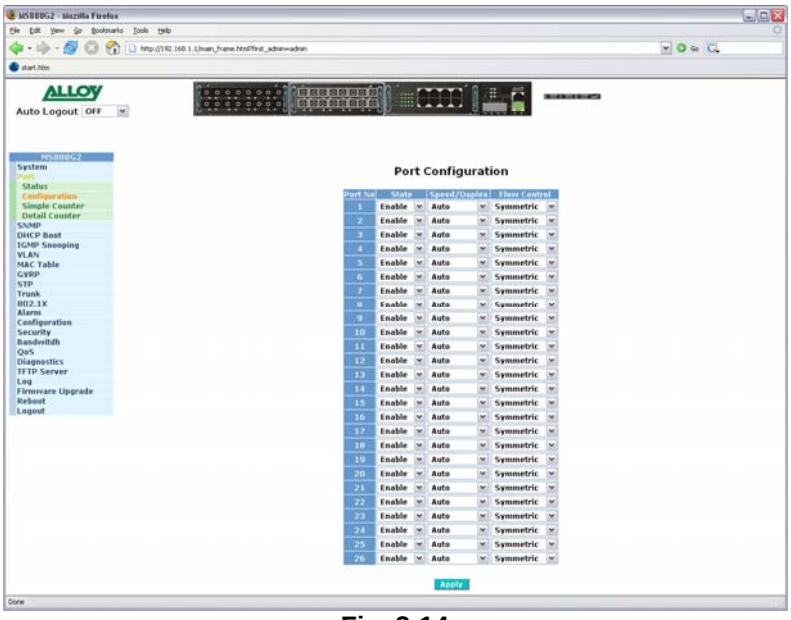

Fig. 3-14

Function Name:

Port Configuration

Function Description:

Allows the Administrator to manually enable or disable a port, disable auto-negotiation and force the speed of a port and also allow flow control to be enabled or disabled for each port.

Parameter Description:

Port No:

Displays every port on the switch.

State:

Shows whether the port is enabled or disabled, if Enabled traffic can be transmitted and received from that port, if Disabled no traffic can be passed through this port. If a cable is plugged into a port and the port is set to disabled the link light will become active but no data will pass through that port.

Default: Enabled

Mode:

Is used to set the speed and duplex settings for a particular port. If Auto is displayed the port is running in auto-negotiation mode. If you are connecting to a device that is having trouble linking when running in Auto mode you made need

to manually force the speed and duplex settings of the port. The port can be forced to 10Mbps Half Duplex (10M/Half), 10Mbps Full Duplex (10M/Full), 100Mbps Half Duplex (100M/Half), 100Mbps Full Duplex (100M/Full) and 1G Full Duplex (1G/Full).

Default: Auto

Flow Control:

Shows the port's flow control status. The MS888G2 supports both Backpressure flow control for Half Duplex and Pause flow control for Full Duplex.
Select Enable to enable flow control and Disable to disable flow control.

Default: Enabled

3-2-3. Simple Counter

The Simple Counter section allows the administrator to view information regarding the amount of data that is being passed through a particular port whether the packets are good or bad.

Fig. 3-15 shows you a screen shot of the simple counter screen. As you can see from the image all ports on the switch are displayed at one time. If the amount of data being displayed on the screen is more that 12 digits long, the counter will be reset back to zero and continue on.

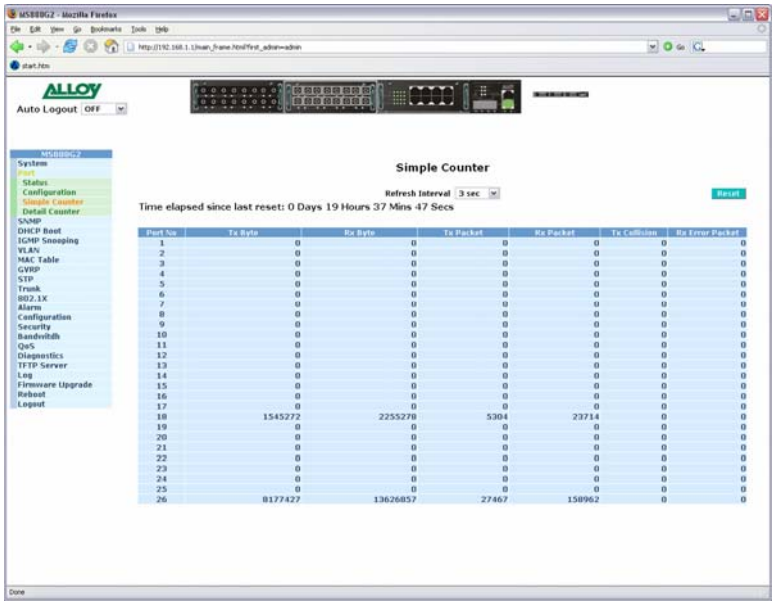

Fig. 3-15

Function Name:

Simple Counter

Function Description:

Displays the amount of data that has passed through the switch's port including, TX Byte, RX Byte, TX Packet, RX Packet, TX Collision and RX Error Packet.

Parameter Description:

TX Byte:

Displays the total transmitted bytes.

RX Byte:

Displays the total received bytes.

TX Packet:

Displays the total amount of packets transmitted.

RX Packet:

Displays the total amount of packets received.

TX Collision:

Displays the total amount of transmitted collisions that have occurred.

RX Error Packet:

Displays the total amount of bad packets received.

Refresh Interval:

The user can define the amount of time the switch will take to update the ports statistics. This is measured in seconds and ranges from 3 – 10.

Default: 3 seconds.

Reset:

The reset button is located at the top right hand side of the screen and is used to reset the counters back to zero.

3-2-3. Detail Counter

The Detail Counter section allows the administrator to view information regarding the amount of data that is being passed through a particular port whether the packets are good or bad.

Fig. 3-16 shows you a screen shot of the detail counter screen. Unlike the simple counter screen the detail counter screen will only display the statistics of one port at a time. If you wish to view a particular ports statistics select the port from the drop down box provided. If the amount of data being displayed on the screen is more that 12 digits long, the counter will be reset back to zero and continue on.

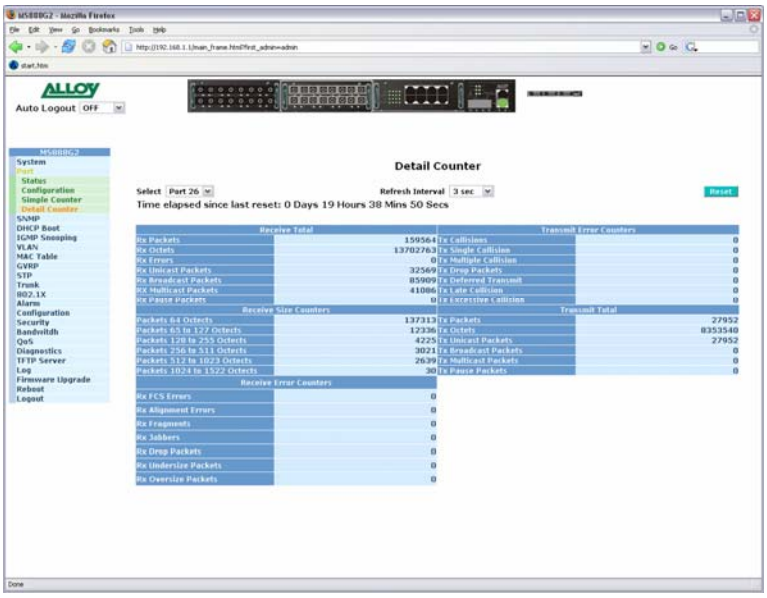

Fig. 3-16

Function Name:

Simple Counter

Function Description:

Displays in detail the amount of data that has passed through each of the ports on the switch.

Parameter Description:

RX Packets:

Displays the total number of packets received.

RX Octets:

Displays the total number of received bytes.

RX Errors:

Displays the total number of received packets with errors.

RX Unicast Packets:

Displays the total number of Unicast packets received.

RX Broadcast Packets:

Displays the total number of broadcast packets received.

RX Multicast Packets:

Displays the total number of multicast packets received.

RX Pause Packets:

Displays the total number of Pause packets received.

RX 64 Octets:

Displays the total number of 64 byte octets received.

RX 65 ~ 127 Octets:

Displays the total number of 65 ~ 127 byte octets received.

RX 128 ~ 255 Octets:

Displays the total number of 128 ~ 255 byte octets received.

RX 256 ~ 511 Octets:

Displays the total number of 256 ~ 511 byte octets received.

RX 512 ~ 1023 Octets:

Displays the total number of 512 ~ 1023 byte octets received.

RX 1024 ~ 1522 Octets:

Displays the total number of 1024 ~ 1522 byte octets received.

RX FCS Errors:

Displays the total number of FCS error packets received.

RX Alignment Errors:

Displays the total number of Alignment error packets received.

RX Fragments:

Displays the total number of short frames (<64 bytes) received with invalid CRC.

RX Jabber:

Displays the total number of long frames (>1024 bytes) received with invalid CRC.

RX Drop Packets:

Displays the total number of frames dropped due to the receive buffer being full.

RX Undersize Packets:

Displays the total number of short frames (<64 bytes) received with valid CRC.

RX Oversize Packets:

Displays the total number of long frames (>1024 bytes) received with valid CRC.

TX Collision:

Displays the total number of collisions transmitted.

TX Single Collision:

Displays the total number of single collisions transmitted.

TX Multiple Collision:

Displays the total number of multiple collisions transmitted.

TX Drop Packets:

Displays the total number of transmitted frames dropped due to excessive collisions, late collisions or frame aging.

TX Deferred Transmit:

Displays the total deferred packets transmitted.

TX Late Collision:

Displays the total Late Collision packets transmitted.

TX Excessive Collision:

Displays the total Excessive collision packets transmitted.

TX Packets:

Displays the total number of packets transmitted.

TX Octets:

Displays the total number of transmitted bytes.

TX Errors:

Displays the total number of transmitted packets with errors.

TX Unicast Packets:

Displays the total number of Unicast packets transmitted.

TX Broadcast Packets:

Displays the total number of broadcast packets transmitted.

TX Multicast Packets:

Displays the total number of multicast packets transmitted.

TX Pause Packets:

Displays the total number of Pause packets transmitted.

Select:

Used to select what ports statistics are being displayed.

Refresh Interval:

The user can define the amount of time the switch will take to update the ports statistics this is measured in seconds and ranges from 3 – 10.

Default: 3 seconds.

Reset:

The reset button is located at the top right hand side of the screen and is used to reset the counters back to zero.

3-3. SNMP Configuration

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage any Managed device equipped with an SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. SNMP is a protocol that is used to govern the transfer of information between SNMP managers and agents and traverses the Object Identity (OID) of the Management Information Base (MIB), described in the form of SMI syntax. The SNMP agent is running on the switch to respond to requests issued by an SNMP manager.

The MS888G2 allows the administrator to turn the SNMP agent on or off. If SNMP is set to “Enable”, the SNMP agent will be started. All supported MIB OIDs, including RMON MIB, can be accessed via an SNMP manager. If SNMP is set to “Disable”, the SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

Fig. 3-17

Function name:

SNMP Configuration

Function description:

This function is used to configure SNMP settings, community name, trap host and public traps as well as the throttle of SNMP. A SNMP manager must pass the authentication by identifying both community names then it can access the MIB information of the target device. Therefore, both parties must have the same community name.

Parameters description:

SNMP:

Is used to Enable or Disable the SNMP Service.

Default: Enable

Get/Set/Trap Community:

The Community name is used as a password for authentication to the Network Management software that is being used. If they both don't have the same community name, they don't belong to the same group. Hence, the requesting network management unit cannot access devices with different community names via the SNMP protocol. If they both have the same community name, they can talk to each other.

The community name is user-definable with a maximum length of 15 characters and is case sensitive. When creating the community name please ensure that no spaces are used.

The community name for each function works independently. Each function has its own community name. Therefore, the community name for GET only works for the GET command and can't be applied to other functions such as SET and Trap.

Default SNMP function: Enable

Default community name for GET: public

Default community name for SET: private

Default community name for Trap: public

Default Set function: Enable

Default trap host IP address: 0.0.0.0

Default port number: 162

Trap:

In the MS888G2, there are six trap hosts supported. Each of them has its own community name and IP address; which are user-definable. To configure a Trap host you will need a network management System to receive the Trap messages from the switch. Six Trap hosts can be configured to allow the trap messages to be received by multiple recipients.

For each public trap, the switch supports the following trap events, Cold Start, Warm Start, Link Down, Link Up and Authentication Failure. They can be enabled or disabled individually. When enabled, the corresponding trap will actively send a trap message to the trap host when a trap happens. If all public traps are disabled, no public trap messages will be sent.

Default for all public traps: Enable.

3-4. DHCP Boot

The MS888G2 supports DHCP Broadcast Suppression allowing the switch to suppress broadcast traffic. If a network loses power and then regains power and all computers on the network boot at the same time, a lot of broadcast traffic is generated especially if all nodes on your network are using DHCP.

The switch supports a random delay time for DHCP and boot delay for each device. This suppresses the broadcast storm while all devices on the network are booting at the same time. The maximum user-defined delay time is 30 seconds. If DHCP Broadcast Suppression is enabled the delay time is set randomly, ranging from 1 to 30 seconds.

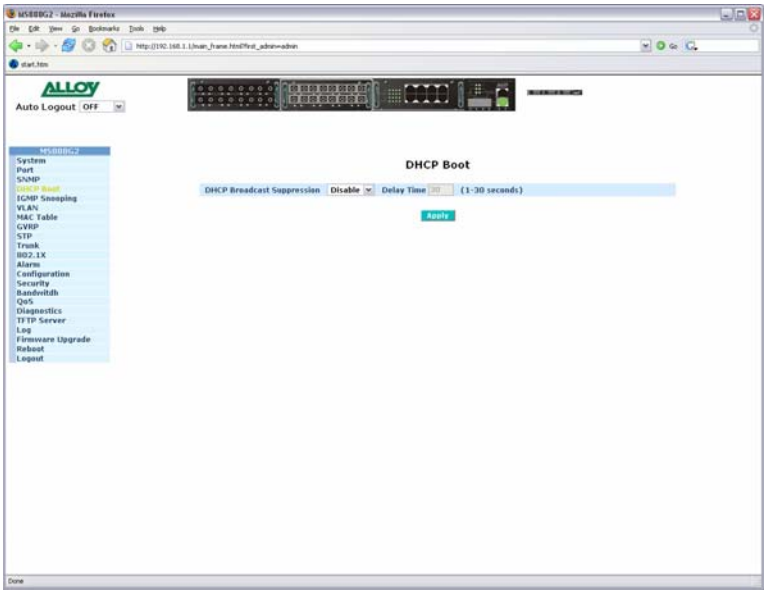

Fig. 3-18

Function name:

DHCP Boot

Function description:

The MS888G2 supports DHCP Broadcast Suppression, used to suppress the amount of broadcast traffic passing through the switch at any given time.

Parameters description:

DHCP Broadcast Suppression:

Enable or Disable DHCP Broadcast Suppression.

Default: Disable

Delay Time:

Select the Delay Time used for the broadcast suppression ranging from 1 to 30 seconds.

3-5. IGMP Snooping

IGMP Snooping is used to establish multicast groups to forward multicast packets to each of the multicast member ports, and, in nature, avoids wasting bandwidth with IP multicast packets. If a switch does not support IGMP or IGMP Snooping it can not tell a multicast packet from a broadcast packet, so it will treat them all as broadcast packets. Without IGMP Snooping, multicast packets are treated as broadcast packets, therefore increasing the overall traffic on your network.

The MS888G2 supports all functions of IGMP Snooping including query, report and leave. IGMP Snooping is used by the switch to learn who belongs to a multicast group and also update the multicast table within the switch with new multicast members. Once the switch has learned who belongs to the multicast group all packets forwarded to a multicast address will be forwarded to all members belonging to the multicast group.

3-5-1. Status

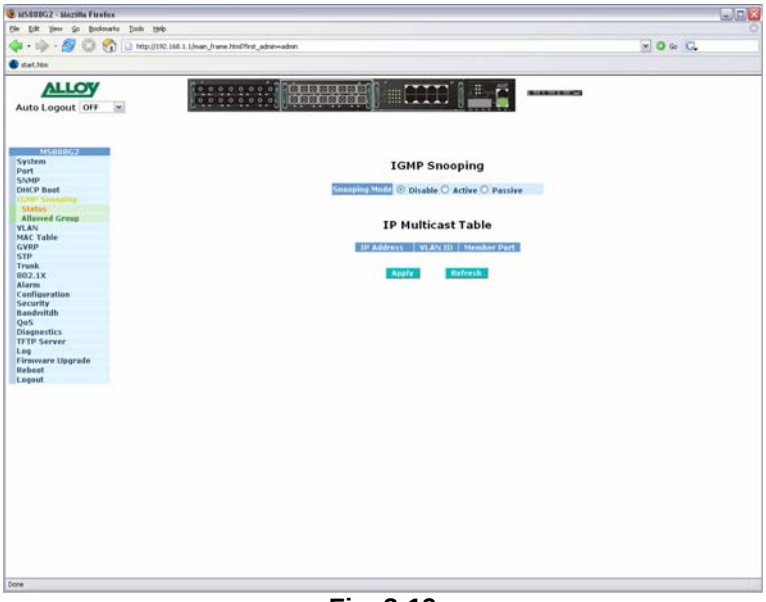

Fig. 3-19

Function name:

IGMP Snooping

Function description:

IGMP is used to snoop the status of IP multicast groups and display its associated information in both tagged VLAN and non-tagged VLAN networks. By enabling IGMP with either passive or active mode, you can monitor the IGMP snooping information, which contains information about the multicast member list including the multicast groups, VID and member ports.

Parameters description:

Snooping Mode:

The MS888G2 supports both Active and Passive modes, IGMP can also be disabled.

Default: Disable

Disable:

To disable IGMP select the disable radio button and click Apply.

Active:

When using Active mode the switch will periodically issue the membership query message to all hosts attached to the switch and update the multicast table respectively. By using Active mode you will reduce multicast traffic on your network.

Passive:

When using Passive mode, IGMP Snooping will not periodically poll the hosts in all multicast groups, it will only send a membership query message to all hosts once it has received a membership query message from a router.

IP Multicast Table:

Is used to display the members of each multicast group.

IP Address:

Shows the IP addresses of all multicast groups that have been registered on the switch.

VLAN ID:

Shows the VLAN ID for each multicast group.

Member Port:

Shows the member ports of each multicast group, a group may contain a single host or multiple hosts.

3-5-2. Allowed Group

The MS888G2 allow the administrator to lock down multicast members by IP Range, VLAN ID, and port number. If the administrator only wants to enable IGMP Snooping on ports 1, 2, 3 and 4 then this can be done in this section.

Fig. 3-20

Function name:

Allowed Group

Function description:

Is used to configure rules based on how Multicast traffic is learned and utilised.

Parameters description:

IP Range:

Select Any to allow any IP range to be queried as multicast members or select custom to specify an IP range.

VID:

Select Any to allow any VID number to be queried as multicast members or select custom to specify a particular VID number.

Port:

Select Any to allow any port number to be queried as multicast members or select custom to specify a particular port number.

The table below the control buttons displays the rules that have been created. Once you have configured a particular rule click on the Add button to add the rule to the list. If you wish to edit an existing rule highlight the required rule and click the Edit button. If you wish to delete an existing rule highlight the required rule and click the Delete button.

3-6. VLAN (Virtual Local Area Network)

The MS888G2 supports both 802.1q Tagged based VLAN's and Port-based VLAN's. VLAN's are used to logically separate your network into smaller more defined networks. VLAN's help to reduce broadcast traffic across your network as all broadcast traffic will be limited to the VLAN group in which it belongs. A typical example of where a VLAN could be used is in a school environment where the teacher and student networks must be kept separate. The switch supports up to 256 active VLAN entries and a VLAN ID ranging from 1 – 4096.

3-6-1. VLAN Mode

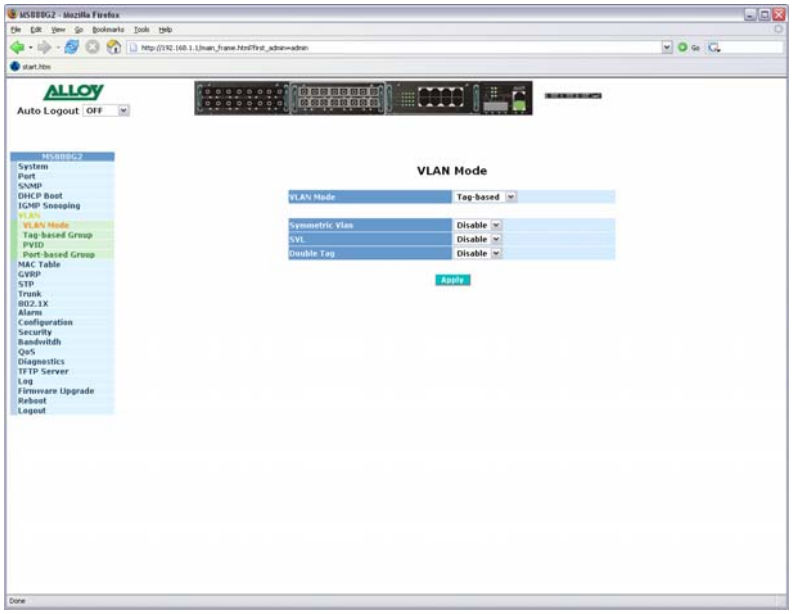

Fig. 3-21

Function name:

VLAN Mode

Function description:

The MS888G2 supports 2 different VLAN modes including, Port-Based and Tag-based. Select the desired VLAN mode from the drop down box and click the Apply button. Changes will take effect immediately.

Default: Tag-based

Parameters description:

Tag-based:

Tag-based VLAN's identify members by its VID. A VID can be applied to a packet from a host machine that supports 802.1q or from the switch itself when a packet is sent from the switch. Ingress and Egress rules can also be applied to each port to identify how a packet is handled. The switch will accept both tagged and un-tagged packets depending on the ingress rules that have been defined. Rules can be created to allow only incoming packets to be tagged; however when this Rule is applied any untagged packets will be dropped.

Each tag-based VLAN you build must have a VLAN name and VLAN ID. Valid VLAN ID's range from 1 – 4096. The maximum number of tag-based VLAN groups that can be created is 256.

Port-based:

Port-based VLAN's are as it states defined by each port. Ports are configured into logical groups allowing data to be sent to and from any port that belongs to a particular group. If a port belongs to VLAN group 1 and another port belongs to VLAN group 2 these ports will not be able to communicate with each other. Ports that belong to the same group can communicate. Ports can also belong to multiple groups for example, allowing an internet connection to be shared among two VLAN groups. The switch has support for up to 26 port-based VLAN groups.

Symmetric VLAN:

This is an Ingress Rule (Rule 1, The Ingress Filtering Rule 1 is "forward only packets with VID matching this port's configured VID".). For example, if port 1 receives a tagged packet with VID=100 (VLAN name=VLAN100), and if Symmetric-Vlan function is enabled, the switch will check if port 1 is a member of VLAN100. If yes, the received packet is forwarded; otherwise, the received packet is dropped.

Note: If Symmetric is enabled and port 1, for example, receives an untagged packet, the switch will apply the PVID of port 1 to tag this packet, the packet then will be forwarded. But if the PVID of port 1 is not 100, the packet will be dropped.
Default: Disabled

SVL:

When SVL is enabled, all VLAN's will use the same filtering database storing the membership information of the VLAN to learn or look up the membership information of the VLAN. If SVL is disabled different VLAN groups will use different filtering databases to store the membership information of the VLAN.
Default: Disabled

Double-tag:

Double-tag mode belongs to tag-based VLAN's; however it treats all packets as untagged packets. This means that a tag with a pre-defined PVID will be added to all packets. Therefore all packets that leave the switch will be tagged, if a tagged packet is received by the switch an additional tag will be added thus becoming a double-tag packet.

Double tag (Q in Q) provides additional flexibility for managing traffic flows, using this method, service providers could use, for example, sending one flow of data to a building and then separate and forward traffic based on supplemental IDs used to identify specific tenants in a site. This can be useful for situations in which traffic must be separated for management, tracking and billing purposes. In addition this method enables customers to maintain their desired tag, without concern that other organisations will share the same ID. Service providers avoid potential problems by simply adding a second ID per customer in addition to the shared tag.

Default: Disabled

3-6-2. Tag-based Group

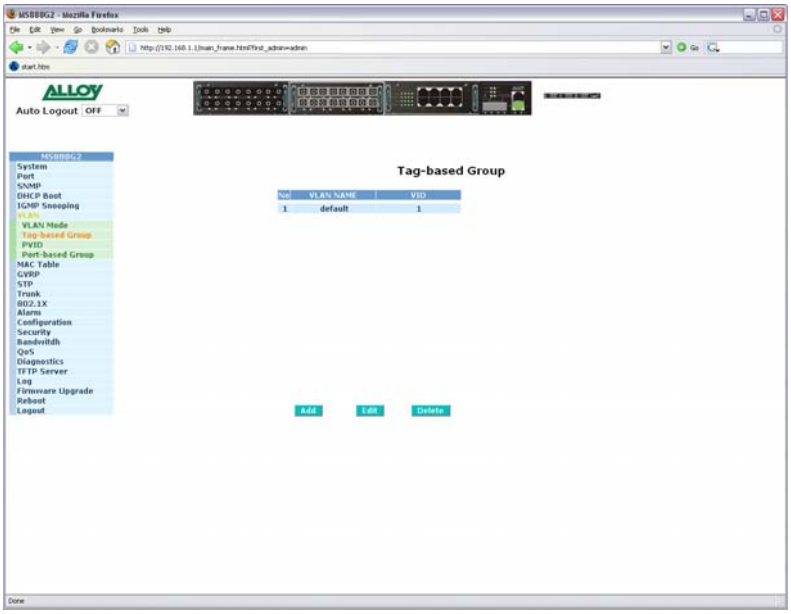

Fig. 3-22

Function name:

Tag-based Group Configuration

Function description:

Shows information of the existing tag-based VLAN groups, the administrator can also Add, Delete and Edit VLAN's using the function buttons provided.

Parameters description:

VLAN Name:

Is the name of the VLAN group defined by the administrator. Valid characters that can be used are A – Z, a – z and 0 – 9. Special characters are not allowed and a total of 15 characters are supported.

VID:

VID is the VLAN Identifier. Each tag-based VLAN group must have a unique VID.

Member:

This is used to add or remove a particular port from the VLAN group, tick the check box next to the port number you would like to be a member of the group.

Untag:

Select whether the port belonging to the VLAN group will be a tagged or untagged port.

Add:

Used to create a new tag-based VLAN group, enter the name and the VID. You will now have to select what ports you would like to belong to this group. Click the Apply button for the settings to take effect.

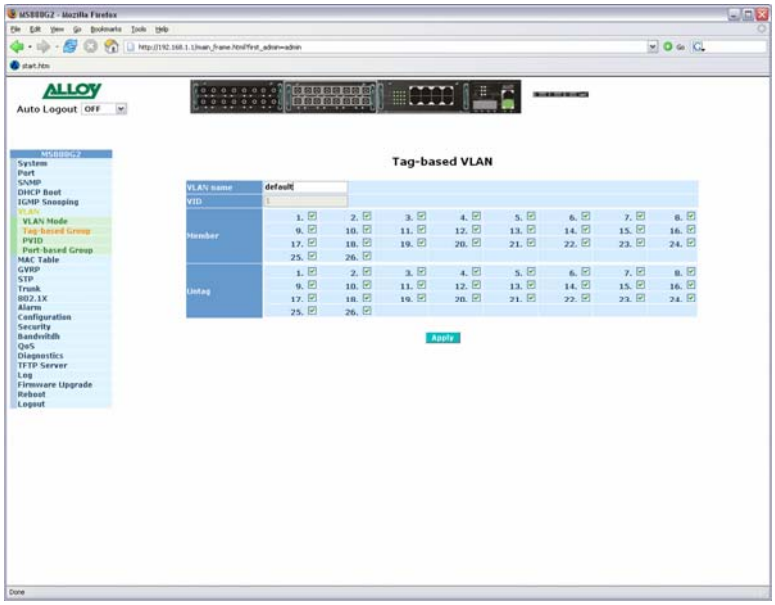

Fig. 3-23

Delete:

Highlight the VLAN group you wish to delete and click the Delete button to remove the VLAN group from the table.

