3 x 10/100Base-TX to 1 x 100Base-FX
Managed Converter Switch

Network Management

User's Guide
Ver : 1.0

.

Table of Contents

1. INTRODUCTION

Thank you for using the 3x10/100TX plus 1x100FX managed converter switch. The built-in management module allows user to configure this managed converter switch and monitor the operation status locally or thru network remotely.

1.1 Management Options

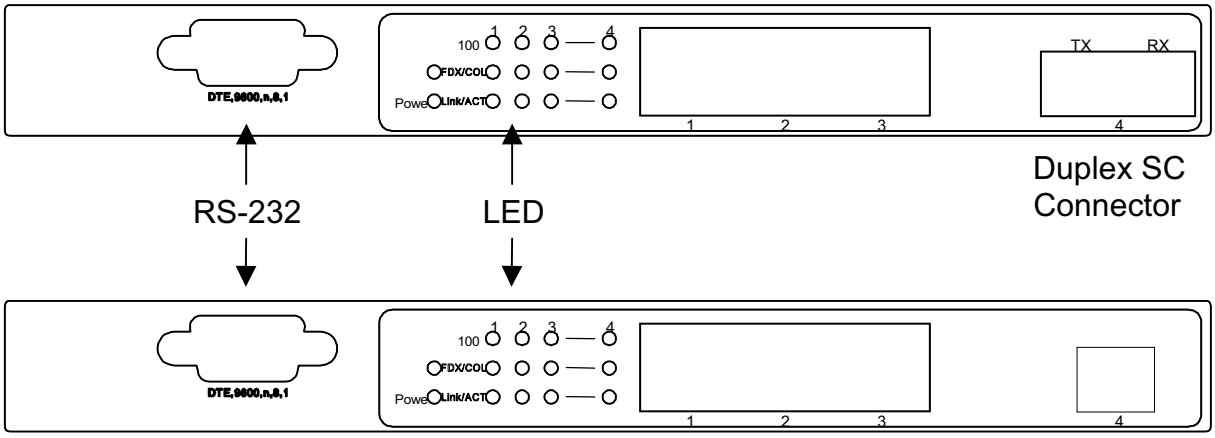


Fig. 1 Front Panel

The managed