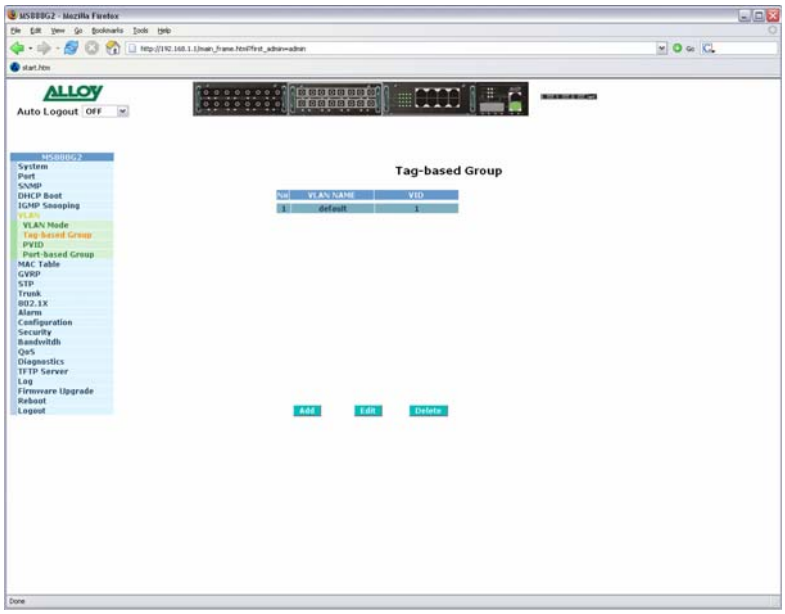

Fig. 3-24

Edit:

Highlight the VLAN group you wish to edit and click the Edit button to modify the selected VLAN group.

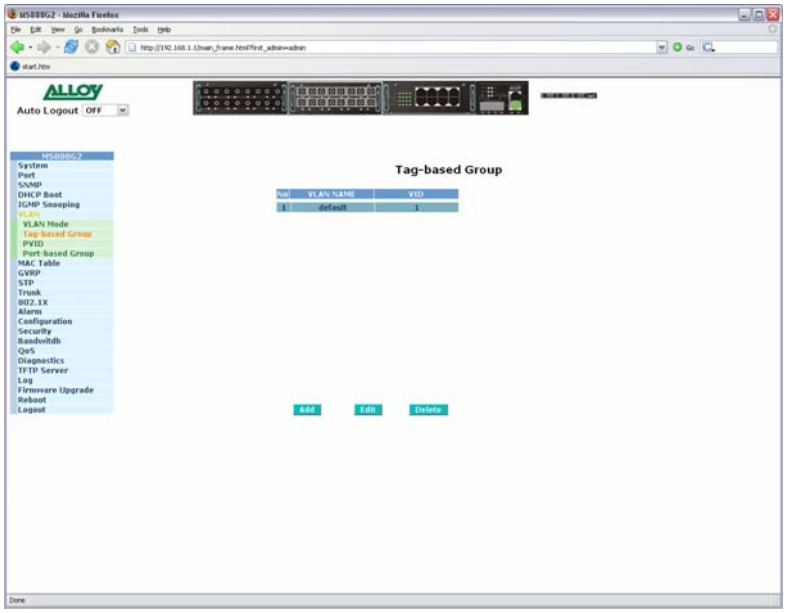

Fig. 3-25

3-6-3. PVID

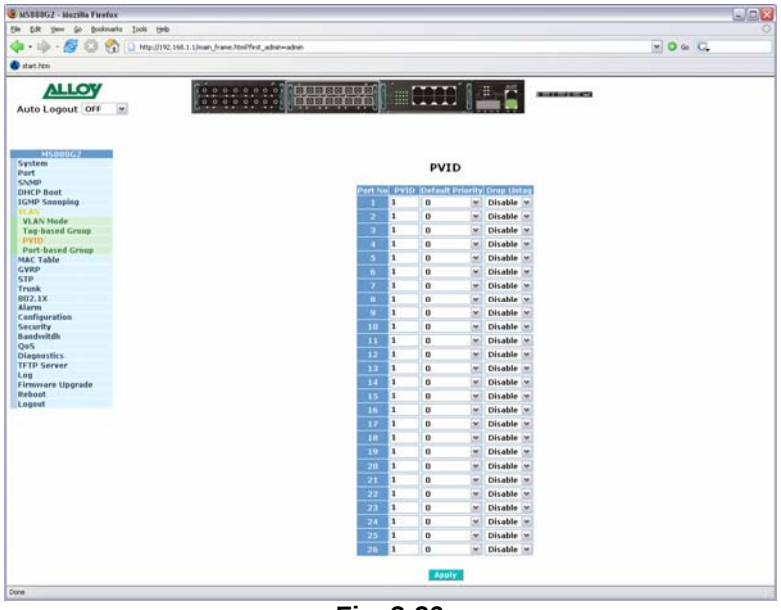

Fig. 3-26

Function name:

PVID

Function description:

The administrator can apply a VID to each port of the switch; the valid range of the VID is from 1 to 4094. A Priority level from 0 through to 7 can also be applied to each port, as

well as an ingress filtering rule called “Drop Untag”. This rule will determine how packets are treated when received by the switch.

Parameters description:

Port No:

Select the port you wish to apply a VLAN Tag Rule.

PVID:

PVID range is 1 – 4094. Before you configure a PVID you must create a Tag-based VLAN with the VID matching the PVID you are about to create. For example, if port x receives an untagged packet, the switch will apply the PVID of port x to this packet, the packet will then be forwarded as a tagged packet with the VID you have created.

Default Priority:

If a packet is received with no tag the port will apply the appropriate PVID and priority level.

Drop Untag:

Each port can be configured to accept both tagged and untagged packets or, just tagged packets. If set to Enabled only tagged packets will be accepted, if Disabled the port will accept both tagged and untagged packets.

3-6-4. Port-based Group

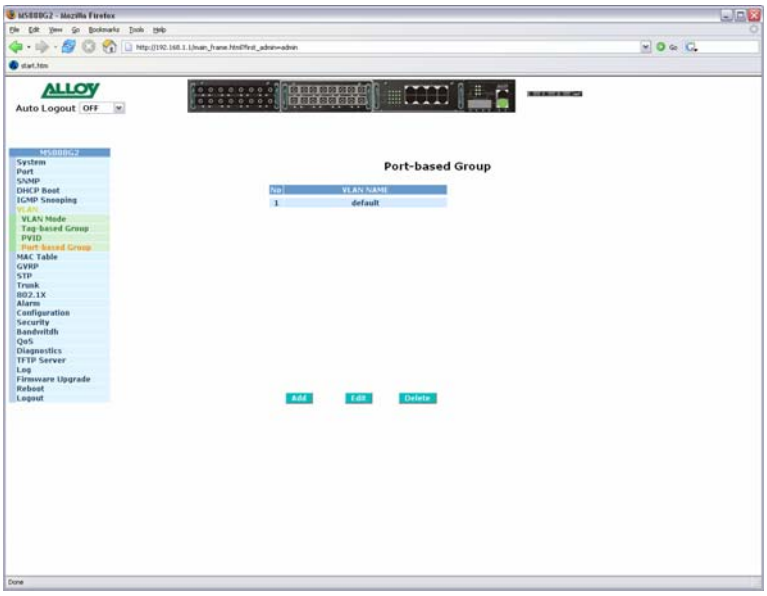

Fig. 3-27

Function name:

Port-based Group Configuration

Function description:

Shows information of the existing port-based VLAN groups, the administrator can also Add, Delete and Edit VLAN’s using the function buttons provided.

Parameters description:

VLAN Name:

Is the name of the VLAN group defined by the Administrator. Valid characters that can be used are A – Z, a – z and 0 – 9. Special characters are not allowed and a total of 15 characters are supported.

Member:

This is used to add or remove a particular port from the VLAN group, tick the check box next to the port number you would like to be a member of the group.

Add:

Used to create a new port-based VLAN group, enter the name and select what ports you would like to belong to this group. Click the Apply button for the settings to take effect.

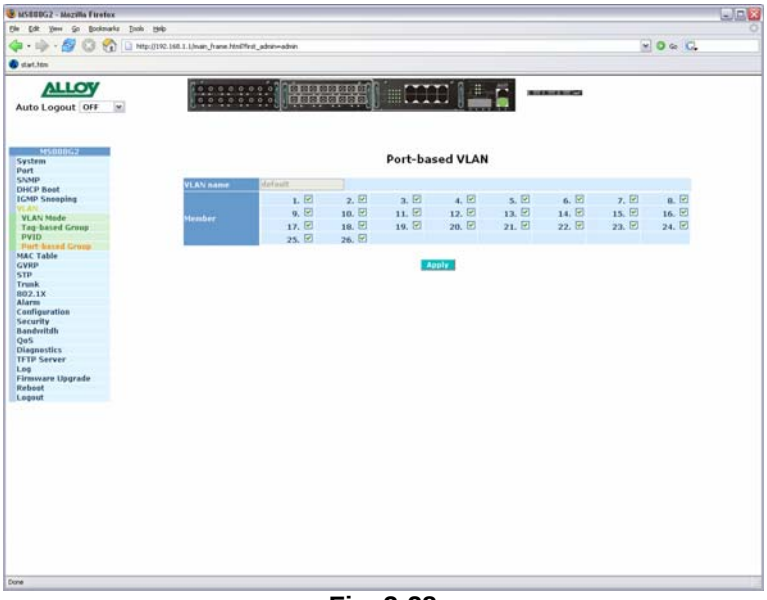

Fig. 3-28

Delete:

Highlight the VLAN group you wish to delete and click the Delete button to remove the VLAN group from the table.

Fig. 3-29

Edit:

Highlight the VLAN group you wish to edit and click the Edit button to modify the selected VLAN group.

Fig. 3-30

3-7. MAC Table

The MAC Table configuration can be used by the administrator to statically add MAC entries to the switches MAC table, display MAC address information from connecting devices, allow you to flush the switches MAC table and also allow you to configure the MAC age out time of the switch.

3-7-1. MAC Table Information

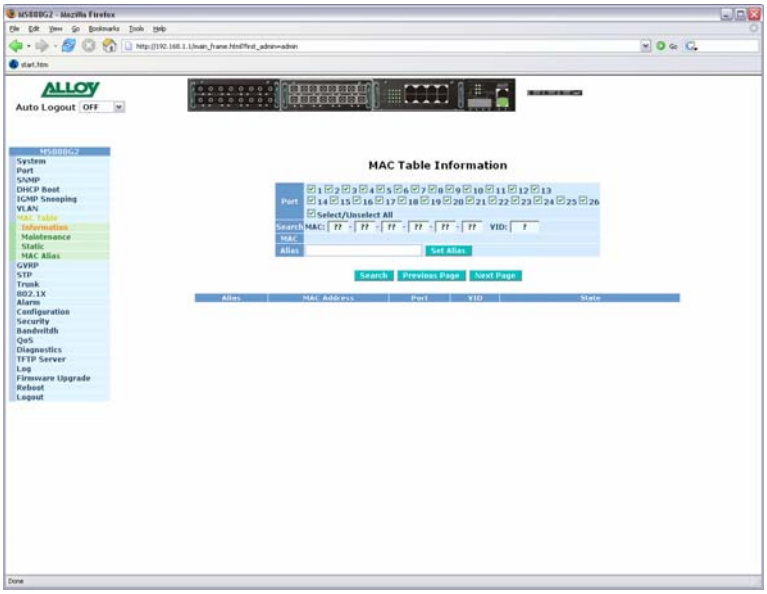

Fig. 3-31

Function name:

MAC Table Information

Function description:

Displays both static and dynamic MAC entries that the switch has learnt.

Parameters description:

Port:

Select the port you would like to query.

Search:

Enter the MAC address that you would like to query.

Default: ??-??-??-??-??-??

MAC:

Select an entry from the MAC table; the MAC address from that entry will be displayed.

Alias:

Set up an Alias for the selected MAC address.

Set Alias:

Saves the Alias to the MAC address selected.

Search:

Is used to search for MAC addresses that are connected to the switch. The search will depend on the criteria entered in the above section. For example if you have all ports selected the switch will display all MAC address connected to all ports of the switch. If you wish to search for a particular MAC address, enter the MAC address in the Search section and click Search.

Previous Page:

If the MAC table can not be displayed on one page, it will be displayed across multiple, click on previous page to move between pages.

Next Page:

If the MAC table can not be displayed on one page, it will be displayed across multiple, click on next page to move between pages.

The MAC table will be displayed after a search has been performed. The MAC table consists of the following information:

Alias:

The Alias of the searched MAC entries.

MAC Address:

The MAC Address of the searched MAC entries.

Port:

The port in which the MAC addresses were found.

VID:

VLAN group in which the searched MAC address exists.

State:

Displays the method used to discover the MAC address, this can either be Static or Dynamic.

3-7-2. MAC Table Maintenance

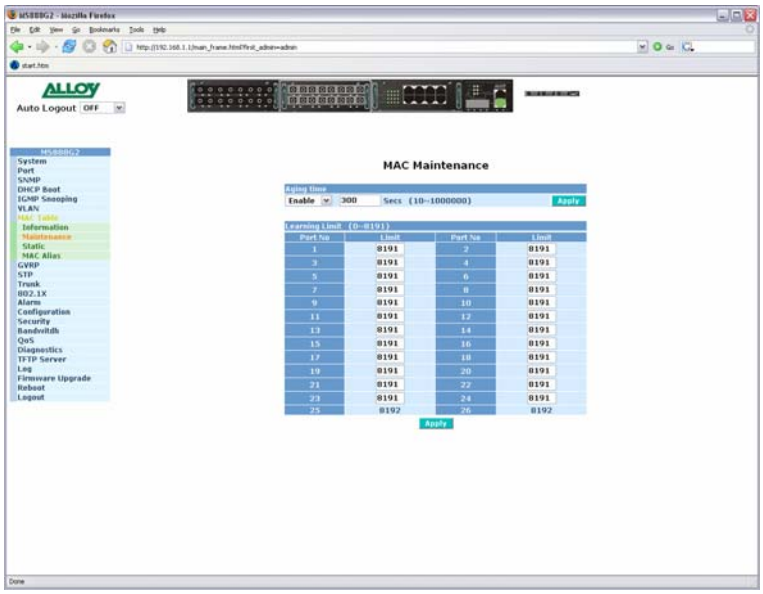

Fig. 3-32

Function name:

MAC Table Maintenance

Function description:

Allows the administrator to set the MAC age time out value and allows you to adjust the MAC learning limit of each port.

Parameters description:

Aging Time:

After a MAC address has been learned by the switch the MAC address is stored in the MAC table of the switch. If the MAC address is no longer used the switch will drop the MAC address from the table after a certain period of time. This time can be defined by the administrator. The MAC Age-out Time can be set from 10 – 65535 seconds. This time-out value does not apply to Static MAC entries.

Default: 300 seconds

Learning Limit:

Each port can be configured to allow only a certain number of MAC addresses to be learnt. The valid range is 0 through to 8191.

Default: 8191

3-7-3. Static

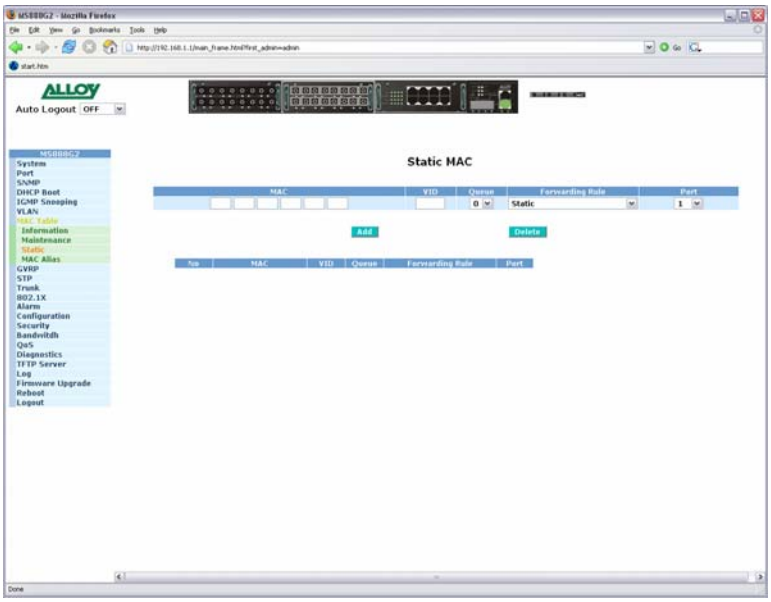

Fig. 3-33

Function name:

Static Mac

Function description:

The Static Forward function is used to associate a MAC address to a particular port of the switch. When a MAC address is assigned to a specific port all of the switches traffic sent to that MAC address will be forwarded to this port.

To add a Static Forward entry to the table enter the MAC address, port number, VID and Alias. If you wish to delete an existing entry highlight the required MAC address and click the delete button.

Parameters description:

MAC:

Enter the MAC address of the static forward entry you wish to create.

Port No:

Port number that the MAC address will be associated with.

VID:

VLAN Identifier, this will only be used if tagged VLAN's are applied. Valid range is 1 – 4094.

Alias:

Alias name of the MAC address that has been assigned.

3-7-4. MAC Alias

Fig. 3-34

Function name:

MAC Alias

Function description:

The MAC Alias function is used to assign a user friendly name to a MAC Address.

Enter the MAC address and its assigned Alias name and click the Create/Edit button to add this entry. If you wish to modify an existing entry highlight the MAC address and click the Create/Edit button. If you wish to Delete an entry, highlight the MAC address and click the Delete button.

Parameters description:

MAC:

Enter the MAC address you wish to assign a user friendly name to.

Alias:

Enter a user friendly name for the MAC address.

3-8. GVRP

The GARP (Generic Attribute Registration Protocol) VLAN Registration Protocol (GVRP) defines a GARP application that provides the 802.1Q-compliant VLAN pruning and dynamic VLAN creation on 802.1Q trunk ports.

With GVRP, the switch can exchange VLAN configuration information with other GVRP switches, prune unnecessary broadcast and unknown unicast traffic, and dynamically create and manage VLAN's on switches connected through 802.1Q trunk ports.

GVRP makes use of GID and GIP, which provide the common state machine descriptions and the common information propagation mechanisms defined for use in GARP-based applications. GVRP runs only on 802.1Q trunk links. GVRP prunes trunk links so that only active VLAN's will be sent across trunk connections. GVRP expects to hear join messages from the switches before it will add a VLAN to the trunk. GVRP ports run in various modes to control how they will prune VLAN's. GVRP can be configured to dynamically add and manage VLANS to the VLAN database for trunking purposes.

3-8-1. GVRP Configuration

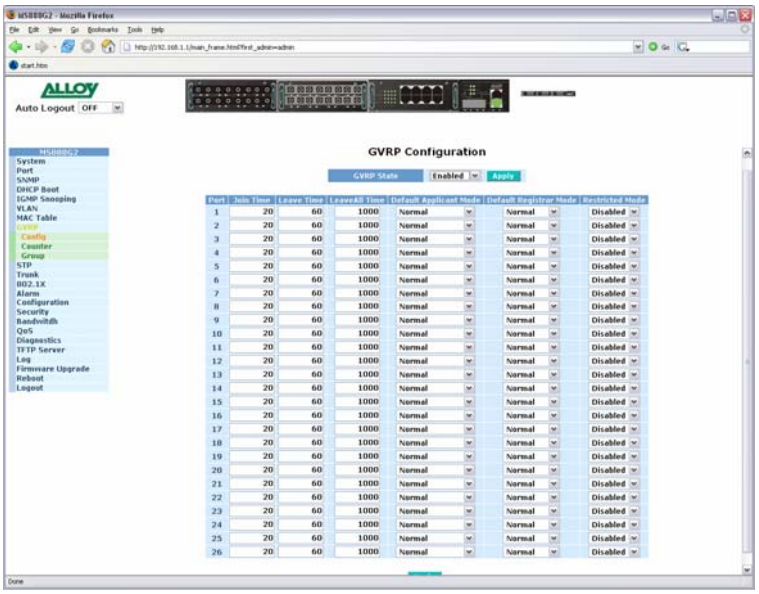

Fig. 3-35

Function name:

GVRP Config

Function description:

Is used to configure each ports GVRP operation mode, in which seven parameters can be configured.

Parameters description:

GVRP State Setting:

Used to enable or disable the GVRP function. Select your option from the drop down box and click the Apply button.

Default: Disable

Join Time:

Used to specify the Join Time in units of 100th of a Second, Valid time range is 20 – 100.

Default: 20

Leave Time:

Used to specify the Leave Time in units of 100th of a Second, Valid time range is 60 – 300.

Default: 60

Leave All Time:

A time period for the announcement that all registered devices are going to be de-registered. If a device issues a new join command, then a registration will be kept in the switch. Valid range is 1000 – 5000 unit time.

Default: 1000 unit time

Default Applicant Mode:

There are two types of participant modes that are supported, normal participant and non-participant.

Normal:

The switch participates normally in the GARP protocol exchanges. This is the default setting.

Non-Participant:

In this mode the switch does not send or reply to any GARP messages, it just listens to messages and reacts to any received GVRP BPDU.

Default Registrar Mode:

There are three types of administrative control values that can be set, they are normal registrar, fixed registrar and forbidden registrar.

Normal:

The Registrar responds normally to incoming GARP messages. This is the default setting.

Fixed:

The Registrar ignores all GARP messages and all members remain in the registered (IN) state.

Forbidden:

The Registrar ignores all GARP messages and all members remain in the unregistered (EMPTY) state.

Restricted Mode:

This function is used to restrict the creation of a dynamic VLAN when this port receives GVRP BDU. There are two modes Enabled and Disabled.

Disabled:

The dynamic VLAN will be created when this port receives a GVRP BDU. This is the default setting.

Enabled:

The switch will not create dynamic VLAN's when this port receives GVRP BDU, except if it receives a dynamic VLAN message and the GVRP PDU is an existing static VLAN entry.

3-8-2. GVRP Counter

Fig. 3-36

Function name:

GVRP Counter

Function description:

All GVRP counters are divided into Received and Transmitted sections to allow you to monitor all GVRP actions.

Parameters description:

Received:

Total GVRP Packets:

The total GVRP BPDU received by the GVRP application.

Invalid GVRP Packets:

The total number of invalid GARP BPDU received by the GARP application.

Leave All Message Packets:

The total number of GARP BPDU with Leave All Messages received by the GARP application.

Join Empty Message Packets:

The total number of GARP BPDU with Join Empty Messages received by the GARP application.

Join In Message Packets:

The total number of GARP BPDU with Join In Messages received by the GARP application.

Leave Empty Message Packets:

The total number of GARP BPDU with Leave Empty Messages received by the GARP application.

Empty Message Packets:

The total number of GARP BPDU with Empty Messages received by the GARP application.

Transmitted:

Total GVRP Packets:

The total GVRP BPDU transmitted by the GVRP application.

Invalid GVRP Packets:

The total number of invalid GARP BPDU transmitted by the GARP application.

Leave All Message Packets:

The total number of GARP BPDU with Leave All Messages transmitted by the GARP application.

Join Empty Message Packets:

The total number of GARP BPDU with Join Empty Messages transmitted by the GARP application.

Join In Message Packets:

The total number of GARP BPDU with Join In Messages transmitted by the GARP application.

Leave Empty Message Packets:

The total number of GARP BPDU with Leave Empty Messages transmitted by the GARP application.

Empty Message Packets:

The total number of GARP BPDU with Empty Messages transmitted by the GARP application.

3-8-3. GVRP Group Information

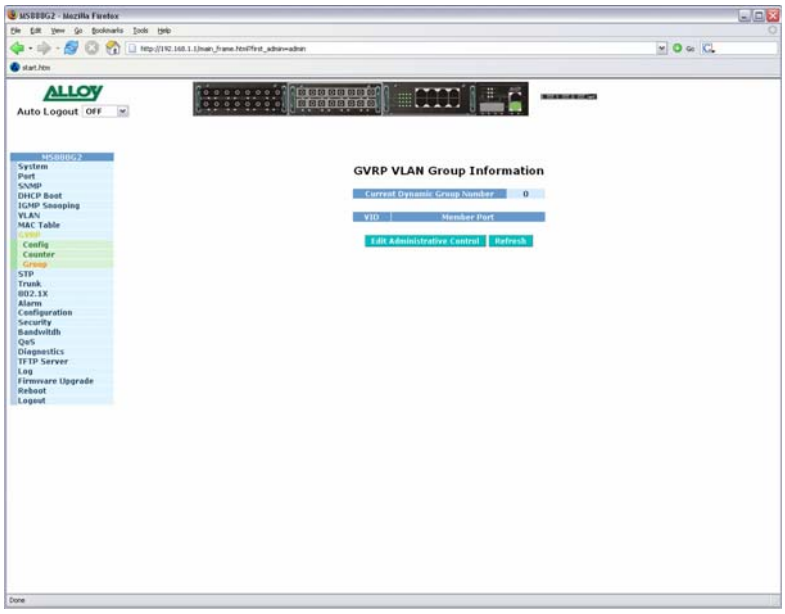

Fig. 3-37

Function name:

GVRP Group

Function description:

Displays the dynamic group members and their relevant information.

Parameters description:

VID:

VLAN Identifier. When a GVRP group has been created it will have its own VID. Valid range is 1 – 4094

Member Port:

Members that belong to the same dynamic VLAN group.

Edit Administrative Control:

When you have created a GVRP group, you can use the Administrative control function to change the Applicant and Registrar modes of the GVRP group.

Refresh:

Click the refresh button to get current GVRP group status.

3-9. STP

The Spanning Tree Protocol (STP) is a standardised method (IEEE 802.1D) for avoiding loops in switched networks. When STP is enabled, the switch will ensure that only one path is active between any two nodes on the network at a time. The administrator can enable Spanning Tree Protocol via the switch's web management and then set up other advanced items. We recommend that you enable STP on all switches to ensure a single active path on the network.

3-9-1. STP Status

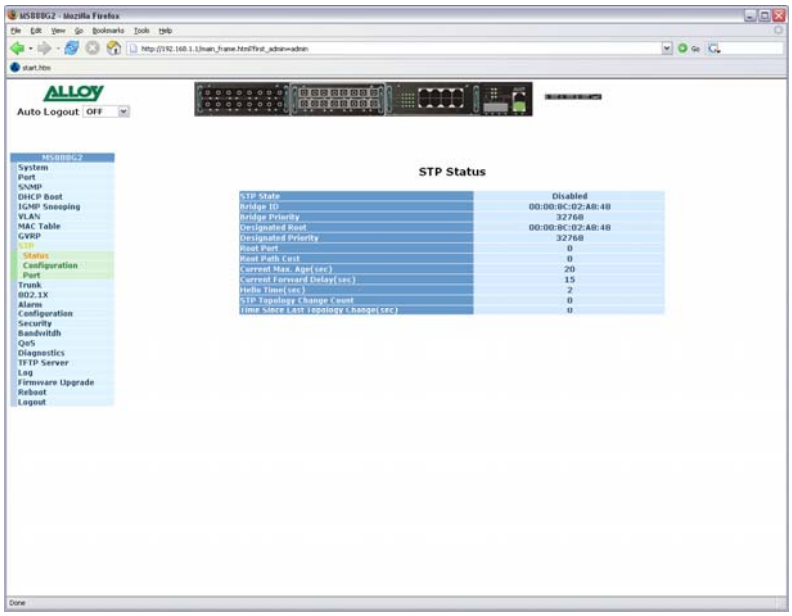

Fig. 3-38

Function name:

STP Status

Function description:

Shows the current status of the STP parameters.

Parameters description:

STP State:

Shows the current status of STP, Enabled or Disabled.

Default: Disabled

Bridge ID:

Shows the switches bridge ID, which is usually the MAC address of the switch.

Bridge Priority:

Shows the switches current bridge priority.

Default: 32768

Designated Root:

Shows the root bridge ID for this network segment. If this switch is the root

bridge, the “Designated Root” will be this switches bridge ID.

Designated Priority:

Shows the current root bridge priority.

Root Port:

Shows the port number connected to the root bridge with the lowest path cost.

Root Path Cost:

Shows the path cost between the root port and the designated port of the root bridge.

Current Max. Age:

Shows the current root bridge maximum age time. Maximum age time is used to monitor if the STP topology needs to change. When a bridge does not receive a hello message from a root bridge until the maximum age time is counted down to 0, the bridge will treat the root bridge as malfunctioned and issue a Topology Change Notification (TCN) BPDU to all other bridges.

All bridges in the LAN will re-learn and determine who the root bridge is. Maximum Age time is assigned by the root bridge in units of seconds.

Default: 20 seconds.

Current Forward Delay:

Shows the current root bridge forward delay time. The value of the Forward Delay time is set by the root. The Forward Delay time is defined as the time spent changing from the Listening state to the Learning state or from the Learning state to the Forwarding state of a port in the bridge.

Hello Time:

Shows the current hello time of the root bridge. The Hello time is a time interval specified by the root bridge, used to request all other bridges to periodically send hello messages every “hello time” in seconds to the bridge attached to its designated port.

STP Topology Change Count:

Shows the time spent in units of seconds since the beginning of the Spanning Tree Topology Change to the end of the STP convergence. Once the STP change is converged, the Topology Change count will be reset to 0.

Time Since Last Topology Change:

Shows the accumulated time in units of seconds since the last STP Topology Change was made. When a Topology Change is initiated again, this counter will be reset to 0.

3-9-2. STP Configuration

Fig. 3-39

Function name:

STP Configuration

Function description:

Used to configure the spanning tree parameters including, enabling and disabling, selecting to use STP or RSTP and you can also change the Bridge Priority, Hello Time, Max. Age and Forward Delay parameters.

Parameters description:

Spanning Tree protocol:

Used to Enable or Disable the Spanning Tree Protocol.

Bridge Priority:

The lower the bridge priority value is, the higher the priority it has. Usually, the switch with the highest bridge priority is the root. If you wish the MS888G2 to be the root bridge you will need to ensure that other bridges on your network have a higher bridge priority than that of this switch. The valid value is 0 – 61440.

Default: 32768

Hello Time:

The Hello Time is used to determine the periodic time to send normal BPDU messages from the designated ports among all bridges on your network. It determines how long a bridge should send this message to other bridges to tell them I am alive. When the MS888G2 is the root bridge of the network, for example all other bridges will use the hello time assigned by this switch to communicate with each other. The valid value is 1 – 10 seconds.

Default: 2 seconds

Max. Age:

If the MS888G2 is the root bridge, the whole network will apply this figure as their maximum age time. When a switch receives a BPDU message originating from the root bridge and if the message age exceeds the maximum age of the bridge, the bridge will treat the root bridge as malfunctioned and issue a Topology Change Notification (TCN) BPDU to all other bridges. All bridges on the network will re-calculate and determine who the root bridge is. The valid value is 6 – 40 seconds.

Default: 20 seconds

Forward delay:

You can set the root bridge forward delay time. This figure is set by the root bridge only. The forward delay time is defined as the time spent changing from the Listening state to the Learning state and also from the Learning state to the Forwarding state of a port in a bridge. The forward delay time contains two states, Listening state to Learning state and Learning state to Forwarding state. It assumes that the forward delay time is 15 seconds, then the total forward delay time will be 30 seconds. This has much to do with the STP convergence time which will be more than 30 seconds because of some other factors. The valid value is 4 ~ 30 seconds

Default: 15 seconds.

Force Version:

The switch supports both STP (802.1d) and RSTP (802.1w). This option can be selected here.

3-9-3. STP Port Configuration

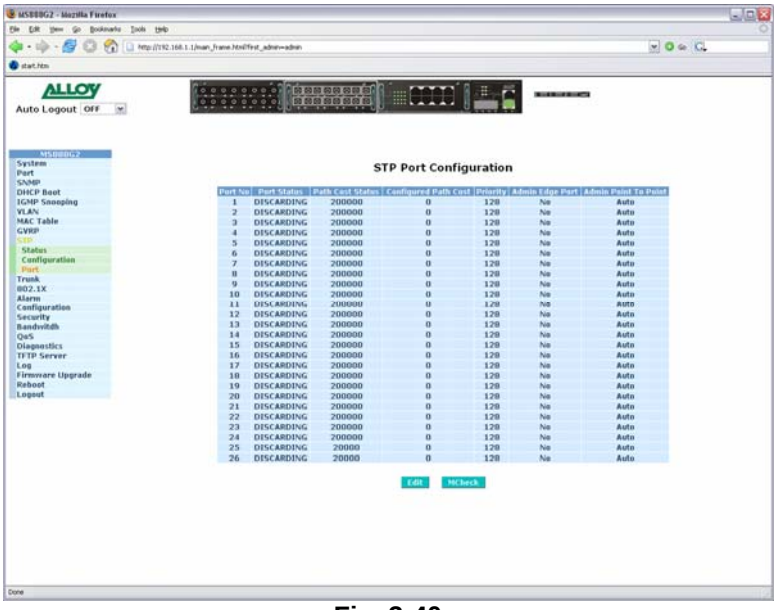

Fig. 3-40

Function name:

STP Port Configuration

Function description:

The STP Port setting is used to configure the “path cost”, “priority”, “admin edge port” and the “admin point to point” settings. Each port can be configured individually by highlighting the port and clicking in the Edit button.

Parameters description:

Port Status:

Displays the current state of the port, there are three possible states according to the 802.1w standard.

Discarding: Indicates that this port can neither forward packets nor contribute in learning.

Note: Three other states Disable, Blocking and Listening defined in the 802.1d standard are now all represented as the Discarding state.

Learning: Indicates that this port can now contribute its learning knowledge but can not forward packets.

Forwarding: Indicates this port can both contribute its learning knowledge as well as forward packets normally.

Path Cost Status:

Determines the shortest path to the root bridge, the smaller the path cost value the more possible the port will become the root port.

Configured Path Cost:

If the path cost is equal to zero, the path cost will be auto-negotiated and displayed in the path cost status field. Otherwise the value that the administrator has set manually will be displayed. Valid range is 0 – 200,000,000

802.1w RSTP recommended values:

10Mbps: 2,000,000

100Mbps: 200,000

1Gbps: 20,000

Default: 0

Priority:

Indicates the port priority, the port priority and port number are mixed to form the port ID. Port ID's are often compared in order to determine which port of a bridge would become the root port. Valid range is 0 – 240

Default: 128

Admin Edge Port:

If Enabled, this port will be an edge port. An Edge Port is a port connected to a device that knows nothing about STP or RSTP. Usually, the connected device is an end station. Edge Ports will immediately transit to forwarding state and skip the listening and learning state because edge ports cannot create bridging loops in the network. When the link on the edge port toggles, the STP topology stays unchanged. Unlike the designated port or root port, an edge port will transit to a normal spanning-tree port immediately if it receives a BPDU.

Default: No

Admin Point to Point:

We say a port is a point-to-point link, if it is in full-duplex mode but is a shared link if it is in half-duplex mode. RSTP's fast convergence can only occur on point-to-point links and on edge ports.

There are three parameters, Auto, True and False, used to configure the type of point-to-point link. If this parameter is configured as Auto, it means that RSTP will use the duplex mode resulting from the auto-negotiation. In today's switched networks, most links are running in full-duplex mode. If the result is half-duplex, then the port will not fast transit to Forwarding state. If it is set as True, the port is treated as a point-to-point link by RSTP and will be unconditionally transited to Forwarding state. If it is set as False, fast transition to Forwarding state will not occur on this port.

Default: Auto

M Check:

Migration Check, forces the port to send out an RSTP BPDU instead of a legacy STP BPDU at the next transmission. The only benefit of this operation is to make the port quickly act as an RSTP port. Click the **<M Check>** button to send a RSTP BPDU from the port you specified.

3-10. Trunking Configuration

Port Trunking is used to Aggregate Ports into a logical trunk usually called Link Aggregation. Link Aggregation can bundle more than one port with the same speed, full duplex and the same MAC address to be a single logical port, thus the logical port aggregates the bandwidth of these ports. This allows the switch to aggregate multiple ports together to form a high bandwidth backbone link.

The MS888G2 supports two kinds of trunking methods:

LACP:

Ports that are using Link Aggregation Control Protocol (according to the IEEE 802.3ad standard) as their trunking method can choose their unique LACP Group ID (1-3) to form a logical “Trunked Port”. The benefit of using LACP is that a port makes an agreement with its peer port before it becomes a ready member of a “Trunk Group” (also called Aggregator).

The MS888G2 LACP function does not support the following:

- Link Aggregation across switches
- Aggregation with non IEEE 802.3 MAC links
- If the ports are operating in Half Duplex mode
- Aggregate the ports with different data rates

Static Trunk:

Ports that are using Static trunk as their Trunk method can choose their unique Static Group ID (also 1 – 3, this static group ID can be the same as a LACP group ID) to form a logical “Trunked Port”. A benefit of using Static Trunking is that a port can become a member of a trunk group without any handshaking with its peer port. This can also be a disadvantage because the peer ports of the Trunk group may not know that the ports should be aggregated together to form a trunk group. Using Static trunking at both ends of the link is highly recommended.

The MS888G2 allows up to 3 LACP trunk groups and another additional 3 trunk groups for static trunking. Only 3 groups can be used at one time. Each trunk group can contain a maximum of 4 member ports.

3-10-1. Trunk Port Settings/Status

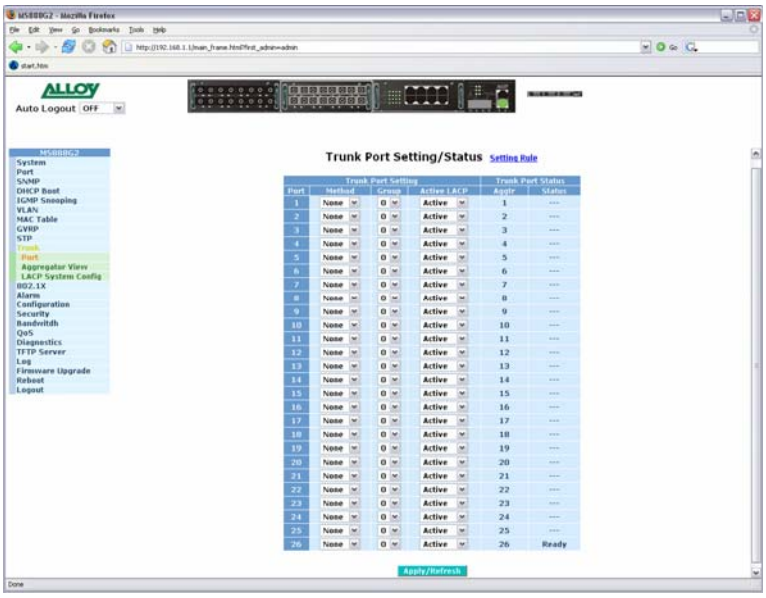

Fig. 3-41

Function name:

Port Settings/Status

Function description:

Port Settings/Status is used to configure the trunk properties of each port on the switch.

Parameters description:

Method:

Determines the method the port will use to aggregate with other ports.

None:

If none is selected the port will not be aggregated with any other ports.

LACP:

The port is using LACP to aggregate with other LACP aware ports.

Static:

The port is using Static Trunking to aggregate with other Static Trunk groups.

Group:

Ports that are going to be aggregated, whether it be with LACP or using Static Trunking must be assigned a unique Group ID, this ID can be from 1 - 3.

Active LACP:

This field will only be used when using LACP.

Active:

An Active LACP port will send LACPDU to its link partner right after the LACP protocol entity has started to take control of the port.

Passive:

A Passive LACP port will not send LACPDU to its link partner until it receives LACPDU from the link partner.

Aggtr:

Aggtr is an abbreviation of “Aggregator”. Every port is an aggregator, and its own aggregator ID is the same as its port number. We can regard an aggregator as a representative of a trunking group. Ports with the same Group ID and trunking method have the opportunity to aggregate to a particular aggregator port. This aggregator port is usually the port with the smallest port number within the trunking group.

Status:

This field represents the status of a port belonging to a trunking group.

3-10-2. Aggregator View

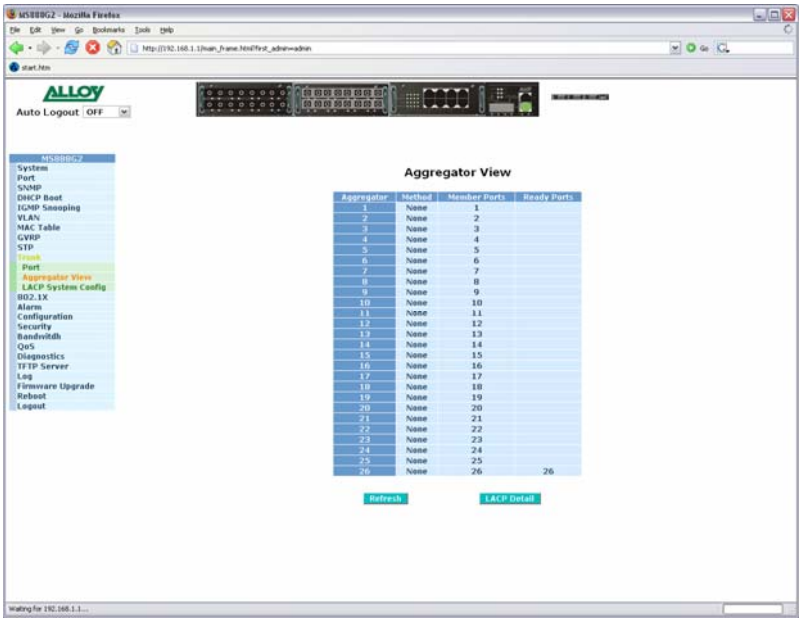

Fig. 3-42

Function name:

Aggregator View

Function description:

Shows the current port trunking information from the aggregator point of view.

Parameters description:

Aggregator:

Shows the aggregator ID of every port. In fact, every port is an aggregator, and its aggregator ID is the same as its own port number.

Method:

Shows the method the port uses to aggregate with other ports.

Member Ports:

Shows all member ports of an aggregator.

Ready Ports:

Shows only the ready member ports within an aggregator.

3-10-2-1. LACP Detail

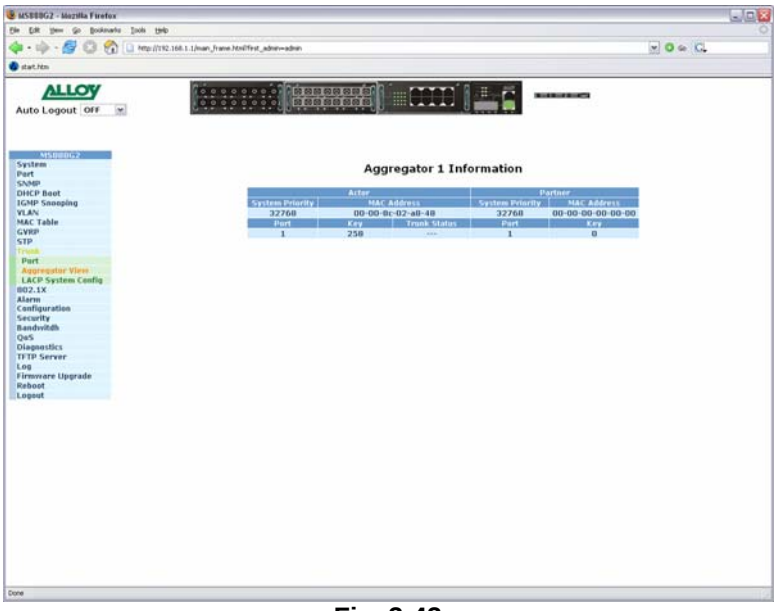

Fig. 3-43

Function name:

LACP Detail (LACP Aggregator Detailed Information

Function description:

Shows detailed information regarding the LACP trunking group

Parameters description:

Actor:

The switch that you are managing.

Partner:

The partner switch of the LACP trunk.

System Priority:

Shows the system priority of trunking group.

MAC Address:

Shows the MAC address of the local switch.

Port:

Shows the port number of a LACP port ID.

Key:

Shows the key value of the aggregator. The key value is determined by the LACP protocol entity and can't be set through the management.

Trunk Status:

Shows the trunk status of a single port.

3-10-3. LACP System Configuration

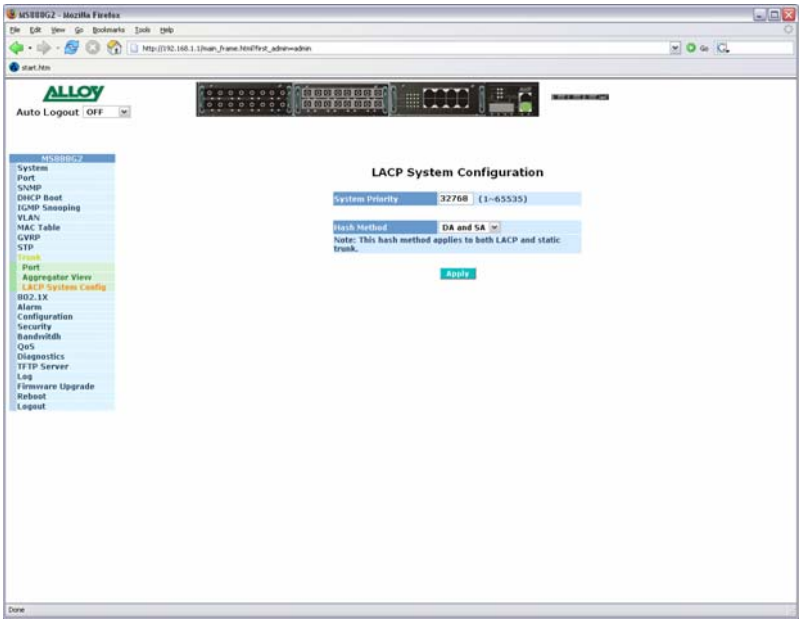

Fig. 3-44

Function name:

LACP System Configuration

Function description:

System Priority:

The LACP System Priority is used to set the priority of the LACP system ID. LACP will only aggregate ports whose partner ports belong to a single switch. Each system that has support for LACP will be assigned a globally unique System Identifier for this purpose. A system ID is a 64-bit field comprising of a 48-bit MAC address and a 16-bit priority value. The system priority can be set by the administrator with a valid range from 1 to 65535.

Default: 32768

Hash Method:

Select the appropriate Hash Method used for your LACP configuration. Options available are SA (Source Address), DA (Destination Address) or DA & SA.

Default: DA & SA

3-11. 802.1x Configuration

The 802.1x port-based network access control provides a method to restrict users to access network resources via authenticating user's information. This restricts users from gaining access to the network resources through an 802.1x-enabled port without authentication. Any user wishing to access the network through a port under 802.1x control, must first input their account name for authentication and then wait for the authorisation to complete before sending or receiving any data from an 802.1x-enabled port.

Before the devices or end stations can access the network resources through the ports under 802.1x control, the devices or end stations connected to a controlled port send the authentication request to the authenticator, the authenticator passes the request to the authentication server to authenticate and verify the username and password, and the server then tells the authenticator if the request has been granted access for that port.

According to IEEE802.1x, there are three components implemented. They are the Authenticator, the Supplicant and the Authentication server.

Supplicant:

It is an entity being authenticated by an authenticator. It is used to communicate with the Authenticator PAE (Port Access Entity) by exchanging the authentication message when the Authenticator PAE requests it.

Authenticator:

The Authenticator controls the state of the port, authorized or unauthorized, according to the result of the authentication message exchanged between it and a supplicant PAE. The authenticator may request the supplicant to re-authenticate itself at a configured time period. Once re-authentication to the supplicant starts, the controlled port will stay in the authorised state until re-authentication fails.

A port acting as an authenticator is thought to be two logical ports, a controlled port and an uncontrolled port. A controlled port can only pass packets when the authenticator PAE is authorised, otherwise, an uncontrolled port will unconditionally pass the packets with the PAE group MAC address, which has a value of 01-80-c2-00-00-03 and will not be forwarded by the MAC bridge, at any time.

Authentication server:

A device that provides the authentication service, through EAP, to an authenticator by using authentication credentials supplied by the supplicant to determine if the supplicant is authorised to access the network resource.

The overview of the 802.1x operation shown in Fig. 3-45 is quite simple. When the Supplicant PAE issues a request to the Authenticator PAE, the Authenticator and the Supplicant exchange authentication messages. Then, the Authenticator passes the request to the RADIUS server to verify the username and password. Finally, the RADIUS server replies if the request is granted or denied.

While in the authentication process, the message packets, encapsulated by Extensible Authentication Protocol over LAN (EAPOL), are exchanged between an authenticator PAE and a supplicant PAE. The Authenticator exchanges the messages to the authentication server using EAP encapsulation. Before successfully authenticating, the supplicant can only communicate with the authenticator to perform the authentication message exchange or access the network from an uncontrolled port.

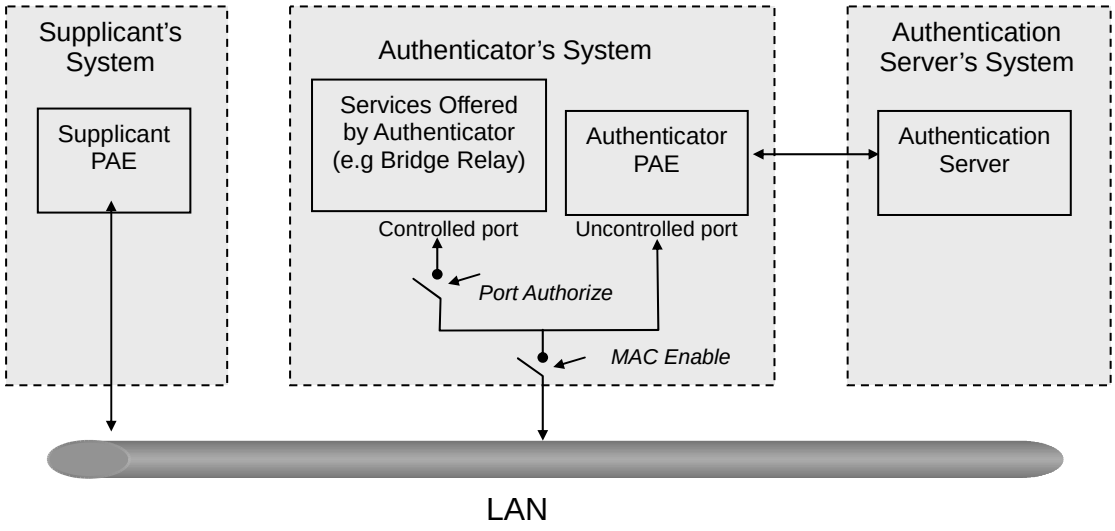

Fig. 3-45

In the Fig. 3-46, this is the typical configuration, a single supplicant, an authenticator and an authentication server. B and C are on the internal network, D is the Authentication server running RADIUS, the switch at the central location acts as the Authenticator connecting to PC A and A is a PC outside the controlled port, running Supplicant PAE. In this case, PC A wants to access the services on device B and C, first, it must exchange the authentication message with the authenticator on the port it is connected via EAPOL packet. The authenticator transfers the supplicant's credentials to the Authentication server for verification. If successful, the authentication server will tell the authenticator to grant access. PC A is then allowed to access B and C via the switch. If there are two switches directly connected together the link connecting the two switches, may have to act as two port roles at the end of the link: authenticator and supplicant, because the traffic is bi-directional.

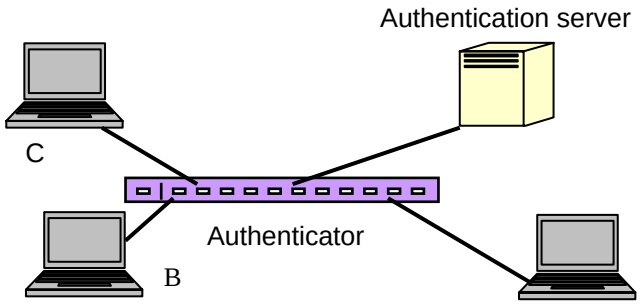

Fig. 3-46

Only MultiHost 802.1X authentication is supported in the MS888G2. In this mode devices connected to an 802.1x enabled port, can access network resources once the supplicant has been authenticated.

3-11-1. State

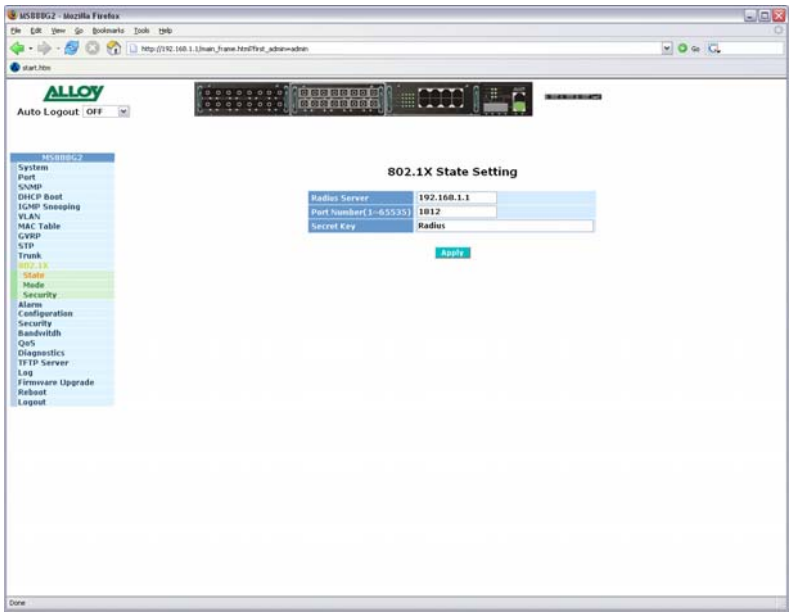

Fig. 3-47

Function name:

802.1x State Setting

Function description:

This function is used to configure the global parameters for the RADIUS authentication used with the 802.1x port security.

Parameters description:

Radius Server:

IP Address of the Radius Server.

Default: 192.168.1.1

Port Number:

The port number used to communicate with the RADIUS server. Valid port range is 1 – 65535.

Default: 1812

Secret Key:

The secret key is used to authenticate the RADIUS server with the Authenticator. The secret key is an ASCII based string with a length of 1 – 31 characters, with no blank spaces allowed.

Default: Radius

3-11-2. Mode

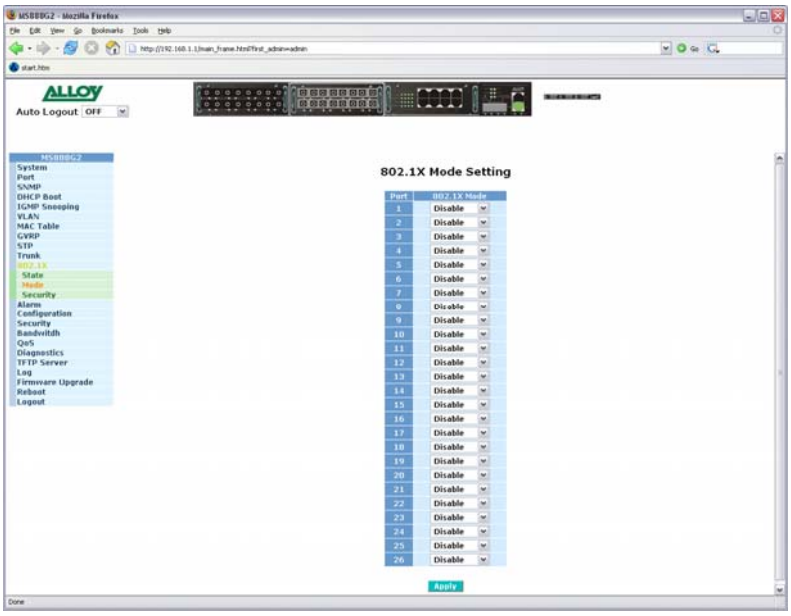

Fig. 3-48

Function name:

802.1x Mode Setting

Function description:

This function is used to set the operation mode of 802.1x for each individual port and only supports Multihost or Disabled modes.

Parameters description:

Port Number:

Indicates which port is selected for setting up the 802.1x mode.

802.1x Mode:

There are two modes that can be selected, they are Disabled and Multihost mode.

Disable:

The selected port will not use 802.1x authentication.

Multihost:

Once the supplicant has been authenticated they can then access network resources through that port.

3-11-3. Security

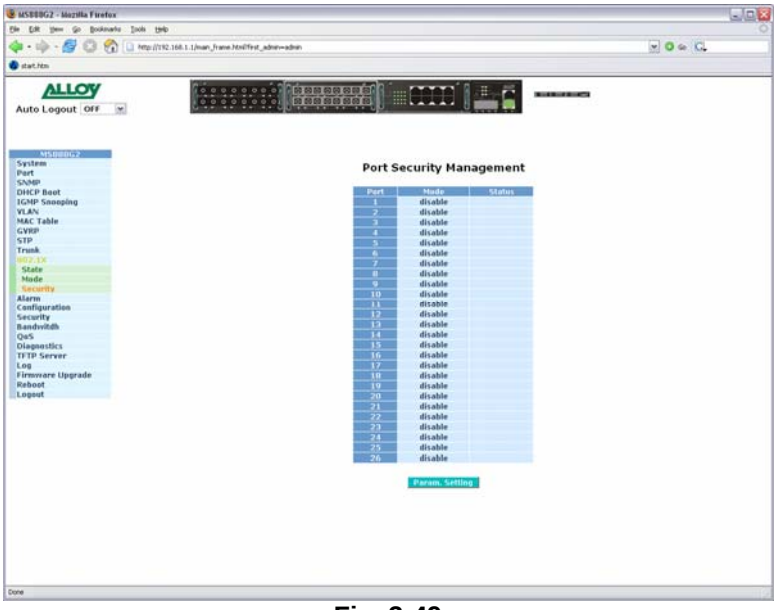

Fig. 3-49

Function name:

Port Security Management

Function description:

Shows the status of each port, the port number, and if the port is authorised or unauthorised.

Parameters description:

Disable Mode:

When set to disabled the port will not use 802.1x to authenticate the user before they have access to network resources.

Port Number:

The port number chosen to show its 802.1x status.

Port Status:

The current 802.1x status of the port.

802.1x with Multihost mode:

If a port has been configured to use 802.1x Multihost mode, devices can access network resources once they have been authorised. If the port has been authorised, authorised will be displayed in the ports status section, if the user has not been authorised, then unauthorised will be displayed.

3-11-4. Parameter Setting

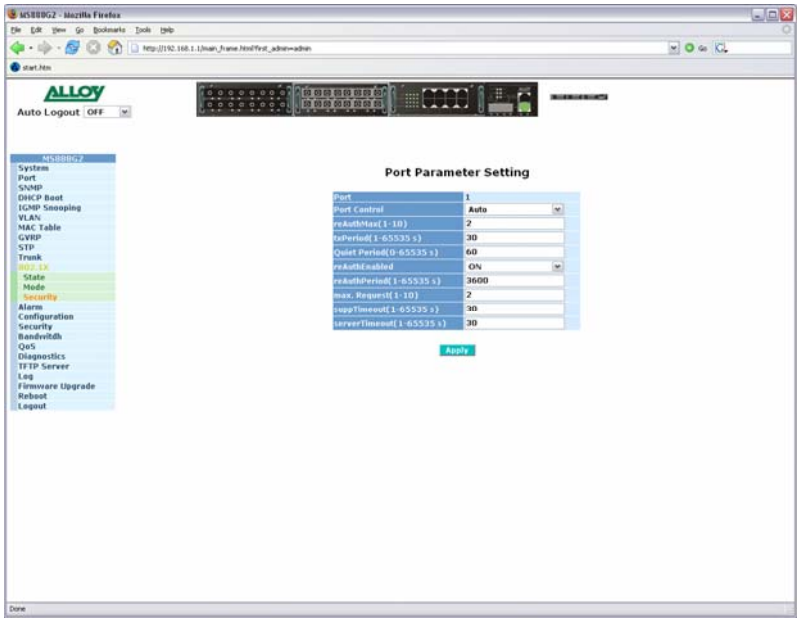

Fig. 3-50

Function name:

Parameter Setting

Function description:

This section is used to configure the parameter settings for each port using 802.1x port security.

Parameters description:

Port:

The port number to be selected to configure 802.1x parameters.

Port Control:

This is used to set the operation mode of the port. There are three modes supported ForceUnauthorised, ForceAuthorised and Auto.

- ForceUnauthorised: The controlled port is forced to stay in the unauthorised state.
- ForceAuthorised: The controlled port is forced to stay in the authorised state.
- Auto: The controlled port will determine its authorisation state depending on the result of the authentication between the authentication server and the supplicant.

Default: Auto

reAuthMAx (1-10):

The number of authentication attempts that are permitted before the port becomes unauthorised.

Default: 2

txPeriod (1 – 65535 sec.):

Period of time in seconds to transmit EAPOL PDU between the authenticator and the supplicant.

Default: 30

Quiet period (0 – 65535 sec.):

Period of time in which we will not attempt to access the supplicant.

Default: 60

reAuthEnabled:

Select whether regular authentication will occur on this port.

Default: On

reAuthPeriod (1 – 65535 sec.):

Period of time in seconds between the periodic re-authentication of the supplicant.

Default: 3600

Max. Request (1-10):

The maximum number of times the authenticator will re-transmit an EAP request to the supplicant before it times out the authentication session.
Valid range: 1 -10.

Default: 2 times

suppTimeout (1 – 65535 sec.):

A time out condition in the exchange between the authenticator and the supplicant.
Valid range: 1 – 65535.

Default: 30

serverTimeout (1- 65535 sec.):

A time out condition in the exchange between the authenticator and the authentication server.
Valid range: 1 – 65535.

Default: 30

3-12. Alarm Configuration

The MS888G2 supports a number of trap messages that can be sent to an administrator if certain events occur on the switch. The switch offers 24 different trap events that can be sent to the administrator in 3 different ways; email, mobile phone SMS or trap.

3-12-1. Trap Events Configuration

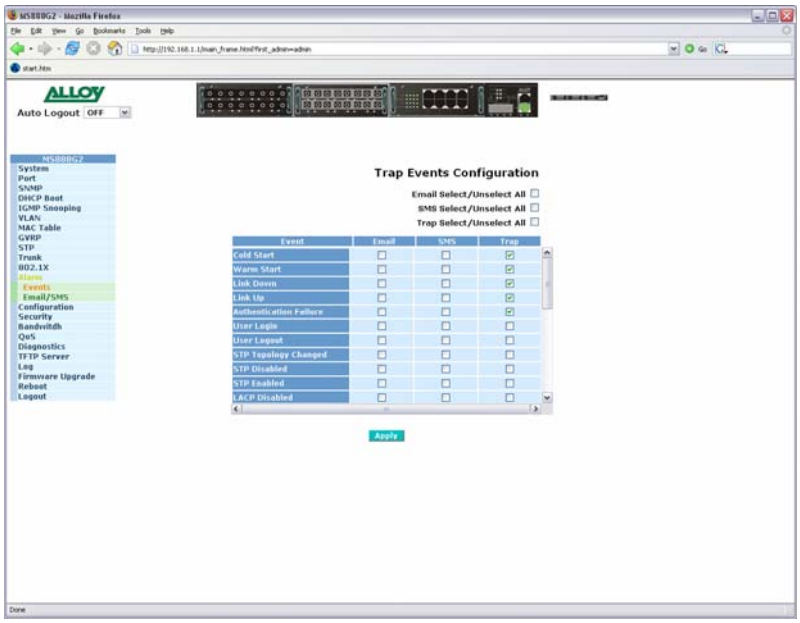

Fig. 3-51

Function name:

Events Configuration

Function description:

The Trap Events Configuration function is used to enable the switch to send out trap information while pre-defined trap events occur.

Parameters description:

Email Select/Unselect All:

Tick this checkbox to automatically highlight all email trap messages.

SMS Select/Unselect All:

Tick this checkbox to automatically highlight all SMS trap messages.

Trap Select/Unselect All:

Tick this checkbox to automatically highlight all Trap messages.

Cold Start:

Tick the required trap method check box to enable a trap to be sent when the switch has a cold start.

Warm Start:

Tick the required trap method check box to enable a trap to be sent when the

switch has a warm start.

Link Down:

Tick the required trap method check box to enable a trap to be sent when a port on the switch loses link.

Link Up:

Tick the required trap method check box to enable a trap to be sent when a port on the switch establishes link.

Authentication Failure:

Tick the required trap method check box to enable a trap to be sent when authorisation to the switches management fails.

User Login:

Tick the required trap method check box to enable a trap to be sent when a user logs on to the switches management.

User Logout:

Tick the required trap method check box to enable a trap to be sent when a user logs out of the switches management.

STP Topology Changed:

Tick the required trap method check box to enable a trap to be sent when the STP Topology has changed.

STP Disabled:

Tick the required trap method check box to enable a trap to be sent when STP has been disabled.

STP Enabled:

Tick the required trap method check box to enable a trap to be sent when STP has been enabled.

LACP Disabled:

Tick the required trap method check box to enable a trap to be sent when LACP has been disabled.

LACP Enabled:

Tick the required trap method check box to enable a trap to be sent when LACP has been enabled.

LACP Member Added:

Tick the required trap method check box to enable a trap to be sent when a LACP Member has been added.

LACP Port Failure:

Tick the required trap method check box to enable a trap to be sent when a LACP Port has failed.

GVRP Disabled:

Tick the required trap method check box to enable a trap to be sent when GVRP has been disabled.

GVRP Enabled:

Tick the required trap method check box to enable a trap to be sent when GVRP has been enabled.

VLAN Disabled:

Tick the required trap method check box to enable a trap to be sent when VLAN support has been disabled.

Port-based VLAN Enabled:

Tick the required trap method check box to enable a trap to be sent when Port-based VLAN support has been enabled.

Tag-based VLAN Enabled:

Tick the required trap method check box to enable a trap to be sent when Tag-based VLAN support has been enabled.

Metro-Mode VLAN Enabled:

Tick the required trap method check box to enable a trap to be sent when Metro-Mode VLAN support has been enabled.

Double-tag VLAN Enabled:

Tick the required trap method check box to enable a trap to be sent when Double-Tag VLAN support has been enabled.

Module Inserted:

Tick the required trap method check box to enable a trap to be sent when a Module has been inserted.

Module Removed:

Tick the required trap method check box to enable a trap to be sent when a Module has been removed.

Dual Media Swapped:

Tick the required trap method check box to enable a trap to be sent when the dual media port has been swapped from fibre to copper or vice versa.

3-12-2. Email/SMS Configuration

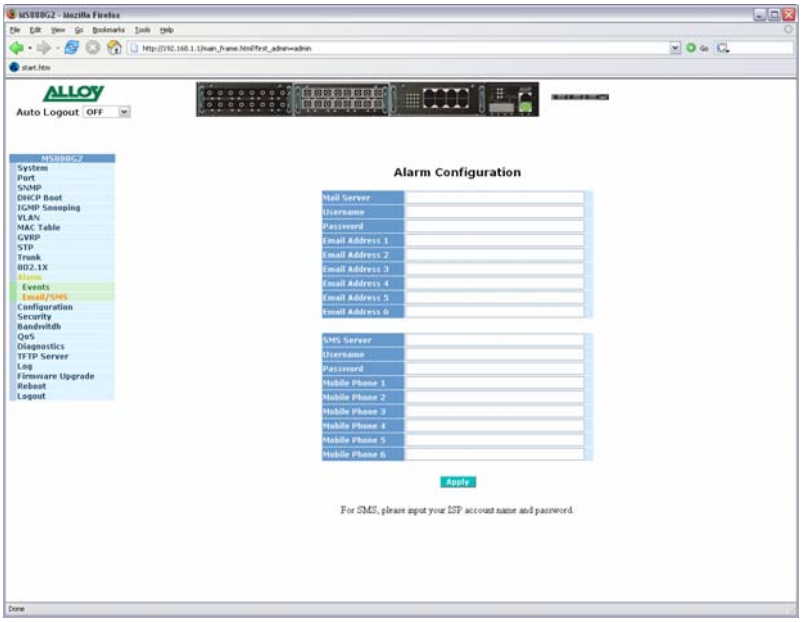

Fig. 3-52

Function name:

Email/SMS Configuration

Function description:

The Alarm Configuration is used to configure who should receive the trap messages via Email, SMS or both which have been sent from the MS888G2. Up to 6 email addresses can be entered as well as 6 SMS mobile phone numbers. If using SMS you will need to enter the SMS ISP details. (Note this may not work with your mobile phone network.) If using Email you also need to enter the Email Server details in the spaces provided.

Parameters description:

Mail Server:

Enter the IP Address of the mail server used to send emails.

Username:

Enter the username required by the email server.

Password:

Enter the password required by the email server.

Email Address 1 – 6:

Enter the email address(s) that will receive the trap messages.

SMS Server:

Enter the IP Address of the SMS server used to send SMS messages.

Username:

Enter the username required by the SMS server.

Password:

Enter the password required by the SMS server.

Email Address 1 – 6:

Enter the mobile phone number(s) that will receive the trap messages.

3-13. Configuration

The MS888G2 has support for multiple configuration files to be used by the administrator including the default configuration, start configuration and user configuration. In this section the administrator can save the switch's configuration, restore the switch to factory default and also save the current configuration as the startup configuration when the switch is re-booted.

3-13-1. Save / Restore Configuration

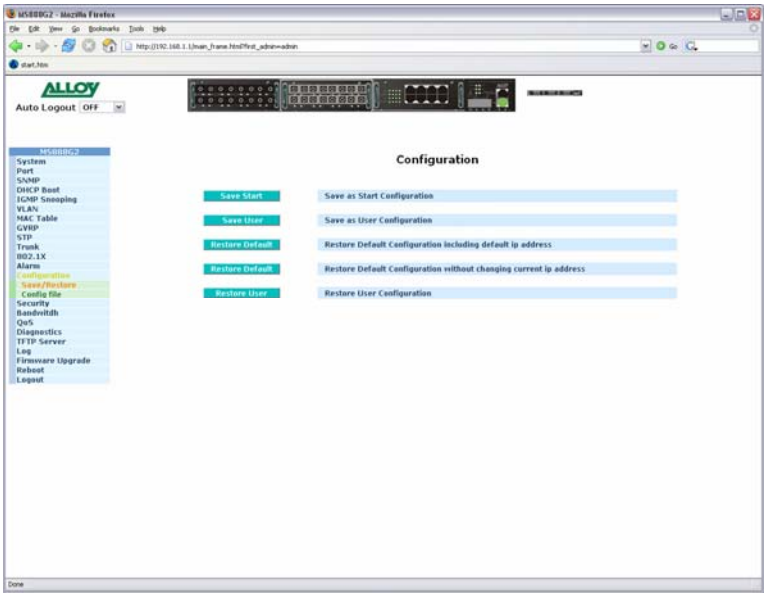

Fig. 3-53

Function name:

Save / Restore Configuration

Function description:

Used by the administrator to save and restore the configuration used in the MS888G2.

Parameters description:

Save Start:

Saves the current switch configuration as the start up configuration of the switch.

Save User:

Saves the current switch configuration as the user configuration.

Restore Default:

Restore the default configuration of the switch including the default IP address.

Restore Default:

Restore the default configuration of the switch without changing the IP address.

Restore User:

Restore the saved user configuration.

3-13-2. Config File

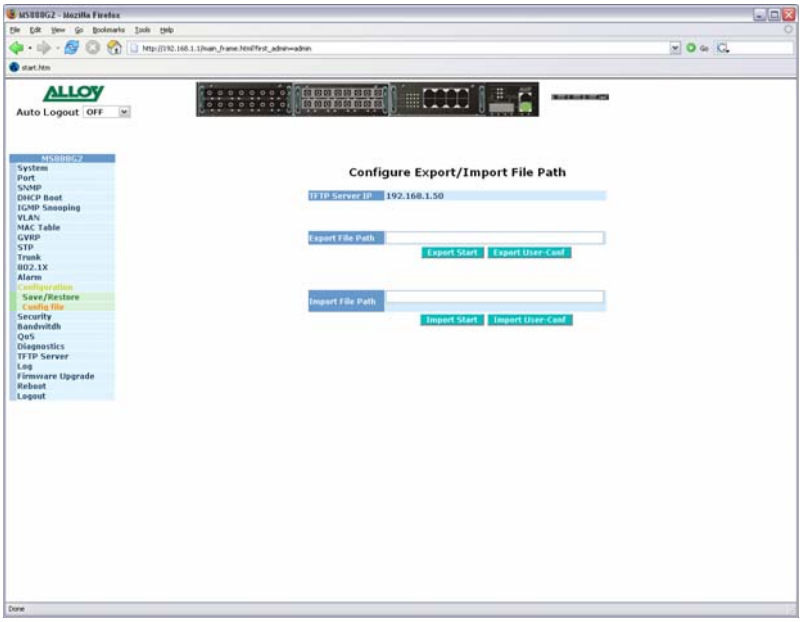

Fig. 3-54

Function name:

Configure Export/Import File Path

Function description:

Used by the administrator to Export and Import the start and user configuration files.

Parameters description:

TFTP Server:

Displays the current TFTP Server configuration. This is read only. TFTP Server can be configured under the TFTP section.

Export File Path:

Enter the file path of where you would like to export the configuration file.

Export Start:

After configuring the export path click on the export start button to export the startup configuration file.

Export User-Conf:

After configuring the export path click on the export user-conf button to export the User-Conf configuration file.

Import File Path:

Enter the file path of where you would like to import the configuration file from.

Import Start:

After configuring the import path click on the import start button to import the startup configuration file.

Import User-Conf:

After configuring the import path click on the import user-conf button to import the User-Conf configuration file.

3-14. Security

The Mirror function of the MS888G2 is used to capture data from a particular port on the switch. Any port on the switch can be selected as the monitoring port; this port will be used to capture data from another port on the switch using third party data capturing software. Data can be captured from more than one port on the switch simultaneously therefore you can have one monitoring port and several other ports being monitored by the one port. The MS888G2 also supports Isolated and restricted group functions for additional security.

3-14-1. Mirror

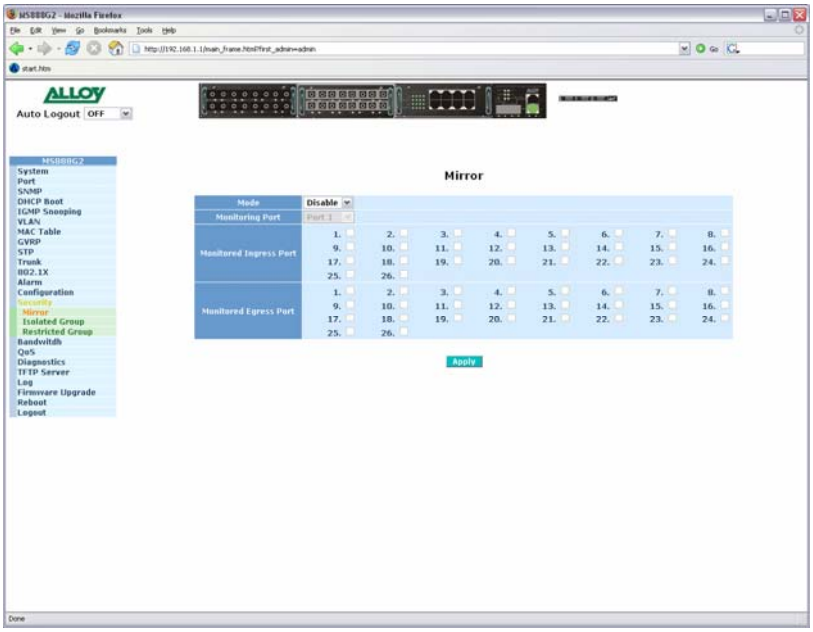

Fig. 3-55

Function Name:

Mirror Configuration

Function Description:

The Mirror Configuration is used to configure a port to capture data that is being sent and received through another port on the switch.

Parameter Description:

Mode:

Is used to enable or disable the mirror function of the switch.

Default: Disable

Monitoring Port:

Here you can select which port is going to be used as the monitoring port.

Default: Port 1

Monitored Port:

Select which port you wish to be monitored. Just tick the check box next to the appropriate port(s) and click apply.

3-14-2. Isolated Group

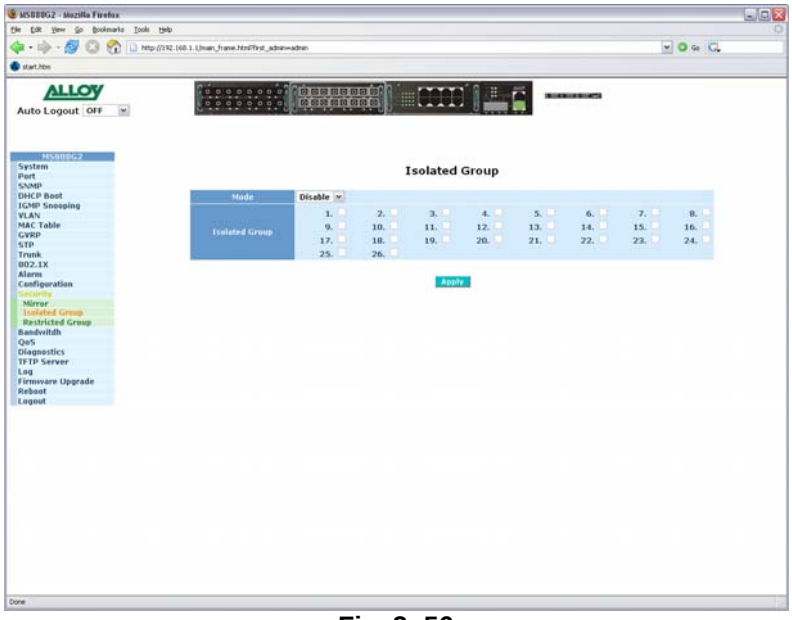

Fig. 3- 56

Function Name:

Isolated Group

Function Description:

The Isolated Group function allows ports to be isolated from other ports on the switch. Communication between any isolated ports is forbidden. Therefore all ports that belong to the isolated group can no longer communicate with each other but, all ports in the isolated group can still communicate with ports that do not belong to the isolated group.

Parameter Description:

Mode:

Select to enable or disable the isolated group function.

Isolated Group:

Select the ports that you wish to belong to the isolated group.

3-14-3. Restricted Group

Fig. 3- 57

Function Name:

Restricted Group

Function Description:

The Restricted Group function enables certain ports packets to be sent directly to another port on the switch. If port 1 is part of the Ingress restricted group and port 10 is part of the Egress restricted group and data is received on port 1 the data will be automatically sent out port 10.

Parameter Description:

Mode:

Select to enable or disable the restricted group function.

Ingress:

Select the ports that you wish to belong to the Ingress Restricted group.

Egress:

Select the ports that you wish to belong to the Egress Restricted group.

3-15. Bandwidth

The Bandwidth Management function of the MS888G2 is used to limit the bandwidth a port may use when sending or receiving data. When limiting received data you can limit the bandwidth on a particular type of data, including all Traffic or Multicast and Broadcast Traffic.

When you click on the bandwidth menu on the left hand side a screen will appear with all ports being displayed with their current Bandwidth settings. To configure each individual ports bandwidth characteristics, highlight the port and click the Edit button on the bottom of the screen.

3-15-1. Ingress

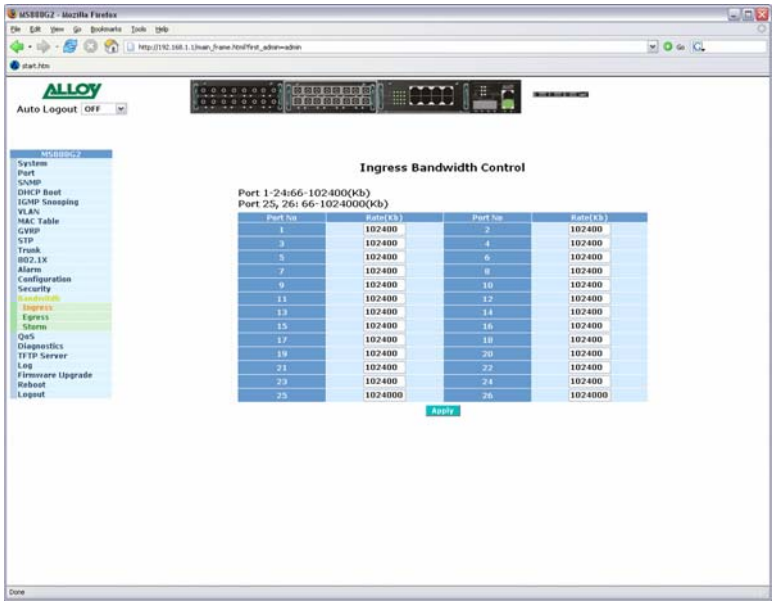

Fig. 3-58

Function Name:

Ingress

Function Description:

The Bandwidth Management function is used to limit the ingress (Incoming) bandwidth for each port.

Parameter Description:

Port Number:

Displays the current port that is being configured, this will depend on the port that was highlighted before the Edit button was pressed.

Rate:

Is used to set up the limit of Ingress bandwidth the port is allowed to utilise before traffic will be discarded. If the data exceeds the limit you have set all traffic will be discarded. Pause frames are also generated to stop the discarding of packets if Flow Control is enabled. The Ingress Rate Limiting will limit all data including unicast, broadcast and multicast traffic. Valid range is 66 ~ 1024000.

3-15-2. Egress

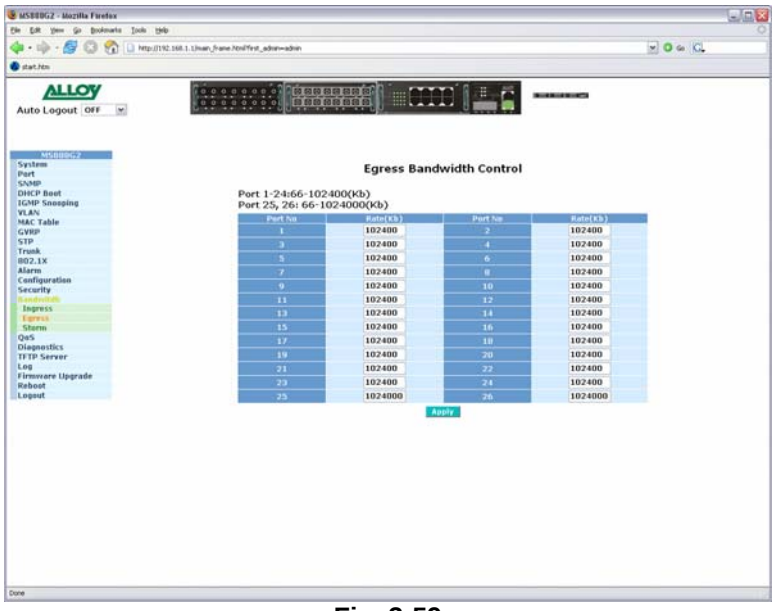

Fig. 3-59

Function Name:

Egress

Function Description:

The Bandwidth Management function is used to limit the Egress (Outgoing) bandwidth for each port.

Parameter Description:

Port Number:

Displays the current port that is being configured, this will depend on the port that was highlighted before the Edit button was pressed.

Rate:

Is used to set up the limit of Egress bandwidth the port is allowed to utilise before traffic will be discarded. If the data exceeds the limit you have set all traffic will be discarded. Pause frames are also generated to stop the discarding of packets if Flow Control is enabled. The Ingress Rate Limiting will limit all data including unicast, broadcast and multicast traffic. Valid range is 66 ~ 1024000.

3-15-3. Storm

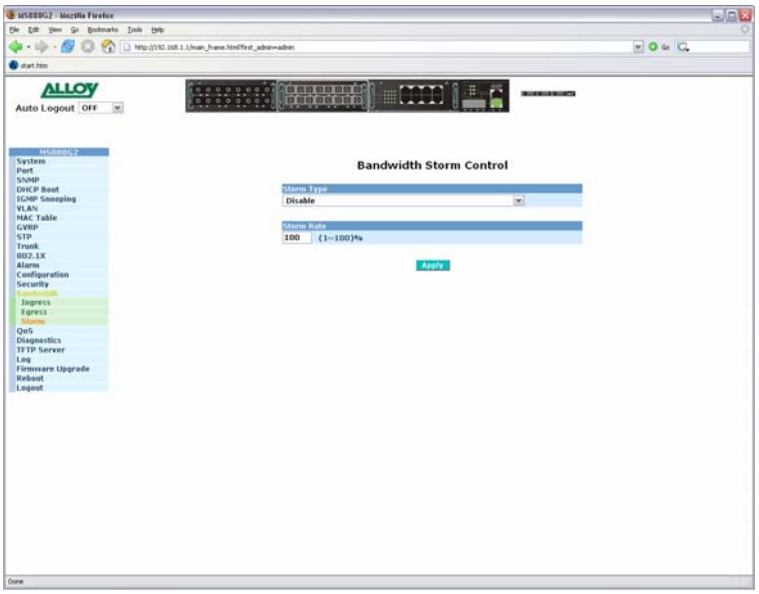

Fig. 3-60

Function Name:

Storm

Function Description:

The Bandwidth Management function is used to limit broadcast traffic on your network.

Parameter Description:

Disable:

Disable bandwidth storm control.

Broadcast Storm Control:

Enables bandwidth storm control for all broadcast traffic.

Multicast Storm Control:

Enables bandwidth storm control for all multicast traffic.

Unknown Unicast Storm Control:

Enables bandwidth storm control for all unknown unicast traffic. This usually consists of packets with MAC addresses that have not yet been learnt by the switch.

Broadcast, Multicast and Unknown Unicast Storm Control:

Enables bandwidth storm control for all traffic.

Storm Rate:

Used to set the storm control limit. Valid values are 1 – 100%.

3-16. QOS (Quality of Service)

The switch offers powerful QoS functions including: Per Port Priority called VIP where any port that is enabled as a VIP Port will have a higher priority over a standard port, 802.1p Priority, IP TOS Priority and IP DiffServe DSCP Priority.

3-16-1. Global

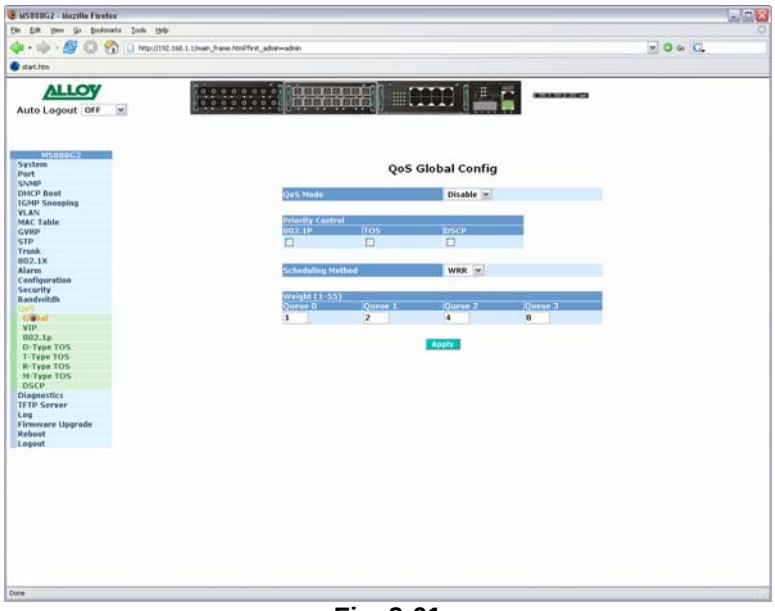

Fig. 3-61

Function Name:

Global

Function Description:

The Global QoS settings are used to enable the QoS function on the switch and select what QoS method to be used. The Priority Control field allows you to select 3 different priority methods including 802.1p, TOS and DSCP. You can also select the scheduling method that you would like to use including Weighted Round Robin and Strict Priority and also set the weight values for bits 0 through to 3.

Parameter Description:

QoS Mode:

Select Enable to enable the QoS function or Disable to disable the QoS function.

Priority Control:

Tick the appropriate tick boxes to enable the type of priority methods to use..

Scheduling Method:

Select the type of scheduling method that you would like to use. The default vale is WRR.

Weight (1 – 55):

Select the weight values for bits 0 through to 3. Valid values 1 through to 55.

3-16-2. VIP

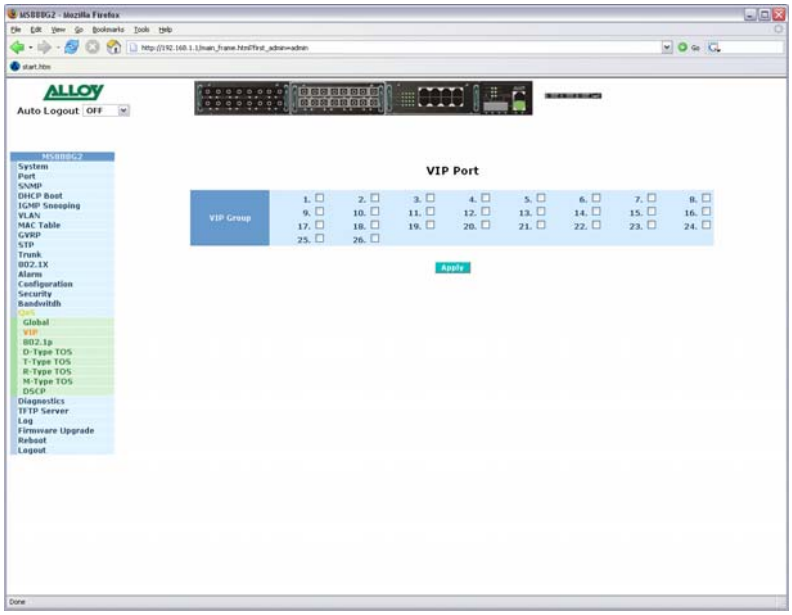

Fig. 3-62

Function Name:

VIP

Function Description:

The VIP function allows an easy way to set a high priority to a particular port on the switch. If you wish to set a high priority on ports 1 through to 5 tick the appropriate check boxes and click the apply button. If the switch now becomes congested ports 1 through to 5 will have a higher priority than all other ports on the switch.

Parameter Description:

VIP Port:

Select the port(s) that you wish to have a high priority and click the apply button.

3-16-3. 802.1p

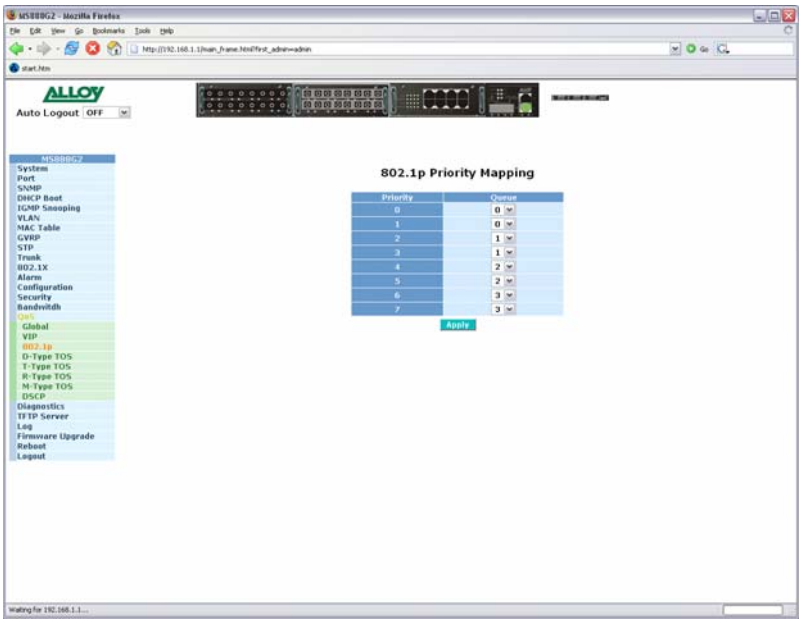

Fig. 3-63

Function Name:

802.1p

Function Description:

The 802.1p priority function is based on the priority of the VLAN tag, it can be arranged into 8 priority levels which map to 4 different priority queues (0 – 3).

Parameter Description:

802.1p Priority Mapping:

Each Priority level can be assigned to any Queue from 0 through to 3. The Default values are as follows: Priority 0 is mapped to Queue 0, Priority 1 is mapped to Queue 0, Priority 2 is mapped to Queue 1, Priority 3 is mapped to Queue 1, Priority 4 is mapped to Queue 2, Priority 5 is mapped to Queue 2, Priority 6 is mapped to Queue 3, and Priority 0 is mapped to Queue 3.

3-16-4. D-Type TOS

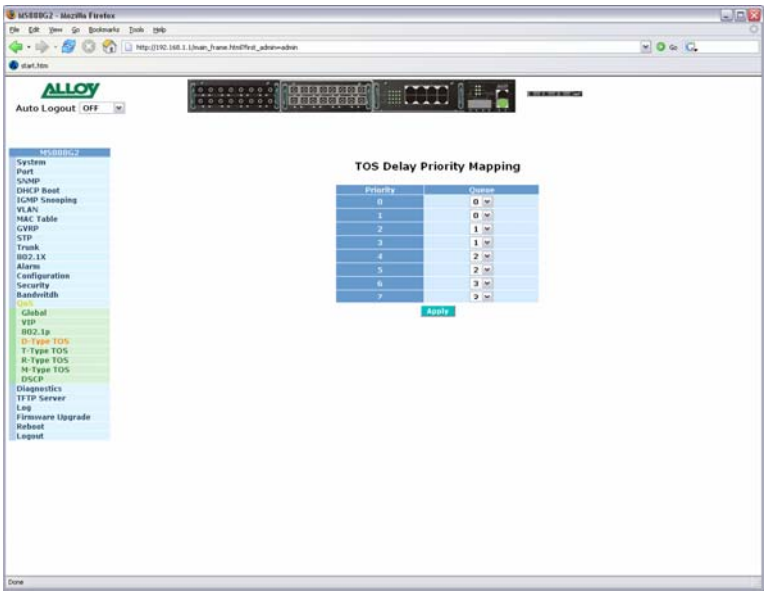

Fig. 3-64

Function Name:

TOS Delay Priority Mapping

Function Description:

The IP TOS Priority affects the TOS fields of the IP header using an 8 bit service type field to specify how the datagram should be handled. The TOS field can be divided into six subfields as follows: Precendence (3 Bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1 bit), R-Type (Reliability Priority, 1 bit), M-Type (Monetary Cost Priority, 1 bit) and Unused. TOS Delay Priority Mapping will be utilised if configured in the following section.

Parameter Description:

TOS Delay Priority Mapping:

Each Priority level can be assigned to any Queue from 0 through to 3. The Default values are as follows: Priority 0 is mapped to Queue 0, Priority 1 is mapped to Queue 0, Priority 2 is mapped to Queue 1, Priority 3 is mapped to Queue 1, Priority 4 is mapped to Queue 2, Priority 5 is mapped to Queue 2, Priority 6 is mapped to Queue 3, and Priority 0 is mapped to Queue 3.

3-16-5. T-Type TOS

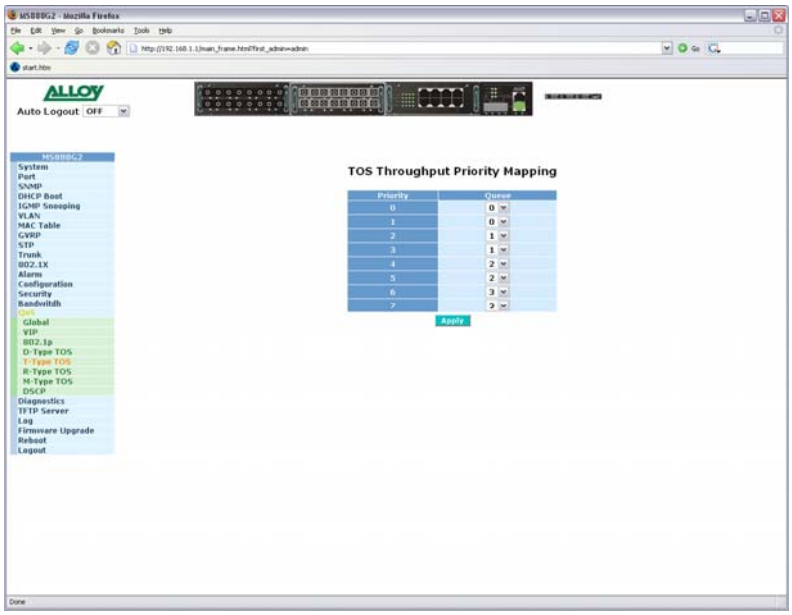

Fig. 3-65

Function Name:

TOS Throughput Priority Mapping

Function Description:

The IP TOS Priority affects the TOS fields of the IP header using an 8 bit service type field to specify how the datagram should be handled. The TOS field can be divided into six subfields as follows: Precendence (3 Bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1 bit), R-Type (Reliability Priority, 1 bit), M-Type (Monetary Cost Priority, 1 bit) and Unused. TOS Throughput Priority Mapping will be utilised if configured in the following section.

Parameter Description:

TOS Throughput Priority Mapping:

Each Priority level can be assigned to any Queue from 0 through to 3. The Default values are as follows: Priority 0 is mapped to Queue 0, Priority 1 is mapped to Queue 0, Priority 2 is mapped to Queue 1, Priority 3 is mapped to Queue 1, Priority 4 is mapped to Queue 2, Priority 5 is mapped to Queue 2, Priority 6 is mapped to Queue 3, and Priority 0 is mapped to Queue 3.

3-16-6. R-Type TOS

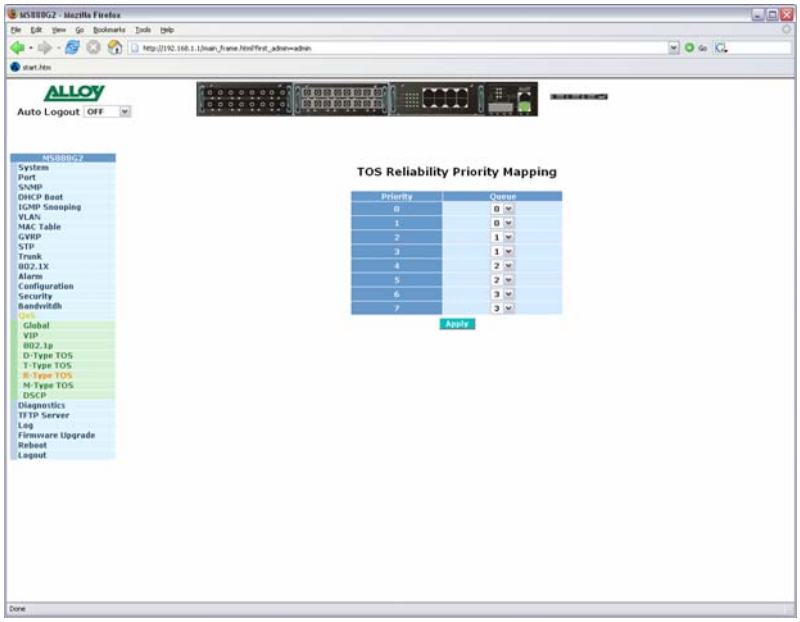

Fig. 3-66

Function Name:

TOS Reliability Priority Mapping

Function Description:

The IP TOS Priority affects the TOS fields of the IP header using an 8 bit service type field to specify how the datagram should be handled. The TOS field can be divided into six subfields as follows: Precendence (3 Bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1 bit), R-Type (Reliability Priority, 1 bit), M-Type (Monetary Cost Priority, 1 bit) and Unused. TOS Reliability Priority Mapping will be utilised if configured in the following section.

Parameter Description:

TOS Reliability Priority Mapping:

Each Priority level can be assigned to any Queue from 0 through to 3. The Default values are as follows: Priority 0 is mapped to Queue 0, Priority 1 is mapped to Queue 0, Priority 2 is mapped to Queue 1, Priority 3 is mapped to Queue 1, Priority 4 is mapped to Queue 2, Priority 5 is mapped to Queue 2, Priority 6 is mapped to Queue 3, and Priority 0 is mapped to Queue 3.

3-16-7. M-Type TOS

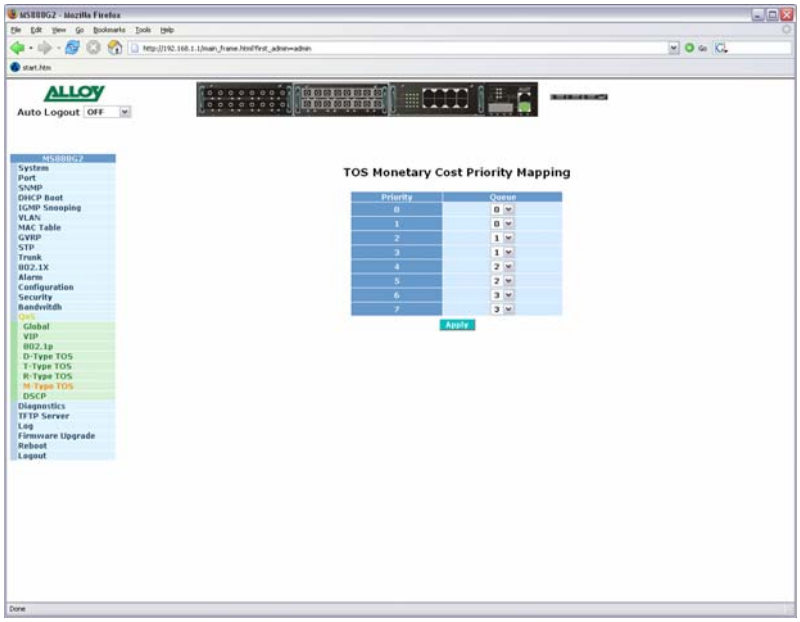

Fig. 3-67

Function Name:

TOS Monetary Cost Priority Mapping

Function Description:

The IP TOS Priority affects the TOS fields of the IP header using an 8 bit service type field to specify how the datagram should be handled. The TOS field can be divided into six subfields as follows: Precendence (3 Bits), D-Type (Delay Priority, 1 bit), T-Type (Throughput Priority, 1 bit), R-Type (Reliability Priority, 1 bit), M-Type (Monetary Cost Priority, 1 bit) and Unused. TOS Monetary Cost Priority Mapping will be utilised if configured in the following section.

Parameter Description:

TOS Monetary Cost Priority Mapping:

Each Priority level can be assigned to any Queue from 0 through to 3. The Default values are as follows: Priority 0 is mapped to Queue 0, Priority 1 is mapped to Queue 0, Priority 2 is mapped to Queue 1, Priority 3 is mapped to Queue 1, Priority 4 is mapped to Queue 2, Priority 5 is mapped to Queue 2, Priority 6 is mapped to Queue 3, and Priority 0 is mapped to Queue 3.

3-16-8. DSCP Setting

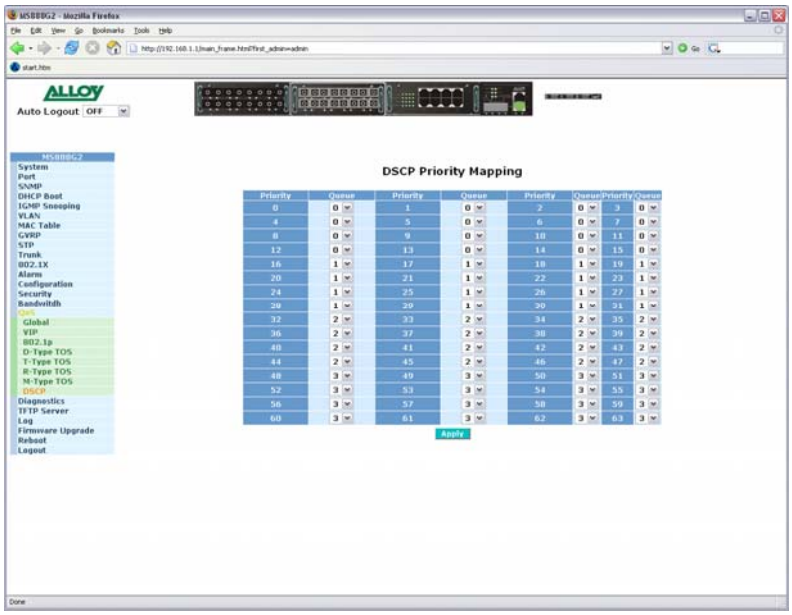

Fig. 3-68

Function Name:

DSCP Setting

Function Description:

The MS888G2 allows the administrator to configure priority levels based on the 6-bit field in the DSCP of the IP packet. The 6-bit field allows a total of 64 different traffic classes in which you can set a High or a Low priority.

Parameter Description:

Diffserv:

Displays the 64 traffic classes in which a priority level can be assigned.

Class:

Set a High or Low priority level to any of the 64 different traffic classes.

3-17. Diagnostics

Three Diagnostic tools are supported in the MS888G2 including Diagnostics, Loopback test and Ping test.

3-17-1. Diag

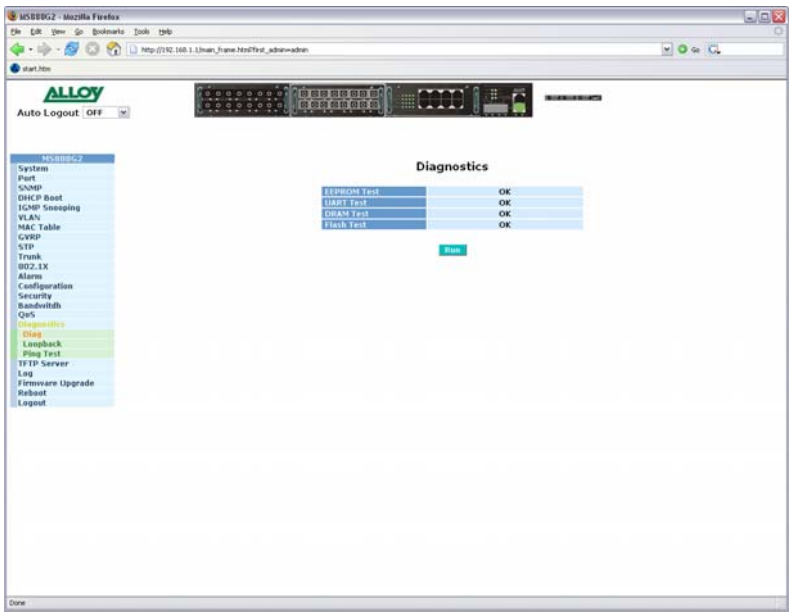

Fig. 3-69

Function name:

Diagnostics

Function description:

Provides a basic set of Diagnostic functions to allow the administrator to diagnose whether the switch is working correctly.

Parameters description:

EEPROM Test:

Self tests the EEPROM used in the switch.

UART Test:

Self tests the UART in the switch.

DRAM Test:

Self test the DRAM used in the switch.

Flash Test:

Self test the Flash RAM used in the switch.

3-17-2. Loopback Test

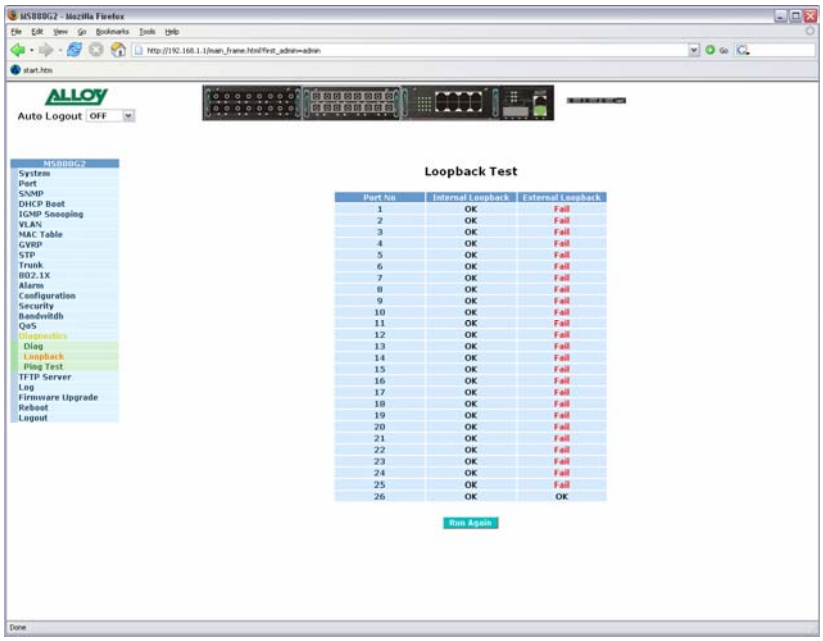

Fig. 3-70

Function name:

Loopback Test

Function description:

The MS888G2 has support for two types of loopback tests including an Internal and an External loopback test. The internal loopback test is an internal test and no test signal is sent out of the switch. The external loopback test will send the test signal to its link partner to check if the port has got an active link. If there is no active link the external loopback test will fail.

Parameters description:

Port No:

Displays all ports on the switch.

Internal Loopback:

Displays the internal loopback test results.

External Loopback:

Displays the external loopback test results.

Run Again:

Click on this button to perform the loopback tests.

3-17-3. Ping Test

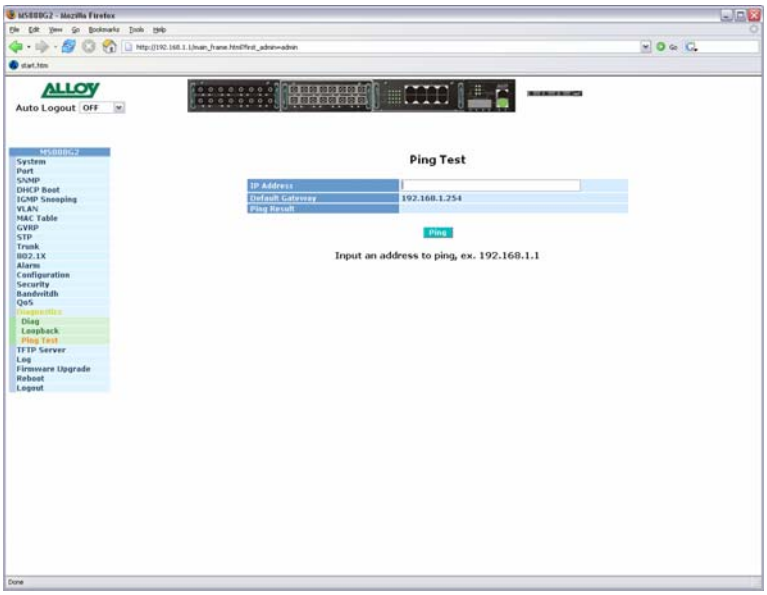

Fig. 3-71

Function name:

Ping Test

Function description:

The MS888G2 supports a ping test function to allow the switch to test communication between other IP based devices.

Parameters description:

IP Address:

Enter an IP Address that you would like to test connectivity between.

Default Gateway:

Displays the default gateway of the switch.

Ping Result:

Displays the ping result from the ping test, the results will be “IP Address is dead” if there is no communication between the devices that you are trying to ping or “IP Address is alive” if there is communication between the devices.

3-18. TFTP Server

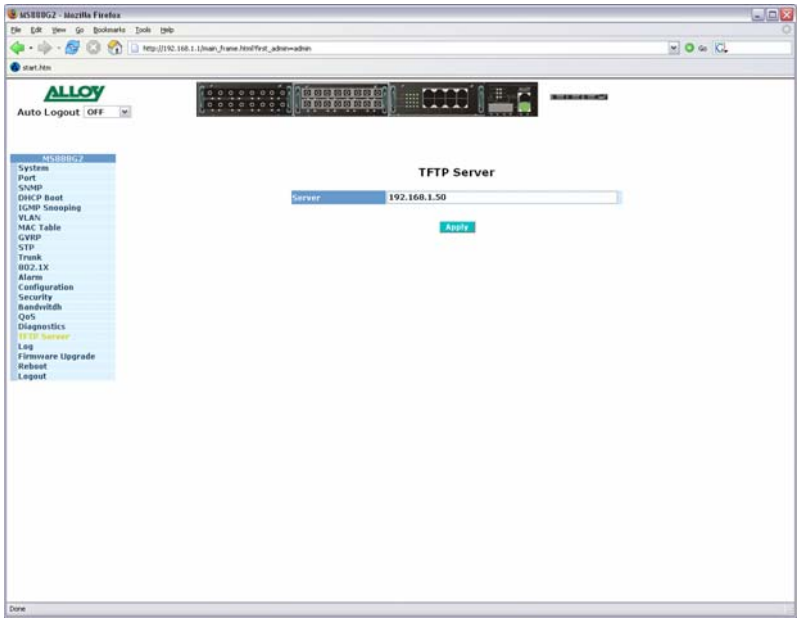

Fig. 3-72

Function name:

TFTP Server

Function description:

Used to set the IP address of the TFTP Server.

Parameters description:

Server:

Enter the IP address of the TFTP Server.

3-19. Log

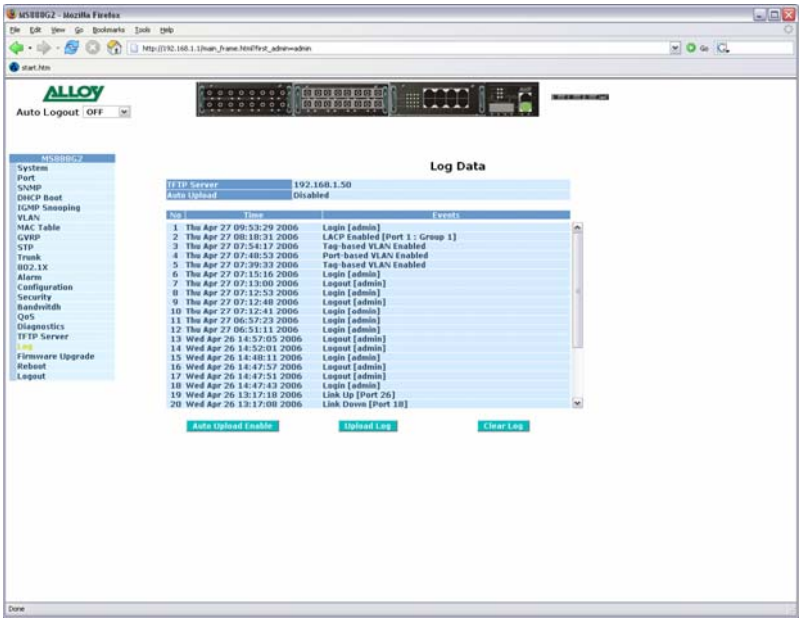

Fig. 3-73

Function name:

Log Data

Function description:

The Trap Log Data displays all SNMP Private trap events, SNMP Public traps and all other user logs. The MS888G2 supports up to 120 log entries.

Parameters description:

No:

Displays the order number of all entries in the log.

Time:

Displays the Time that the trap occurred.

Events:

Displays the name of the trap event that has occurred.

Auto Upload Enable:

Switch the Auto Upload status from enabled to disabled.

Upload Log:

Upload the contents of the log via a TFTP Server.

Clear Log:

Clear all data contained in the log.

3-20. Firmware Upgrade

The MS888G2 allows the administrator to upgrade the firmware to improve the features and capabilities of the switch. The firmware is upgraded via a TFTP server using any Ethernet port on the switch.

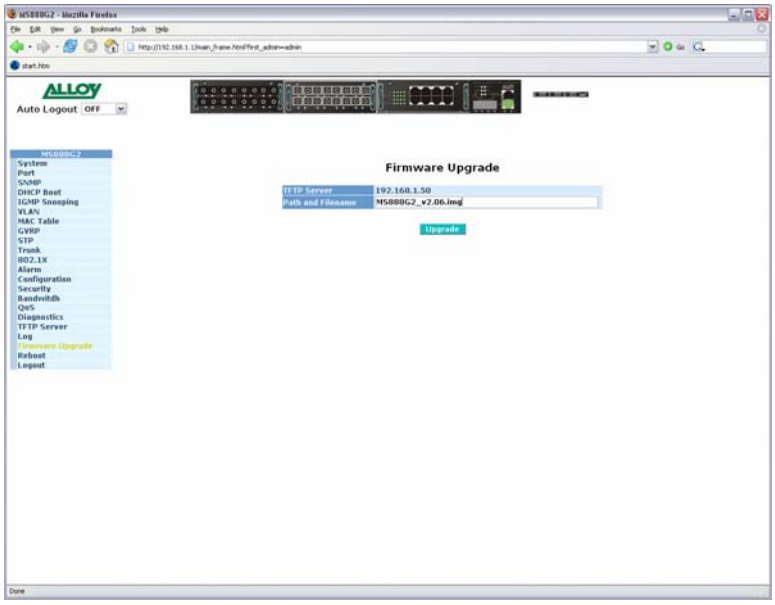

Fig. 3-74

Function name:

Firmware Upgrade

Function description:

Used to upload new firmware into the MS888G2.

Once you have set the path and filename for the firmware file, click the upgrade button to proceed. The switch will now start downloading the firmware file from the TFTP server, once it has finished downloading the file the switch will upgrade. A reboot message will then be displayed once the upgrade is complete, you must reboot the switch for the upgrade to complete.

If the switch fails to download the correct firmware image, you will return to the firmware upgrade screen.

Parameters description:

TFTP Server:

The TFTP Server used to upgrade the firmware.

Path and Filename:

Path and File Name of the firmware file.

3-21. Reboot

The MS888G2 allows the Administrator to reboot the switch from the web management you can also reboot the switch using the reset button on the front panel of the switch.

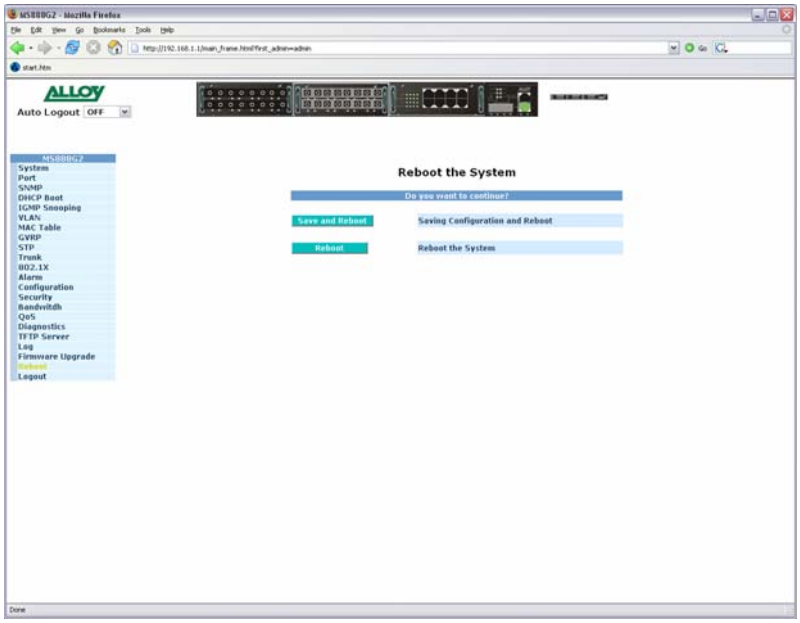

Fig. 3-75

Function name:

Reboot

Function description:

Used to reboot the switch, this can also be performed via the RESET button on the front panel of the switch. It takes about 30 seconds for the reboot to complete.

Parameters description:

Save and Reboot:

Saves the current settings as the start configuration and reboots the switch.

Reboot:

Reboots the switch.

3-22. Logout

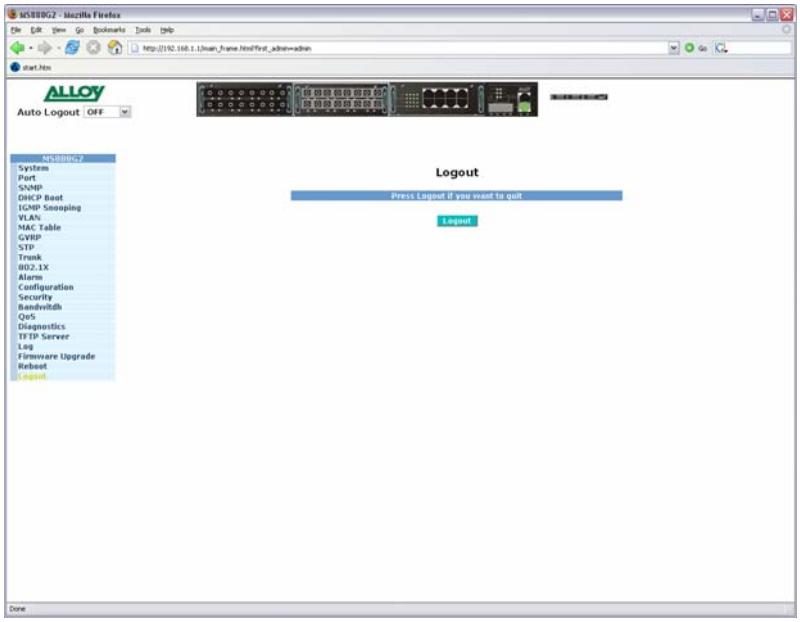

Fig. 3-76

Function name:

Logout

Function description:

Used to logout of the web management interface.

Parameters description:

Logout:

Click the Logout button to log out of the management interface.

Auto Logout:

The Web management interface allows the user to be automatically logged out after a predetermined period of the time.

Default: 3 minutes

4. Operation of CLI Management

4-1. CLI Management

Refer to chapter 2 for basic installation.

When configuring the MS888G2 via the RS-232 console please connect the switch via the provided serial cable to a DCE device such as a PC. Once you have connection run a terminal emulation program such as Hyper Terminal. When connecting to the switch please use the serial settings of the switch to create the connection, the default settings are below:

Baud Rate: 57600

Data Bits: 8

Parity: None

Stop Bits: 1

Flow Control: None

The same interface can also be accessed using Telnet.

The default IP Address, Subnet Mask and Gateway addresses are shown below:

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Gateway: 192.168.1.254

Open a command prompt and telnet to the default IP address shown above.

4-1-1. Login

The command line interface (CLI) is a text based interface, users can access the CLI through either a direct serial connection to the device or a Telnet session. The default username and password for the device is shown below:

Username: admin

Password: admin

After you have logged in successfully the prompt will be shown as “#” meaning that you are the first to login to the switch with administrator rights. If a “$” prompt is shown it means that you have logged in as a guest and you are only allowed to view the system, no changes can be made to the switch.

Fig. 4-1

4-2. Commands of the CLI

To display the list of commands that are supported on the MS888G2 Switches CLI type “?” and press enter. All commands on the switch are divided into 2 groups Global commands and Local commands. The Global commands include “exit”, “end”, “help”, “history”, “logout”, “save start”, “save user”, “restore default” and “restore user”. For more details, please refer to Section 4-2-1.

All Local commands will be run through in Section 4-2-2.

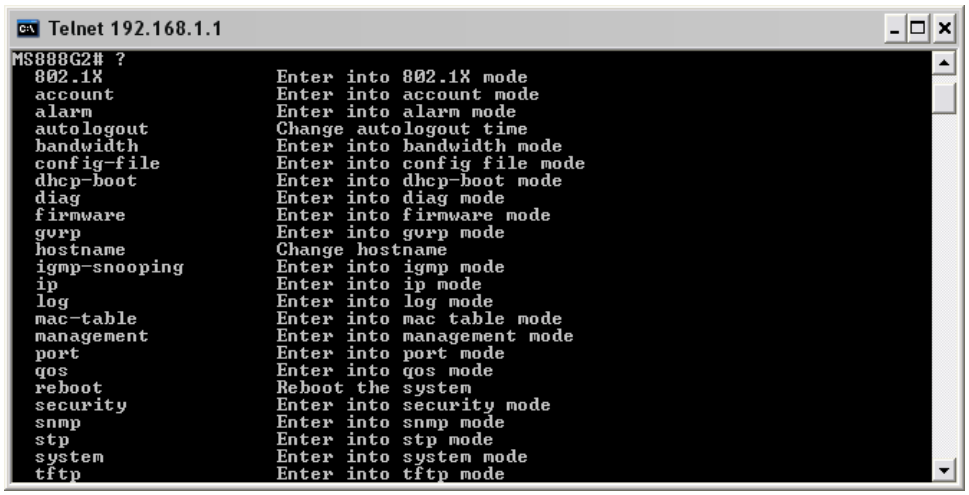

Fig. 4-2

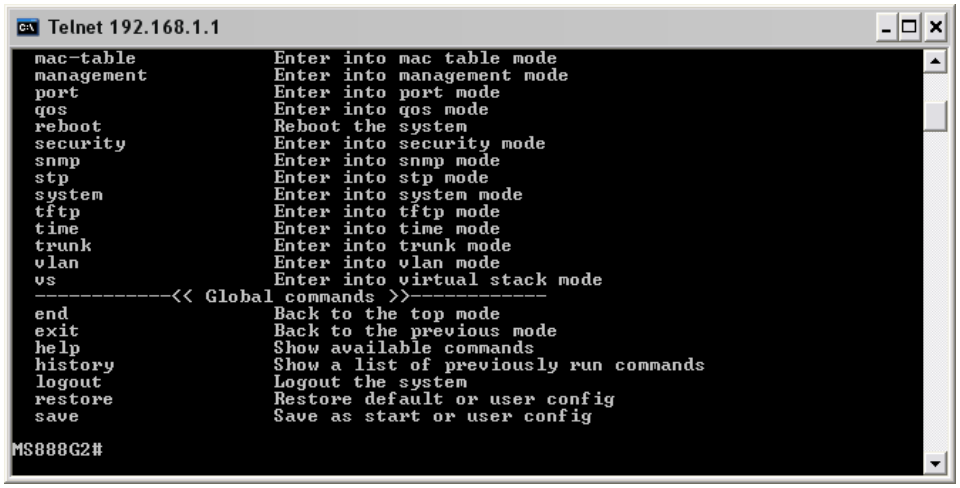

Fig. 4-3

4-2-1. Global Commands of the CLI

exit

Syntax:

exit

Description:

Back to the previous menu.

Use this command to navigate back to previous menus.

Argument:

None.

Possible value:

None.

Example:

MS888G2# trunk

MS888G2 (trunk)# exit

MS888G2#

end

Syntax:

end

Description:

Back to the root menu.

Use this command to return to the root menu. Unlike the exit command which will take you back to the previous menu, the end command will take you directly to the root menu.

Argument:

None.

Possible value:

None.

Example:

MS888G2# alarm

MS888G2(alarm)# events

MS888G2(alarm-events)# end

MS888G2#

help

Syntax:

help

Description:

Displays available commands in the current menu.

To display the available commands in any given menu enter the appropriate menu and type help. This will display all available commands for that menu.

Argument:

None.

Possible value:

None.

Example:

MS888G2# ip

MS888G2(ip)# help

Commands available:

```
 ------------<< Local commands >>------------
 set ip              Set ip, subnet mask and gateway
 set dns             Set dns
 enable dhcp         Enable DHCP, and set dns auto or manual
 disable dhcp        Disable DHCP
 show                Show IP Configuration
 ------------<< Global commands >>------------
 exit                Back to the previous mode
 end                 Back to the top mode
 help                Show available commands
 history             Show a list of previously run commands
 logout              Logout of the system
 save start          Save as start config
 save user           Save as user config
 restore default     Restore default config
 restore user        Restore user config
```

MS888G2(ip)#

history

Syntax:

history [#]

Description:

Shows you a list of commands that have previously been entered.

When you enter this command, the CLI will show a list of commands which you have entered before. The CLI supports up to 256 records. If no argument is typed, the CLI will list all records up to 256. If an optional argument is given, the CLI will only show the last number of records given by the argument.

Argument:

[#]: show last number of history records. (optional)

Possible value:

[#]: 1, 2, 3, …., 256

Example:

MS888G2(ip)# history

Command history:

0. trunk
1. exit
2. MS888G2# trunk
3. MS888G2(trunk)# exit
4. MS888G2#
5. ?
6. trunk
7. exit
8. alarm
9. events
10. end
11. ip
12. help
13. ip
14. history

MS888G2(ip)# history 3

Command history:

13. ip
14. history
15. history 3

logout

Syntax:

logout

Description:

When you enter this command via a Telnet connection, you will be automatically logged out of the system and disconnected. If you connect to the system via a direct serial port, you will be logged out of the system and the login prompt will be displayed.

Argument:

None.

Possible value:

None.

Example:

None.

save start

Syntax:

save start

Description:

To save the current configuration as the startup configuration.

When you enter this command, the CLI will save your current configuration into the non-volatile FLASH as the start up configuration.

Argument:

None.

Possible value:

None.

Example:

MS888G2# save start

Saving start...

Save Successfully

MS888G2#

save user

Syntax:

save user

Description:

To save the current configuration as the user-defined configuration.

When you enter this command, the CLI will save your current configuration into the non-volatile FLASH as the user-defined configuration.

Argument:

None.

Possible value:

None.

Example:

MS888G2# save user

Saving user...

Save Successfully

MS888G2#

restore default

Syntax:

restore default

Description:

To restore the startup configuration back to the original factory default configuration.

If the switch has been correctly restored back to default you will be prompted immediately to reboot the switch. If you press “Y” or “y” the switch will be rebooted and loaded with the default configuration. If you select “N” or “n” you will return to the previous screen.

Argument:

None.

Possible value:

None.

Example:

MS888G2# restore default

Restoring ...

Restore Default Configuration Successfully

Press any key to reboot system.

restore user

Syntax:

restore user

Description:

To restore the startup configuration as the user defined configuration.

If the switch has been correctly restored back to the user defined configuration you will be prompted immediately to reboot the switch. If you press “Y” or “y” the switch will be rebooted and loaded with the user defined configuration. If you select “N” or “n” you will return to the previous screen.

Argument:

None

Possible value:

None

Example:

MS888G2# restore user

Restoring ...

Restore User Configuration Successfully

Press any key to reboot system.

4-2-2. Local Commands of CLI

■ **system**

show

Syntax:

show

Description:

Display's the basic information of the switch.

Argument:

None

Possible value:

None

Example:

MS888G2(system)# show

Model Name	: MS888G2
System Description	: 24 Port Modular Fast Ethernet Switch
Location	:
Contact	:
Device Name	: MS888G2
System Up Time	: 0 Days 1 Hours 19 Mins 17 Secs
Current Time	: Fri Apr 27 01:26:11 2006
BIOS Version	: v1.05
Firmware Version	: v2.06
Hardware-Mechanical Version	: v1.01-v1.01
Series Number	: 123456789012
Host IP Address	: 192.168.1.1
Host MAC Address	: 00-00-8C-02-10-51
Device Port	: UART * 1, TP * 8, Fibre*16, Combo* 2
RAM Size	: 16 M
Flash Size	: 2 M

set location

Syntax:

set location <location string>

Description:

Enter a descriptive location for the MS888G2.

Argument:

String length up to 32 characters.

Possible values:

a, b, c, d, ... ,z and 1, 2, 3, …. etc.

Example:

MS888G2(system)# set location Canberra

set contact

Syntax:

set contact <contact string>

Description:

Enter the contact name responsible for the switch.

Argument:

String length up to 32 characters.

Possible value:

a, b, c, d, ... ,z and 1, 2, 3, …. etc.

Example:

MS888G2(system)# set contact Administrator

set device-name

Syntax:

set device-name <string>

Description:

Enter a descriptive name for the switch.

Argument:

String length up to 32 characters.

Possible value:

a, b, c, d, ... ,z and 1, 2, 3, …. etc.

Example:

MS888G2(system)# set device-name MS888G2

■ **IP**

set ip

Syntax:

set ip <ip> <mask> <gateway>

Description:

To set the system IP address, subnet mask and gateway.

Argument:

<ip> : ip address

<mask> : Subnet Mask

<gateway> : Default Gateway

Possible value:

<ip> : 192.168.1.2 or other.

<mask> : 255.255.255.0 or other.

<gateway> : 192.168.1.253 or other.

Example:

MS888G2(ip)# set ip 192.168.1.2 255.255.255.0 192.168.1.253

: Sets the IP address of the switch to 192.168.1.2, subnet mask to 255.255.255.0 and the default gateway to 192.168.1.253

set dns

Syntax:

set dns <ip address>

Description:

To set the IP address of a DNS server.

Argument:

<ip address> : dns ip address

Possible value:

168.95.1.1

Example:

MS888G2(ip)# set dns 168.95.1.1

: Sets the MS888G2 switches DNS Server address to 168.95.1.1

enable dhcp

Syntax:

enable dhcp <manual or auto>

Description:

To enable the DHCP function and assign a DNS Server address manually or automatically.

Argument:

<manual or auto> : enable DHCP and assign DNS address using manual or auto mode.

Possible value:

Manual or auto

Example:

MS888G2(ip)# enable dhcp manual

: Enables DHCP function and sets DNS server via manual mode.

disable dhcp

Syntax:

disable dhcp

Description:

Disables the DHCP function in the Switch.

Argument:

None

Possible value:

None

Example:

MS888G2(ip)# disable dhcp

: Disables the DHCP function.

show

Syntax:

show

Description:

To display the system's DHCP function state, IP address, subnet mask, default gateway, DNS mode, DNS server IP address and current IP address.

Argument:

None

Possible value:

None

Example:

MS888G2(ip)# show

DHCP : Disable
IP Address : 192.168.2.65
Subnet mask : 255.255.255.0
Gateway : 192.168.2.252
DNS Setting : Manual
DNS Server : 168.95.1.1
Current IP : 192.168.2.65

■ **time**

set manual

Syntax:

set manual <YYYY/MM/DD> <hh:mm:ss>

Description:

Used to set up the current time manually.

Argument:

<YYYY/MM/DD> <hh:mm:ss>

Possible value:

YYYY	: Year	(2000-2036)
MM	: Month	(01-12)
DD	: Day	(01-31)
hh	: Hour	(00-23)
mm	: Minute	(00-59)
ss	: Second	(00-59)

Example:

MS888G2(time)# set manual 2006/02/24 16:18:00

set ntp

Syntax:

set ntp <ip> <timezone>

Description:

Used to set up the current time via a NTP server.

Argument:

ip	: ntp server ip address or domain name
timezone	: time zone (GMT), range: -12 to +13

Possible value:

Timezone: -12,-11…,0,1…,13

Example:

MS888G2(time)# set ntp 210.59.157.10 8

set daylightsaving

Syntax:

set daylightsaving <hr> <s:MM/DD/hh> <e:MM/DD/hh>

Description:

Used to configure the daylight savings start and ending dates.

Argument:

<hr> <s:MM/DD/hh> <e:MM/DD/hh>

Possible value:

hr : daylight saving hour, range: -5 to +5

s: : daylight saving start month/day/hour

e: : daylight saving end month/day/hour

MM : Month (01-12)

DD : Day (01-31)

hh : Hour (00-23)

Example:

MS888G2(time)# set daylightsaving 3 10/12/01 11/12/01

Save Successfully

show

Syntax:

show

Description:

To show the time configuration, including “Current Time”, “NTP Server”,” Timezone”, ” Daylight Saving”,” Daylight Saving Start” and “Daylight Saving End”

Argument:

None.

Possible value:

None.

Example:

MS888G2(time)# show

Current Time : Fri Feb 24 15:04:03 2006

NTP Server : 209.81.9.7

Timezone : GMT+10:00

Day light Saving : 0 Hours

Day light Saving Start : Mth: 1 Day: 1 Hour: 0

Day light Saving End : Mth: 1 Day: 1 Hour: 0

■ **account**

add

Syntax:

add guest <name>

Description:

To create a new guest user.

When you create a new guest user, you must type in a password and then confirm the password.

Argument:

<name> : new account name

Possible value:

A string must be at least 5 characters.

Example:

MS888G2(account)# add Freddy

Password:

Confirm Password:

Save Successfully

del

Syntax:

del <name>

Description:

Used to delete an existing account.

Argument:

<name> : existing user account

Possible value:

None.

Example:

MS888G2(account)# del Freddy

Account Freddy deleted

modify

Syntax:

modify <name>

Description:

Used to change the username and password of an existing account.

Argument:

<name> : existing user account

Possible value:

None.

Example:

MS888G2(account)# modify Freddy

username/password: the length is from 5 to 15 characters.

Current username (Freddy):Freddy2

New password:

Confirm password:

Username changed successfully.

Password changed successfully.

show

Syntax:

show

Description:

Displays the current users configured in the switch.

Argument:

None.

Possible value:

None.

Example:

MS888G2(account)# show

Account Name Identity

--- ---

admin : Administrator

guest : guest

■ **port**

set speed-duplex

Syntax:

set speed-duplex <range> <auto|10half|10full|100half|100full|1Gfull>

Description:

Used to configure the speed and duplex settings of each port.

Argument:

<range>:syntax 1,5-7, available from 1 to 24

<port-speed>:

auto: set auto-negotiation mode

10half: set speed/duplex 10M Half

10full: set speed/duplex 10M Full

100half: set speed/duplex 100M Half

100full: set speed/duplex 100M Full

1Gfull: set speed/duplex 1G Full.

Possible value:

<range>: 1 to 24

<port-speed>: auto, 10half, 10full, 100half, 100full, 1Gfull

Example:

MS888G2(port)# set speed-duplex 5 auto

: Sets port 5 to auto negotiation mode.

show status

Syntax:

show status

Description:

Used to display the port's current status.

Argument:

None

Possible value:

None

Example:

MS888G2(port)# show status

show simple-counter

Syntax:

show simple-counter

Description:

Used to display the summary of each port's traffic usage.

Argument:

None

Possible value:

None

Example:

MS888G2(port)# show simple-counter

show detail-counter

Syntax:

Show detail-counter <range>

Description:

Used to display a detailed traffic counter for each port.

Argument:

<range>:syntax 1,5-7, available from 1 to 24

Possible value:

1 to 24

Example:

MS888G2(port)# show detail-counter 5

: Displays the detailed counter for port 5

show conf

Syntax:

show conf

Description:

Used to display each port's state, speed-duplex and flow control settings.

Argument:

None

Possible value:

None

Example:

MS888G2(port)# show conf

show sfp

Syntax:

show sfp <port>

Description:

Used to display the SFP module information.

Argument:

<port>: available 25, 26

Possible value:

25, 26

Example:

MS888G2(port)# show sfp 25

: Displays the SFP module information for port 25.

clear counter

Syntax:

clear counter

Description:

Used to clear all ports' counter (include simple and detail port counter) information.

Argument:

None

Possible value:

None

Example:

MS888G2(port)# clear counter

enable state

Syntax:

enable state <range>

Description:

Used to enable the port.

Argument:

range syntax: 1,5-7, available from 1 to 24

Possible value:

<range>: 1 ~ 24

Example:

MS888G2(port)# enable state 3-12

: Enables ports 3 through to 12.

enable flow-control

Syntax:

enable flow-control <range>

Description:

Used to enable flow control on a particular port.

Argument:

range syntax: 1,5-7, available from 1 to 24

Possible value:

<range>: 1 ~ 24

Example:

MS888G2(port)# enable flow-control 3-8

: Enables flow control for ports 3 through to 8.

disable state

Syntax:

disable state <range>

Description:

Used to Disable the port.

Argument:

range syntax: 1,5-7, available from 1 to 24

Possible value:

<range>: 1 ~ 24

Example:

MS888G2(port)# disable state 12

: Disables port 12.

disable flow-control

Syntax:

disable flow-control <range>

Description:

Used to disable flow control on a particular port.

Argument:

range syntax: 1,5-7, available from 1 to 24

Possible value:

<range>: 1 ~ 24

Example:

MS888G2(port)# disable flow-control 6

: Disables flow control for port 6.

■ **mirror**

set mirror-mode

Syntax:

set mirror-mode <rx or disable>

Description:

Used to set the switches Mirror mode. (rx mode or disabled).

Argument:

<rx | disable>

rx : Enable the switch to mirror all received packets.

disable: Disables the mirror function.

Possible value:

None

Example:

MS888G2(mirror)# set mirror-mode rx

: Enables RX mirroring mode on the switch.

set monitoring-port

Syntax:

set monitoring-port <#>

Description:

Used to set up the monitoring port of the mirror function, this port will be used to capture all packets that the monitored port receives.

Argument:

<#>: the monitoring port that is chosen for the mirror function. Only one port can be the monitoring port.

Possible value:

None

Example:

MS888G2(mirror)# set monitoring-port 2

: Enables port 2 to become the monitoring port which will capture all packets received by the monitored port.

set monitored-port

Syntax:

set monitored-port <range>

Description:

Used to set up the port(s) that will be monitored, the packets received by this port(s) will be copied to the monitoring port.

Argument:

<range>: the port(s) that have been chosen for monitoring.

Possible value:

None

Example:

MS888G2(mirror)# set monitored-port 3-5,8,10

: Enables all traffic received on ports 3 through to 5, port 8 and port 10 to be copied to the monitoring port.

show

Syntax:

Show

Description:

Displays the status of the mirror function.

Argument:

None

Possible value:

None

Example:

MS888G2(mirror)# show

Mirror Mode   : rx

Monitoring Port : 2

Monitored Port : 3 4 5 7 10

■ **bandwidth**

enable ingress-rate

Syntax:

enable ingress-rate <range> <data_rate>

Description:

Used to set up the Ingress-rate of each port on the switch.

Argument:

<range>:syntax 1,5-7, available from 1 – 24

<data_rate>: 0-1000Mbps.

Possible value:

<range>: 1 to 24

<data_rate>: 0-1000Mbps.

Example:

MS888G2(bandwidth)# enable ingress-rate 1-16 100

: Enables an ingress rate of 100Mbps on all 16 ports.

enable storm-rate

Syntax:

enable storm-rate <range> <data_rate>

Description:

Used to configure the storm-rate of each port(s).

Argument:

<range>:syntax 1,5-7, available from 1 – 24

<data_rate>: 0-1000Mbps.

Possible value:

<range>: 1 to 24

<data_rate>: 0-1000Mbps.

Example:

MS888G2(bandwidth)# enable storm-rate 1-16 150

: Enables the broadcast storm rate on ports 1 through to 16 at 150.

enable egress-rate

Syntax:

enable egress-rate <range> <data_rate>

Description:

Used to set up the Egress-rate of each port on the switch.

Argument:

<range>:syntax 1, 5-7, available from 1 – 24

<data_rate>: 0-1000Mbps.

Possible value:

<range>: 1 to 24

<data_rate>: 0-1000Mbps.

Example:

MS888G2(bandwidth)# enable egress-rate 1-24 20.

: Enables an Egress rate of 20Mbps on all 24 ports.

disable ingress-rate

Syntax:

disable ingress-rate <range>

Description:

Used to disable the Ingress-rate of the port.

Argument:

<range>:syntax 1,5-7, available from 1 – 24

Possible value:

<range>: 1 to 24

Example:

MS888G2(bandwidth)# disable ingress-rate 1-24

: Disables the Ingress rate control for all ports from 1 through to 24.

d*isable storm-rate*

Syntax:

disable ingress-rate <range>

Description:

Used to disable the storm-rate of the port.

Argument:

<range>:syntax 1,5-7, available from 1 – 24

Possible value:

<range>: 1 to 24

Example:

MS888G2(bandwidth)# disable storm-rate 1-24

: Disables the storm rate control for all ports from 1 through to 24.

d*isable egress-rate*

Syntax:

disable egress-rate <range>

Description:

Used to disable the egress-rate of the port.

Argument:

<range>:syntax 1,5-7, available from 1 – 24

Possible value:

<range>: 1 to 24

Example:

MS888G2(bandwidth)# disable egress-rate 1-24

Disable the egress rate control on all port from 1 through to 24.

show

Syntax:

show

Description:

Used to display all current settings of the bandwidth rate control.

Argument:

None

Possible value:

None

Example:

MS888G2(bandwidth)# show

	All State	All Rate	Storm State	Storm Rate	All state	All Rate
1	Disabled	0	Disabled	0	Disabled	0
2	Disabled	0	Disabled	0	Disabled	0
3	Disabled	0	Disabled	0	Disabled	0
4	Disabled	0	Disabled	0	Disabled	0
5	Disabled	0	Disabled	0	Disabled	0
6	Disabled	0	Disabled	0	Disabled	0
7	Disabled	0	Disabled	0	Disabled	0
8	Disabled	0	Disabled	0	Disabled	0
9	Disabled	0	Disabled	0	Disabled	0
10	Disabled	0	Disabled	0	Disabled	0
11	Disabled	0	Disabled	0	Disabled	0
12	Disabled	0	Disabled	0	Disabled	0
13	Disabled	0	Disabled	0	Disabled	0
14	Disabled	0	Disabled	0	Disabled	0
15	Disabled	0	Disabled	0	Disabled	0
16	Disabled	0	Disabled	0	Disabled	0
17	Disabled	0	Disabled	0	Disabled	0
18	Disabled	0	Disabled	0	Disabled	0
19	Disabled	0	Disabled	0	Disabled	0
20	Disabled	0	Disabled	0	Disabled	0
21	Disabled	0	Disabled	0	Disabled	0

22	Disabled	0	Disabled	0	Disabled	0
23	Disabled	0	Disabled	0	Disabled	0
24	Disabled	0	Disabled	0	Disabled	0
25	Disabled	0	Disabled	0	Disabled	0
26	Disabled	0	Disabled	0	Disabled	0

■ **QoS**

set mode

Syntax:

set mode <port/pri_tag/tos/layer4/diffserv>

Description:

To set the QoS priority mode of the switch

Argument:

port: per port priority

pri_tag: vlan tag priority

tos: ip tos classification

layer4: ip tcp/udp port classification

diffserv: ip diffserv classification

Possible value:

port/pri_tag/tos/layer4/diffserv

Example:

MS888G2(qos)# set mode port

: Sets the QoS mode of the switch to per port priority.

set default

Syntax:

set default <class>

Description:

Used to set a priority class on all packets that won't be affected by QoS.

Argument:

class: class of service

Possible value:

setting. 1: high, 0: low

Example:

MS888G2(qos)# set default 1

: Sets a high priority to all ports not using the QoS function.

set port

Syntax:

set port <range> <class>

Description:

Used to set a High or Low priority class to all ports being used by port-based QoS.

Argument:

<range> : port range

<class> : class of service setting.

Possible value:

<range>: syntax: 1,5-7, available from 1 to 26

<class>: 1: high, 0: low

Example:

MS888G2(qos)# set port 1-10 1

: Sets a high priority on all port from 1 through to 10.

set pri-tag

Syntax:

set pri_tag <port-range> <tag-range> <class>

Description:

Used to set a priority level based on vlan tag QoS.

Argument:

<port-range>: port range

<tag-range>: tag priority level

<class>: class of service

Possible value:

<port-range>: syntax: 1,5-7, available from 1 to 26

<tag-range>: priority level, syntax: 1,5-7, available from 0 to 7

<class>: class of service setting. 1: high, 0: low

Example:

MS888G2(qos)# set pri-tag 1-10 1-2 1

: Sets a high priority level to all packets containing a VLAN tag of 1 or 2 to all ports from 1 through to 10.

set tos

Syntax:

set tos <port-range> <tos-range> <class>

Description:

Used to set a priority level to ports based on the TOS field of an IP packet.

Argument:

<port-range>: port range

<tos-range>: tos precedence field

<class>: class of service

Possible value:

<port-range>: syntax: 1,5-7, available from 1 to 26

<tos-range>: syntax: 1,5-7, available from 0 to 7

<class>: 1: high, 0: low

Example:

MS888G2(qos)# set tos 1-5 0-3 0

: Sets a low priority to all packets containing a TOS filed ranging from 0 through to 3 for all ports from 1 through to 5.

set diffserv

Syntax:

set diffserv <ds-range> <class>

Description:

Used to prioritse data based on IP DiffServe qos.

Argument:

<ds-range>: dscp field

<class>: class of service

Possible value:

<ds-range>: syntax: 1,5-7, available from 0 to 63

<class>: 1: high, 0: low

Example:

MS888G2(qos)# set diffserv 0-20 1

:Sets all classes of traffic with a diffserv value from 1 through to 20 with a high priority.

show

Syntax:

show

Description:

Display's the information of the mode that you have chosen.

Argument:

None

Possible value:

None

Example:

MS888G2(qos)# show

IP Diffserv Classification

Default Class:high

DiffServ	Class	DiffServ	Class	DiffServ	Class	DiffServ	Class
0	high	1	high	2	high	3	high
4	high	5	high	6	high	7	high
8	high	9	high	10	high	11	high
12	high	13	high	14	high	15	high
16	high	17	high	18	high	19	high
20	high	21	high	22	high	23	high
24	high	25	high	26	high	27	high
28	high	29	high	30	high	31	high
32	high	33	high	34	high	35	high
36	high	37	high	38	high	39	high
40	high	41	high	42	high	43	high
44	high	45	high	46	high	47	high
48	high	49	high	50	high	51	high
52	high	53	high	54	high	55	high
56	high	57	high	58	high	59	high
60	high	61	high	62	high	63	high

■ **snmp**

enable

Syntax:

enable snmp

enable set-ability

Description:

Used to enable the SNMP function and configure your community names.

Argument:

None.

Possible value:

None.

Example:

MS888G2(snmp)# enable snmp

: Enables the SNMP function in the switch.

MS888G2(snmp)# enable set-ability

: Enables the private community of the SNMP function.

disable

Syntax:

disable snmp

disable set-ability

Description:

Used to disable the SNMP function.

Argument:

None.

Possible value:

None.

Example:

MS888G2(snmp)# disable snmp

: Disables the SNMP function in the switch.

MS888G2(snmp)# disable set-ability

: Disables the private community of the SNMP function.

set

Syntax:

set get-community <community>

set set-community <community>

set trap <#> <ip> [port] [community]

Description:

Set is used to configure the setup of the get-community, set-community, trap host ip, host port and trap-community.

Argument:

<#>: trap number

<ip>: ip address or domain name

<port>: trap port

<community>:trap community name

Possible value:

trap number: 1 to 6

port:1~65535

Example:

MS888G2(snmp)# set get-community public

: Sets the get-community name to public.

MS888G2(snmp)# set set-community private

: Sets the set-community name to private.

MS888G2(snmp)# set trap 1 192.168.1.1 162 public

: Sets trap 1 host IP address of 192.168.1.1 using port number 162. The community name is set to public. Any SNMP traps will be sent to the IP address specified above.

show

Syntax:

show

Description:

Displays the configuration of the SNMP function.

Argument:

None.

Possible value:

None.

Example:

MS888G2(snmp)# show

SNMP: Enable

Get Community: public

Set Community: private [Enable]

Trap Host 1 IP Address: 192.168.1.1 Port: 162 Community: public

Trap Host 2 IP Address: 0.0.0.0 Port: 162 Community: public

Trap Host 3 IP Address: 0.0.0.0 Port: 162 Community: public

Trap Host 4 IP Address: 0.0.0.0 Port: 162 Community: public

Trap Host 5 IP Address: 0.0.0.0 Port: 162 Community: public

Trap Host 6 IP Address: 0.0.0.0 Port: 162 Community: public

■ **igmp**

set igmp_snooping

Syntax:

set igmp_snooping <status>

Description:

Used to set the IGMP Snooping mode.

Argument:

<status> 0:disable , 1:active , 2:passive

Possible value:

<status> 0,1,2

Example:

MS888G2(igmp)# set igmp-snooping 2

: Sets the IGMP Snooping mode to passive mode.

show

Syntax:

show

Description:

Display's the IGMP snooping mode and IP Multicast Table.

Argument:

None

Possible value:

None

Example:

MS888G2(igmp)# show

Snoop Mode: Active

IP Multicast:

1) IP Address : 224.1.1.1
   VLAN ID : 0
   Member Port : 22

■ **dhcp-boot**

set dhcp-boot

Syntax:

set dhcp-boot <sec>

Description:

Used to set the delay time for DHCP Broadcast Suppression.

Argument:

<sec>:range syntax: 0, 1-30. The value “0” will disable the dhcp-boot delay.

Possible value:

<sec>:0-30

Example:

MS888G2(dhcp-boot)# set dhcp-boot 30

: Sets the DHCP Broadcast Suppression delay time to 30 seconds.

show

Syntax:

show

Description:

Display’s the status of DHCP Broadcast Suppression.

Argument:

None

Possible value:

None

Example:

MS888G2(dhcp-boot)# show

Dhcp Boot : Enable

Second : 10

■ **vlan**

set mode

Syntax:

set mode <disable | port | tag>

Description:

Used to configure the VLAN mode of the switch, including disable, port-based and tag-based

Argument:

disable: vlan disable

tag: set tag-based vlan

port: set port-based vlan

double-tag: enable Q-in-Q function

Possible value:

<disable | port | tag>: disable, port, tag

Example:

MS888G2(vlan)# set mode port

: Sets the VLAN mode for the switch to port-based mode

set tag-group

Syntax:

set tag-group <vid> <name> <range> <#>

Description:

Used to create or edit a tag-based vlan group.

Argument:

vid: vlan ID

name: vlan name

range: vlan group members, syntax: 1,5-7

Possible value:

vid: range from 1 to 4094

name: tag-vlan name

range: from 1 to 26

Example:

MS888G2(vlan)# set tag-group 2 VLAN-2 2-5, 6 0

: Creates a Tag-based VLAN group with a VID of 2, and a group name of VLAN-2. The ports that will belong to this group are 2 to 5 and 6, sym vlan set to symmetric.

set port-group

Syntax:

set port-group <name> <range>

Description:

Used to create or edit a port-based VLAN group.

Argument:

name: vlan name

range: vlan group members, syntax: 1,5-7

Possible value:

name: port-vlan name

range: available from 1 to 26

Example:

MS888G2(vlan)# set port-group VLAN-1 2-5,6,10,12

: Creates a port-based VLAN group with a group name of VLAN-1 and member ports consisting of ports 2 through to 5, 6, 10 and 12.

set pvid

Syntax:

set pvid <range> <pvid>

Description:

Used to set the vlan pvid for use when using tag-based VLAN's.

Argument:

Range: which port(s) you want to set PVID(s).
syntax: 1,5-7

pvid: which PVID(s) you want to set.

Possible value:

Range: available from 1 to 26

pvid: available from 1 to 4094

Example:

MS888G2(vlan)# set pvid 3,5,6-8 5

: Sets ports 3, 4, 5, 6, 7, 8 with a PVID of 5.

enable sym-vlan <range>

Syntax:

enable sym-vlan <range>

Description:

Used to drop frames with a particular VID that do not belong to the same VLAN group.

Argument:

range: what port(s) you want to configure. Syntax: 1,5-7

Possible value:

range: available from 1 to 26

Example:

MS888G2(vlan)# enable sym-vlan 5-10

: Enables sym-vlan on all ports ranging from 5 through to 10.

disable sym-vlan

Syntax:

disable sym-vlan <range>

Description:

Used to drop frames from the non-member ports.

Argument:

range : which port(s) you want to configure.

Possible value:

range: available from 1 to 26

Example:

MS888G2(vlan)# disable sym-vlan 5-10

: Disables sym-vlan on all ports ranging from 5 through to 10.

enable drop-untag

Syntax:

enable drop-untag <range>

Description:

Used to create a rule so that all untagged frames received on this port will be dropped.

Argument:

range: which port(s) you want to configure. Syntax: 1,5-7

Possible value:

range: available from 1 to 26

Example:

MS888G2(vlan)# enable drop-untag 5-10

: Creates a rule to drop all untagged frames received on ports 5 through to 10.

disable drop-untag

Syntax:

disable drop-untag <range>

Description:

Used to create a rule so that all untagged frames received on this port will not be dropped.

Argument:

range : which port(s) you want to configure. Syntax: 1,5-7

Possible value:

range: available from 1 to 26

Example:

MS888G2(vlan)# disable drop-untag 5-10

: Creates a rule so that all untagged frames received on ports 5 through to 10 will not be dropped.

del tag-group <vid>

Syntax:

del tag-group <vid>

Description:

Used to delete an existing tag-based vlan group.

Argument:

vid: which vlan group you want to delete.

Possible value:

vid: available from 1 to 4094

Example:

MS888G2(vlan)# del tag-group 2

:Deletes VLAN group 2.

del port-group <name>

Syntax:

del port-group <name>

Description:

Used to delete the port-based vlan group.

Argument:

name: which vlan group you want to delete.

Possible value:

name: port-vlan name

Example:

MS888G2(vlan)# del port-group VLAN-2

: Deletes port-based VLAN group VLAN-2

show group

Syntax:

show group

Description:

Used to display the vlan mode and vlan group(s).

Argument:

None

Possible value:

None

Example:

MS888G2(vlan)# show group

Vlan mode is double-tag.

1) Vlan Name : default
   Vlan ID : 1
   Sym-vlan : Disable
   Member : 1 2 3 4 5 6 7 8 9 10 11 12

2) Vlan Name : VLAN-2
   Vlan ID : 2
   Sym-vlan : Disable
   Member : 2 3 4 5 6

show pvid

Syntax:

show pvid

Description:

Used to display the pvid and the ingress/egress rule(s).

Argument:

None

Possible value:

None

Example:

MS888G2(vlan)# show pvid

Port	PVID	Rule1	Rule2	Port Rule	Untag Vid
1	1	Disable	Disable	Access	-
2	1	Disable	Disable	Access	-
3	5	Disable	Disable	Access	-
4	1	Disable	Disable	Access	-
5	5	Enable	Disable	Hybrid	6
6	5	Enable	Disable	Access	-
7	5	Enable	Disable	Access	-
8	5	Enable	Disable	Access	-
9	1	Enable	Disable	Access	-
10	1	Enable	Disable	Access	-
11	1	Disable	Disable	Access	-
12	1	Disable	Disable	Access	-
13	1	Disable	Disable	Access	-
14	1	Disable	Disable	Access	-
15	1	Disable	Disable	Access	-
16	1	Disable	Disable	Access	-
17	1	Disable	Disable	Access	-
18	1	Disable	Disable	Access	-
19	1	Disable	Disable	Access	-
20	1	Disable	Disable	Access	-
21	1	Disable	Disable	Access	-
22	1	Disable	Disable	Access	-

23	1	Disable	Disable	Access	-
24	1	Disable	Disable	Access	-
25	1	Disable	Disable	Access	-
26	1	Disable	Disable	Access	-

■ **mac-table**

<<information>>

show

Syntax:

Show

Description:

Used to display all MAC table information.

Argument:

None

Possible value:

None

Example:

MS888G2(mac-table-information)# show

MAC Table List

Alias	MAC Address	Port	VID	State

search

Syntax:

search <port> <mac> <vid>

Description:

Used to search the MAC table for specific MAC information.

Argument:

<port> : set up the range of the ports to search for,
syntax: 1,5-7, available from 1 to 24

<mac> : mac address, format: 01-02-03-04-05-06, '?' can be used

<vid> : vid: vlan id, from 1 to 4094; '?' as don't care, 0 as untagged

Possible value:

None

Example:

MS888G2(mac-table-information)# search 1-16 ??-??-??-??-??-?? ?

MAC Table List

Alias	MAC Address	Port	VID	State
	00-00-8C-88-00-06	1	0	Dynamic

: Searches ports 1 through to 16 for any MAC address with an VID.

<<maintain>>

set aging

Syntax:

set aging <#>

Description:

Used to set up the age out time value of MAC addresses learnt dynamically.

Argument:

<#> : age-timer in seconds, 0, 10 to 65535. The value zero disables aging

Possible value:

None

Example:

MS888G2(mac-table-maintain)# set aging 300

: Sets the MAC aging time to 300 seconds

set flush

Syntax:

set flush

Description:

Used to delete all of the MAC's that have been learnt dynamically.

Argument:

None

Possible value:

None

Example:

MS888G2(mac-table-maintain)# set flush

: Flushes all learnt dynamic MAC addresses from the MAC table.

show

Syntax:

show

Description:

Used to display the settings of age-timer.

Argument:

None

Possible value:

None

Example:

MS888G2(mac-table-maintain)# show

age-timer : 300 seconds

<<static-mac>>

add

Syntax:

add <mac> <port> <vid> [alias]

Description:

Used to add a static MAC entry into the switches MAC table.

Argument:

<mac> : mac address, format: 00-02-03-04-05-06

<port> : 0-26

<vid> : vlan id. 0, 1-4094. vid must be zero if vlan mode is not tag-based

[alias] : mac alias name, max 15 characters

Possible value:

None

Example:

MS888G2(mac-table-static-mac)# add 00-02-03-04-05-06 3 0 Test

: Adds a static MAC entry with MAC address 00-02-03-04-05-06 fro port 3 with a VID of 0 and a Alias name of Test.

del

Syntax:

del <mac> <vid>

Description:

Used to remove a selected static MAC address entry.

Argument:

<mac>: mac address, format: 00-02-03-04-05-06

<vid>: vlan id. 0, 1-4094. vid must be zero if vlan mode is not tag-based

Possible value:

None

Example:

MS888G2(mac-table-static-mac)# del 00-02-03-04-05-06 0

: Removes the static MAC entry of 00-02-03-04-05-06 with a VID of 0.

show forward

Syntax:

show forward

Description:

Used to display the static forward table.

Argument:

None

Possible value:

None

Example:

MS888G2(mac-table-static-mac)# show forward

Static Forwarding Entry: (Total 1 item(s))

1) MAC: 00-02-03-04-05-06, port: 3, vid: -, alias: aaa

show filter

Syntax:

show filter

Description:

Used to display the static MAC filter table.

Argument:

None

Possible value:

None

Example:

MS888G2(mac-table-static-mac)# show filter

Static Filtering Entry: (Total 1 item(s))

1) mac: 00-33-03-04-05-06, vid: -, alias: ccc

<<alias>>

set

Syntax:

set <mac> <alias>

Description:

Used to configure a MAC alias entry.

Argument:

<mac> : mac address, format: 00-02-03-04-05-06

<alias> : mac alias name, max 15 characters

Possible value:

None

Example:

MS888G2(mac-table-alias)# set 00-44-33-44-55-44 Test

: Create a MAC Alias of Test for MAC address 00-02-03-04-05-06

del

Syntax:

del <mac>

Description:

Used to delete a MAC alias entry.

Argument:

<mac> : mac address, format: 00-02-03-04-05-06

Possible value:

None

Example:

MS888G2(mac-table-alias)# del 00-44-33-44-55-44

: Deletes the MAC Alias name for MAC address 00-02-03-04-05-06.

show

Syntax:

show

Description:

Used to display the MAC alias entries.

Argument:

None

Possible value:

None

Example:

MS888G2(mac-table-alias)# show

MAC Alias List

	MAC Address	Alias
1)	00-02-03-04-05-06	Test
2)	00-33-03-04-05-06	Test1
3)	00-44-33-44-55-66	Test2

■ **gvrp**

enable

Syntax:

enable

Description:

Used to enable the GVRP function.

Argument:

None

Possible value:

None

Example:

MS888G2(gvrp)# enable

: Enables GVRP on the switch.

disable

Syntax:

disable

Description:

Used to disable the GVRP function.

Argument:

None

Possible value:

None

Example:

MS888G2(gvrp)# disable

: Disables GVRP on the switch.

set timer

Syntax:

set timer <range> <join> <leave> <leaveall>

Description:

Used to set GVRP join time, leave time, and leaveall time for each port.

Argument:

<range> : port range

<join>: join timer

<leave>: leave timer

<leaveall>: leaveall timer

Possible value:

<range> : syntax 1,5-7, available from 1 to 26

<join>: available from 20 to 100 seconds

<leave>: available from 60 to 300 seconds

<leaveall>: available from 1000 to 5000 seconds

Leave Time must equal at least double the Join Time.

Example:

MS888G2(gvrp)# set timer 2-8 25 80 2000

: Sets the GVRP timer for ports 2 through to 8 with a join time of 25, a leave time of 80 and a leave all time of 2000.

set applicant

Syntax:

set applicant <range> <normal | non-participant>

Description:

Used to set default applicant mode for each port.

Argument:

range: port range

normal: set applicant as normal mode

non-participant: set applicant as non-participant mode

Possible value:

<range>: syntax 1,5-7, available from 1 to 26

<normal | non-participant>: normal or non-participant

Example:

MS888G2(gvrp)# set applicant 1-10 non-participant

: Sets ports 1 through to 10 as non-participant mode.

set registrar

Syntax:

set registrar <range> <normal | fixed | forbidden>

Description:

Used to set default registrar mode for each port.

Argument:

range: port range

normal: set registrar as normal mode

fixed: set registrar as fixed mode

forbidden: set registrar as forbidden mode

Possible value:

<range>: syntax 1,5-7, available from 1 to 26

<normal | fixed | forbidden>: normal, fixed or forbidden

Example:

MS888G2(gvrp)# set registrar 1-5 fixed

: Sets ports 1 through to 5 as fixed mode.

show counter

Syntax:

show counter

Description:

Usage: show counter <port>

Argument:

<port>: port number

Possible value:

<port>: available from 1 to 24

Example:

MS888G2(gvrp)# show counter 2

GVRP Counter port: 2

Counter Name	Received	Transmitted
Total GVRP Packets	0	0
Invalid GVRP Packets	0	----
LeaveAll message	0	0
JoinEmpty message	0	0
JoinIn message	0	0
LeaveEmpty message	0	0
Empty message	0	0

show config

Syntax:

show config

Description:

Used to display the GVRP configuration.

Argument:

none

Possible value:

none

Example:

MS888G2(gvrp)# show config

GVRP state: Enable

Port	Join Time	Leave Time	LeaveAll Time	Applicant	Registrar	Restricted
1	20	60	1000	Normal	Normal	Disable
2	25	80	2000	Normal	Normal	Disable
3	25	80	2000	Normal	Normal	Disable
4	25	80	2000	Normal	Normal	Disable
5	25	80	2000	Normal	Normal	Disable
6	25	80	2000	Normal	Normal	Disable
7	25	80	2000	Normal	Normal	Disable
8	25	80	2000	Normal	Normal	Disable
9	20	60	1000	Normal	Normal	Disable
10	20	60	1000	Normal	Normal	Disable
11	20	60	1000	Normal	Normal	Disable
12	20	60	1000	Normal	Normal	Disable
13	20	60	1000	Normal	Normal	Disable
14	20	60	1000	Normal	Normal	Disable
15	20	60	1000	Normal	Normal	Disable
16	20	60	1000	Normal	Normal	Disable
17	20	60	1000	Normal	Normal	Disable
18	20	60	1000	Normal	Normal	Disable
19	20	60	1000	Normal	Normal	Disable
20	20	60	1000	Normal	Normal	Disable

21	20	60	1000	Normal	Normal	Disable
22	20	60	1000	Normal	Normal	Disable
23	20	60	1000	Normal	Normal	Disable
24	20	60	1000	Normal	Normal	Disable
25	20	60	1000	Normal	Normal	Disable
26	20	60	1000	Normal	Normal	Disable

show group

Syntax:

show group

Description:

Used to show the GVRP group(s).

Argument:

none

Possible value:

none

Example:

MS888G2(gvrp)# show group

GVRP group information

VID Member Port

---- ---

■ **stp**

enable

Syntax:

enable

Description:

Used to enable the STP function.

Argument:

None

Possible value:

None

Example:

MS888G2(stp)# enable

disable

Syntax:

disable

Description:

Used to disable the STP function.

Argument:

None

Possible value:

None

Example:

MS888G2(stp)# disable

set config

Syntax:

set config <Bridge Priority> <Hello Time> <Max. Age> <Forward Delay>

Description:

Used to configure the STP parameters.

Argument:

<Bridge Priority> :Priority must be a multiple of 4096,available from 0 to 61440.

<Hello Time>: available from 1 to 10.

<Max. Age>: available from 6 to 40.

<Forward Delay>: available from 4 to 30.

Possible value:

<Bridge Priority> 0 to 61440.

<Hello Time>: 1 to 10.

<Max. Age>: 6 to 40.

<Forward Delay>: 4 to 30.

Example:

MS888G2(stp)# set config 61440 2 20 15

: Configures the STP parameters as follows, Bridge Priority of 61440, Hello Time of 2, Max Age of 20 and a Forward Delay of 15.

set version

Syntax:

set version <stp | rstp>

Description:

Used to select the STP mode.

Argument:

<stp | rstp>:stp / rstp

Possible value:

<stp | rstp>:stp / rstp

Example:

MS888G2(stp)# set version rstp

: Sets the STP mode to RSTP (Rapid Spanning Tree Protocol).

set port

Syntax:

set port <range> <path cost> <priority> <edge_port> <admin p2p>

Description:

Used to configure the port information of STP.

Argument:

<range>: syntax 1,5-7, available from 1 to 26

<path cost>: 0, 1-200000000. If 0 is entered path cost is automatic.

<priority>: priority must be a multiple of 16, available from 0 to 240

<edge_port>: Admin Edge Port, <yes | no>

<admin p2p>: Admin point to point, <auto |true | false>

Possible value:

<range> : 1 to 26

<path cost>: 0, 1-200000000.

<priority> : 0 to 240

<edge_port> : yes / no

<admin p2p>: auto / true / false

Example:

MS888G2(stp)# set port 1-16 0 128 yes auto

: Configures ports 1 through to 16 with a path cost of 0, priority of 128, edge port is set as yes and the admin P2P is set to auto.

show status

Syntax:

show status

Description:

Used to display the status of STP.

Argument:

None

Possible value:

None

Example:

MS888G2(stp)# show status

STP Status :

STP State:	Enabled
Bridge ID:	00:00:8C:D8:09:1D
Bridge Priority:	61440
Designated Root:	00:00:8C:D8:09:1D
Designated Priority:	61440
Root Port:	0
Root Path Cost:	0
Current Max. Age(sec):	20
Current Forward Delay(sec):	15
Hello Time(sec):	2
STP Topology Change Count:	0

Time Since Last Topology Change(sec) : 848

show config

Syntax:

show config

Description:

Used to display the configuration of STP.

Argument:

None

Possible value:

None

Example:

MS888G2(stp)# show config

STP State Configuration:

Spanning Tree Protocol:	Enabled
Bridge Priority (0-61440):	61440
Hello Time (1-10 sec):	2
Max. Age (6-40 sec):	20
Forward Delay (4-30 sec):	15
Force Version:	RSTP

show port

Syntax:

show port

Description:

Used to display the port information of STP.

Argument:

None

Possible value:

None

Example:

MS888G2(stp)# show port

Port Port Status Path Cost Priority Admin Edge Port Admin Point To Point

==== ========== ========= ======== ============== ====================

1	DISCARDING	2000000	128	Yes	Auto
2	DISCARDING	2000000	128	Yes	Auto
3	DISCARDING	2000000	128	Yes	Auto
4	DISCARDING	2000000	128	Yes	Auto
5	DISCARDING	2000000	128	Yes	Auto
6	DISCARDING	2000000	128	Yes	Auto
7	DISCARDING	2000000	128	Yes	Auto
8	DISCARDING	2000000	128	Yes	Auto
9	DISCARDING	2000000	128	Yes	Auto
10	DISCARDING	2000000	128	Yes	Auto
11	DISCARDING	2000000	128	Yes	Auto
12	DISCARDING	2000000	128	Yes	Auto
13	DISCARDING	2000000	128	Yes	Auto
14	DISCARDING	2000000	128	Yes	Auto
15	DISCARDING	2000000	128	Yes	Auto
16	DISCARDING	2000000	128	Yes	Auto
17	DISCARDING	2000000	128	Yes	Auto
18	DISCARDING	2000000	128	Yes	Auto
19	DISCARDING	2000000	128	Yes	Auto
20	DISCARDING	2000000	128	Yes	Auto
21	DISCARDING	2000000	128	Yes	Auto
22	DISCARDING	2000000	128	Yes	Auto

23	DISCARDING	2000000	128	Yes	Auto
24	DISCARDING	2000000	128	Yes	Auto
25	DISCARDING	2000000	128	Yes	Auto
26	DISCARDING	2000000	128	Yes	Auto

■ **trunk**

set priority

Syntax:

set priority <range>

Description:

Used to configure the LACP system priority settings.

Argument:

<range> : available from 1 to 65535.

Possible value:

1 to 65535

Example:

MS888G2(trunk)# set priority 33333

: Sets the LACP priority setting to 33333.

set trunk

Syntax:

set trunk <port-range> <method> <group> <active LACP>

Description:

Used to configure the trunk method including the status of the trunk, the group number and the mode of the trunk, this also includes LACP mode.

Argument:

<port-range> : syntax 1,5-7, available from 1 to 24

<method>:

static: Configure the switch to use static link aggregation.

lacp: Configure the switch to use LACP based link aggregation.

<group>: 1-8.

<active LACP>:

active : set the LACP to active mode

passive : set the LACP to passive mode

Possible value:

None

Example:

MS888G2(trunk)# set trunk 1-4 lacp 1 active

: Sets up a LACP based trunk group containing ports 1 through to 4 using LACP active mode.

del trunk

Syntax:

del trunk <port-range>

Description:

Delete trunk port

Argument:

<port-range> : syntax 1,5-7, available from 1 to 24

Possible value:

None

Example:

MS888G2(trunk)# del trunk 1

: Deletes trunk group 1.

show status

Syntax:

show status

Description:

Used to display the aggregator status and the settings of each port.

Argument:

None

Possible value:

None

Example:

MS888G2(trunk)# show status

Trunk Port Setting Trunk Port Status

port	Method	Group	Active LACP	Aggregator	Status
1	None	0	Active	1	Ready
2	LACP	1	Active	2	---
3	LACP	1	Active	3	---
4	LACP	1	Active	4	---
5	LACP	1	Active	5	---
6	LACP	1	Active	6	---
7	LACP	1	Active	7	---
8	LACP	1	Active	8	---
9	LACP	1	Active	9	---
10	LACP	1	Active	10	---
11	LACP	1	Active	11	---
12	LACP	1	Active	12	---
13	LACP	1	Active	13	---
14	LACP	1	Active	14	---
15	None	0	Active	15	---
16	None	0	Active	16	---

show aggtr-view

Syntax:

show aggtr-view

Description:

Used to display the aggregator list.

Argument:

None

Possible value:

None

Example:

MS888G2(trunk)# show aggtr-view

Aggregator 1) Method: None

Member Ports: 1

Ready Ports:1

Aggregator 2) Method: LACP

Member Ports: 2

Ready Ports:

show lacp-detail

Syntax:

show lacp-detail <aggtr>

Description:

Used to display detailed information of a LACP trunk group.

Argument:

<aggtr> : available from 1 to 24

Possible value:

None

Example:

MS888G2(trunk)# show lacp-detail 2

Aggregator 2 Information:

Actor		Partner	
System Priority	MAC Address	System Priority	MAC Address
32768	00-00-8C-E8-00-02	32768	00-00-00-00-00-00

Port	Key	Trunk Status	Port	Key
2	257	---	2	0

show lacp-priority

Syntax:

show lacp-priority

Description:

Used to display the value of LACP Priority.

Argument:

None

Possible value:

None

Example:

MS888G2(trunk)# show lacp-priority

LACP System Priority: 32768

■ **802.1x**

set state

Syntax:

set state <ip> <port-number> <secret-key>

Description:

To configure the settings related with 802.1X Radius Server.

Argument:

<ip>: the IP address of the Radius Server.

<port-number>: the service port of the Radius Server(Authorisation port)

<secret-key>: Enter a secret-key, length of secret-key is from 1 to 31.

Possible value:

<port-number> : 1~65535, default is 1812

Example:

MS888G2(802.1x)# set state 192.168.1.115 1812 WinRadius

: Configures the switch to use a RADIUS Server with an IP Address of 192.168.1.115 using port 1812 and a secret key of WinRadius.

set mode

Syntax:

set mode <port-range> <mode>

Description:

Used to set up the 802.1X authentication mode of each port.

Argument:

<port range> : syntax 1,5-7, available from 1 to 26

<mode>: set up 802.1x mode

0: disable the 802.1x function

1: set 802.1x to Multi-host mode

Possible value:

<port range> : 1 to 26

<mode>: 0 or 1

Example:

MS888G2(802.1x)# set mode 2 1

: Sets port 2 to use 802.1x Multi-host Mode.

set port-control

Syntax:

set port-control <port-range> <authorised>

Description:

Use to set up the 802.1X settings for each port.

Argument:

<port range> : syntax 1,5-7, available from 1 to 26

<authorized> : Set up the status of each port

0: ForceUnauthorised

1: ForceAuthorised

2: Auto

Possible value:

<port range> : 1 to 24

<authorized> : 0, 1 or 2

Example:

MS888G2(802.1x)# set port-control 2 2

: Sets port 2 to use Auto mode for the 802.1x port mode.

set reAuthMax

Syntax:

set reAuthMax <port-range> <max>

Description:

The number of re-authentication attempts that are permitted before the port becomes Unauthorised.

Argument:

<port range>: syntax 1,5-7, available from 1 to 24

<max>: max. value , range 1-10

Possible value:

<port range> : 1 to 24

<max>: 1-10, default is 2

Example:

MS888G2(802.1x)# set reAuthMax 2 2

: Allows port 2 to have only 2 re-authentication attempts before the port will be set to unauthorised.

set txPeriod

Syntax:

set txPeriod <port-range> <sec>

Description:

A timer used by the Authenticator PAE state machine to determine when an EAPOL PDU is to be transmitted.

Argument:

<port range>: syntax 1, 5-7, available from 1 to 26

<sec>: timer , range 1-65535

Possible value:

<port range>: 1 to 26

<sec>: 1-65535, default is 30

Example:

MS888G2(802.1x)# set txPeriod 2 30

: Sets the timer for port 2 to 30 seconds.

set quiet-period

Syntax:

set quiet-period <port-range> <sec>

Description:

A timer used by the Authenticator state machine to define periods of time when it will not attempt to acquire a Supplicant.

Argument:

<port range> : syntax 1,5-7, available from 1 to 26

<sec> : timer , range 0-65535

Possible value:

<port range> : 1 to 26

<sec> : 0-65535, default is 60

Example:

GS-2116C(802.1x)# set quiet-period 2 30

: Sets the quiet period for port 2 to 30 seconds.

set reAuthEnabled

Syntax:

set reAuthEnabled <port-range> <ebl>

Description:

Defines whether a regular re-authentication will take place on this port.

Argument:

<port range> : syntax 1,5-7, available from 1 to 26

<ebl> :

0: OFF Disable re-authentication

1: ON Enable re-authentication

Possible value:

<port range> : 1 to 26

<ebl> : 0 or 1, default is 1

Example:

MS888G2(802.1x)# set reAuthEnabled 2 1

: Enables re-authentication for port 2.

set reAuthPeriod

Syntax:

set reAuthPeriod <port-range> <sec>

Description:

Defines a nonzero number of seconds between periodic re-authentication of the supplicant.

Argument:

<port range> : syntax 1,5-7, available from 1 to 26

<sec> : timer , range 1-65535

Possible value:

<port range> : 1 to 26

<sec> : 1-65535, default is 3600

Example:

MS888G2(802.1x)# set reAuthPeriod 2 3600

: Sets port 2 to re-authenticate with the RADIUS Server every 3600 seconds.

set max-request

Syntax:

set max-request <port-range> <times>

Description:

The maximum number of times that the state machine will retransmit an EAP Request packet to the Supplicant before it times out the authentication session.

Argument:

<port range> : syntax 1,5-7, available from 1 to 26

<times>: max-times , range 1-10

Possible value:

<port range> : 1 to 26

<times>: 1-10, default is 2

Example:

MS888G2(802.1x)# set max-request 2 2

: Sets the maximum number of request times for port 2 to 2.

set suppTimeout

Syntax:

set suppTimeout <port-range> <sec>

Description:

A timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.

Argument:

<port range> : syntax 1,5-7, available from 1 to 26

<sec> : timer , range 1-65535

Possible value:

<port range> : 1 to 26

<sec> : 1-65535, default is 30

Example:

MS888G2(802.1x)# set suppTimeout 2 30

: Sets the suppTimeout value for port 2 to 30 seconds.

set serverTimeout

Syntax:

set serverTimeout <port-range> <sec>

Description:

A timer used by the Backend Authentication state machine in order to determine timeout conditions in the exchanges between the Authenticator and the Supplicant or Authentication Server. The initial value of this timer is either suppTimeout or serverTimeout, as determined by the operation of the Backend Authentication state machine.

Argument:

<port range> : syntax 1,5-7, available from 1 to 26

<sec> : timer , range 1-65535

Possible value:

<port range> : 1 to 26

<sec> : 1-65535, default is 30

Example:

MS888G2(802.1x)# set serverTimeout 2 30

: Sets the server timeout value for port 2 to 30 seconds.

show state

Syntax:

show state

Description:

Shows the Radius server configuration.

Argument:

None

Possible value:

None

Example:

MS888G2(802.1x)# show state

Radius Server: 192.168.1.115

Port Number : 1812

Secret Key   : WinRadius

show mode

Syntax:

show mode

Description:

Displays what mode each port is using.

Argument:

None

Possible value:

None

Example:

MS888G2(802.1x)# show mode

Port	Mode
1	Disable
2	Multi-host
3	Disable
4	Disable
5	Disable
6	Disable
:	
:	
:	

show security

Syntax:

show security

Description:

Displays the authentication status of each port.

Argument:

None

Possible value:

None

Example:

MS888G2(802.1x)# show security

Port	Mode	Status
1	Disable	
2	Multi-host	Unauthorised
3	Disable	
4	Disable	
5	Disable	
6	Disable	
	:	
	:	
	:	

show parameter

Syntax:

show parameter

Description:

Displays the parameter settings of each port.

Argument:

None

Possible value:

None

Example:

MS888G2(802.1x)# show parameter

Port. 1) port control : Auto
reAuthMax : 2
txPeriod : 30
Quiet Period : 60
reAuthEnabled : ON
reAuthPeriod : 3600
max. Request : 2
suppTimeout : 30
serverTimeout : 30

Port. 2) port control : Auto
reAuthMax : 2
txPeriod : 30
Quiet Period : 60
reAuthEnabled : ON
reAuthPeriod : 3600
max. Request : 2
suppTimeout : 30
serverTimeout : 30

:
:
:

■ **alarm**

<<events>>

set

Syntax:

set sms <range>

set email <range>

set trap <range>

set all <range>

Description:

Used to activate the different alarm events supported including sms, email and traps.

Argument:

<range>: syntax 1,5-7, trap number.

Possible value:

available from 1 to 26.

Example:

MS888G2(alarm-events)# set sms 1-3

MS888G2(alarm-events)# set email 1-3

MS888G2(alarm-events)# set trap 1-3

MS888G2(alarm-events)# set all 1-3

: Sends an SMS, Email and trap event when alarms 1 to 3 occur. Alarms 1, 2 and 3 are “Cold Start”, “Warm Start” and “Link Down” respectively.

del

Syntax:

del sms <range>

del email <range>

del trap <range>

del all <range>

Description:

Used to de-activate the different alarm events supported including sms, email and traps.

Argument:

<range>:trap number.

Possible value:

available from 1 to 26.

Example:

MS888G2(alarm-events)# del sms 1-3

MS888G2(alarm-events)# del email 1-3

MS888G2(alarm-events)# del trap 1-3

MS888G2(alarm-events)# del all 1-3

: Deletes all trap events configured including SMS, Email and SNMP Trap.

show

Syntax:

show

Description:

Displays the configuration of the alarm events.

Argument: None

Possible value: None

Example:

MS888G2(alarm-events)# show

Events	Email	SMS	Trap
1 Cold Start			v
2 Warm Start			v
3 Link Down			v
4 Link Up			v
5 Authentication Failure			v
6 User Login			
7 User Logout			
8 STP Topology Changed			
9 STP Disabled			
10 STP Enabled			
11 LACP Disabled			
12 LACP Enabled			
13 LACP Member Added			
14 LACP Port Failure			
15 GVRP Disabled			
16 GVRP Enabled			
17 VLAN Disabled			
18 Port-based Vlan Enabled			
19 Tag-based Vlan Enabled			
20 Metro-mode Vlan Enabled			
21 Double-tag Vlan Enabled			
22 Module Inserted			
23 Module Removed			
24 Module Media Swapped			

<<email>>

set

Syntax:

set server <ip>

set user <username>

set mail-address <#> <mail address>

Description:

Used for the configuration of the e-mail server, username, password and email address.

Argument:

<ip>: E-mail server ip

<username>: email server account and password

<#>: email address number, range: 1 to 6

<mail address>: email address

Possible value:

<#>: 1 to 6

Example:

MS888G2(alarm-email)# set server 192.168.1.6

: Sets the Email Server address to 192.168.1.6.

MS888G2(alarm-email)# set user admin

: Sets the username for the email account to admin.

Password: 123

: Sets the password to 123

Confirm Password: 123

MS888G2(alarm-email)# set mail-address 1 test@alloy.com.au

: Sets email recipient 1 of the trap events to test@alloy.com.au.

del

Syntax:

del <#>

Description:

Used to remove the configuration of the E-mail address.

Argument:

<#>: email address number, range: 1 to 6

Possible value:

<#>: 1 to 6

Example:

MS888G2(alarm-email)# del 2

: Deletes email recipient 2.

show

Syntax:

show

Description:

Display's the configuration of the e-mail trap event.

Argument:

None.

Possible value:

None.

Example:

MS888G2(alarm-email)# show

Mail Server : 192.168.1.6

Username : admin

Password : **********

Email Address 1: test@alloy.com.au

Email Address 2:

Email Address 3:

Email Address 4:

Email Address 5:

Email Address 6:

<<sms>>

set

Syntax:

set server <ip>

set user <username>

set phone-number <#> <phone-number>

Description:

Used for the configuration of the SMS server, username, password and phone number.

Argument:

<ip>: SMS server ip

<username>: SMS server account and password

<#>: mobile phone number, range: 1 to 6

<phone-number>: phone number

Possible value:

<#>: 1 to 6

Example:

MS888G2(alarm-sms)# set server 192.168.1.7

: Sets the SMS Server to 192.168.1.7

MS888G2(alarm-sms)# set user admin

: Sets the username for the SMS account to admin.

Password: 123

: Sets the password to 123

Confirm Password: 123

MS888G2(alarm-sms)# set phone-number 1 0411111111

: Sets SMS recipient 1 of the trap events to 0411111111

del

Syntax:

del <#>

Description:

Used to remove the configuration of a mobile phone number.

Argument:

<#>: mobile phone number, range: 1 to 6

Possible value:

<#>: 1 to 6

Example:

MS888G2(alarm-sms)# del 3

: Removes SMS recipient 3 from the list.

show

Syntax:

show

Description:

Display's the configuration of the SMS trap events.

Argument:

None.

Possible value:

None.

Example:

MS888G2(alarm-sms)# show

SMS Server : 192.168.1.7

Username :

Password : **********

Mobile Phone 1: 0411111111

Mobile Phone 2:

Mobile Phone 3:

Mobile Phone 4:

Mobile Phone 5:

Mobile Phone 6:

show (alarm)

Syntax:

show

Description:

Display's the configuration of Trap, SMS or E-mail.

Argument:

None.

Possible value:

None.

Example:

MS888G2(alarm)# show events

MS888G2(alarm)# show email

MS888G2(alarm)# show sms

■ **diag**

diag

Syntax:

diag

Description:

Diag is used to test the UART, DRAM, Flash and EEPROM.

Argument:

None.

Possible value:

None.

Example:

MS888G2(diag)# diag

EEPROM Test: OK

UART Test: OK

DRAM Test: OK

Flash Test: OK

Loopback

Syntax:

Loopback

Description:

For Internal/External Loopback Test.

Argument:

None.

Possible value:

None.

Example:

MS888G2(diag)# loopback

Internal Loopback Test : OK

External Loopback Test : Port 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 Fail

ping

Syntax:

ping <ip>

Description:

Used to test connectivity between other IP based devices on your network.

Argument:

[ip] : ip address or domain name

Possible value:

IP address, e.g. 192.168.2.65 or domain name, e.g. alloy.com.au

Example:

MS888G2(diag)# ping 192.168.1.115

Gateway : 192.168.1.253

192.168.1.115 is alive.

■ **log**

show

Syntax:

show

Description:

Display's a list of trap log events. If a trap event occurs, it will be recorded into the log. The log can hold up to 120 records. Use the show command to display the log.

Argument:

None.

Possible value:

None.

Example:

MS888G2(log)# show

Tftp Server : 0.0.0.0

Auto Upload : Disable

1) Wed Feb13 12:13:27 2006 Link Up [Port 1]
2) Wed Feb 13 12:13:26 2006 Link Down [Port 1]
3) Wed Feb 13 11:58:31 2006 Login [admin]
4) Wed Feb 13 11:19:45 2006 Login [admin]
5) Wed Feb 13 11:19:37 2006 Logout [admin]

clear

Syntax:

clear

Description:

Used to clear the log data.

Argument:

None.

Possible value:

None.

Example:

MS888G2(log)# clear

upload

Syntax:

Upload

Description:

Used to upload log data through TFTP.

Argument:

None.

Possible value:

None.

Example:

MS888G2(log)# upload

: Uploads the contents of the log to a preconfigured TFTP Server. (see TFTP section)

enable auto-upload

Syntax:

enable auto-upload

Description:

Used to enable the auto-upload function.

Argument:

None.

Possible value:

None.

Example:

MS888G2(log)# enable auto-upload

: Enables the auto-upload function so the log is automatically uploaded to the TFTP server.

disable auto-upload

Syntax:

disable auto-upload

Description:

Used to disable the auto-upload function.

Argument:

None.

Possible value:

None.

Example:

MS888G2(log)# disable auto-upload

: Disables the auto-upload function.

■ **firmware**

set upgrade-path

Syntax:

set upgrade-path <filepath>

Description:

Sets the firmware file needed to upgrade the switch.

Argument:

<filepath>: upgrade file path

Possible value:

<filepath>: upgrade file path

Example:

MS888G2(firmware)# set upgrade-path ms888g2_v2.06.bin

upgrade

Syntax:

upgrade

Description:

Used to upgrade the firmware in the switch for known issues or to add additional features.

Argument:

None

Possible value:

None

Example:

MS888G2(firmware)# upgrade

Upgrading firmware ...

show

Syntax:

show

Description:

Display's the TFTP server and upgrade-path information.

Argument:

None

Possible value:

None

Example:

MS888G2(firmware)# show

TFTP Server IP Address: 192.168.1.100

Path and Filename : ms888g2_v2.06.bin

■ **config-file**

set export-path

Syntax:

set export-path <filepath>

Description:

To set the filepath and filename that will be used to export the configuration of the switch.

Argument:

<filepath>: filepath and filename

Possible value:

<filepath>: filepath and filename

Example:

MS888G2(config-file)# set export-path log/21511.txt

: Exports the config file to a folder called log with a file name of 21511.txt.

set import-path

Syntax:

set import-path <filepath>

Description:

To set up the filepath and filename of a configuration file that will be imported into the switch.

Argument:

<filepath>: filepath and filename

Possible value:

<filepath>: filepath and filename

Example:

MS888G2(config-file)# set import-path log/21511.txt

: Used to browse to a specific location to import the configuration file named 21511.txt.

e*xport start*

Syntax:

export start

Description:

Exports the start up configuration of the switch.

Argument:

None

Possible value:

None

Example:

MS888G2(config-file)# export start

Export successful.

e*xport user-conf*

Syntax:

export user-conf

Description:

Exports the user configuration of the switch.

Argument:

None

Possible value:

None

Example:

MS888G2(config-file)# export user-conf

Export successful.

import start

Syntax:

import start

Description:

Imports the startup configuration into the switch.

Argument:

None

Possible value:

None

Example:

MS888G2(config-file)# import start

Import successful.

import user-conf

Syntax:

import user-conf

Description:

Imports the user configuration into the switch.

Argument:

None

Possible value:

None

Example:

MS888G2(config-file)# import user-conf

Import successful.

show

Syntax:

show

Description:

Display's the config-file information.

Argument:

None

Possible value:

None

Example:

MS888G2(config-file)# show

TFTP Server IP Address: 192.168.1.100

Export Path and Filename: log/21511.txt

Import Path and Filename: log/21511.txt

■ **tftp**

set server

Syntax:

set server <ip>

Description:

To set up the IP address of the TFTP server.

Argument:

<ip>: TFTP server ip

Possible value:

<ip>: TFTP server ip

Example:

MS888G2(tftp)# set server 192.168.1.100

: Sets the IP address of the TFTP Server to 192.168.1.100

show

Syntax:

show

Description:

Display's the information of the TFTP server.

Argument:

None

Possible value:

None

Example:

MS888G2(tftp)# show

TFTP Server : 192.168.1.100

■ **hostname**

hostname

Syntax:

hostname

Description:

Used to configure a hostname for the switch.

Argument:

<name>: hostname, max 128 characters.

Possible value:

<name>: hostname, max 128 characters.

Example:

MS888G2# hostname Company

: Sets the hostname of the switch to Company.

■ **autologout**

autologout

Syntax:

autologout <time>

Description:

Used to configure the auto logout timer.

Argument:

<time>: range 1 to 3600 seconds, 0 for auto logout off, current setting is 180 seconds.

Possible value:

<time>: 0,1-3600

Example:

MS888G2# autologout 3600

: Sets the auto logout time to 3600 seconds

■ **reboot**

reboot

Syntax:

reboot

Description:

Used to reboot the switch.

Argument:

None

Possible value:

None

Example:

MS888G2# reboot

: Reboots the switch.

Appendix A
Technical Specifications

Hardware Specifications

- ***Standard Compliance:*** IEEE802.3ab / 802.3z / 802.3u / 802.3x
  802.3z and 802.3ab compliant Gigabit Ethernet ports

- ***Transmission Mode:*** 10/100Mbps support full or half duplex
  1000Mbps support full duplex only

- ***Transmission Speed:*** 10/100/1000Mbps for TP
  10/100Mbps for 8-port FE TP Module
  100Mbps for 8-port FE Fibre Module
  1000Mbps for SFP Fibre

- ***Full Forwarding/Filtering Packet Rate: PPS (packets per second)***

1,488,000PPS	1000Mbps
148,800PPS	100Mbps
14,880PPS	10Mbps

- ***MAC Address and Self-learning:*** 8K address table entries,
  256 VLAN table entries,
  256 IP multicast table entries

- ***Buffer Memory:*** Embedded 256KB packet buffers and 128KB control memory.

- ***Flow Control:*** IEEE802.3x compliant for full duplex
  Backpressure flow control for half duplex

- ***Cable and Maximum Length:***

TP	Cat. 5 UTP cable, up to 100m
100Base-FX SC/ST M-M	Multi-Mode Fibre, up to 2Km
100Base-FX SC S-M	Single-Mode Fibre, up to 5/20/60/80Km
100Base-FX WDM SC S-M	Single Fibre, BiDi 20/40/60Km
1000Base-SX SC M-M	Up to 220/275/500/550m, which depends on Multi-Mode Fibre type
1000Base-LX SC S-M	Single-Mode Fibre, up to10/30/50Km
1000Base-FX WDM SC S-M	Single Fibre, BiDi 20Km

- ***Diagnostic LED:***

System LED : Power A/B
CPURUN
ACT (LEDSET)
FDX (LEDSET)
SPD (LEDSET)

Per Port LED:

10/100M Port 1 to 8 of 3 Modules : LINK/ACT, FDX, SPD

1000M Fiber/TP Port 25,26 : LINK/ACT, FDX, SPD

- ***Power Requirement : AC/DC Line***

Voltage : 100~240 VAC or –48VDC

Frequency : 50~60 Hz

Consumption : Max. 55W

- ***Ambient Temperature*** : 0° to 40°C
- ***Humidity*** : 5% to 90%
- ***Dimensions*** : 44(H) × 442(W) × 366(D) mm
- ***Comply with FCC Part 15 Class A & CE Mark Approval & C-Tick***

Note: Any specification is subject to change without notice.

Appendix B
Null Modem Cable Specifications

The DB-9 cable is used for connecting a terminal or terminal emulator to the Managed Switch's RS-232 port to access the command-line interface.

The table below shows the pin assignments for the DB-9 cable.

Function	Mnemonic	Pin
Carrier	CD	1
Receive Data	RXD	2
Transmit Data	TXD	3
Data Terminal Ready	DTR	4
Signal Ground	GND	5
Data Set Ready	DSR	6
Request To Send	RTS	7
Clear To Send	CTS	8

9 Pin Null Modem Cable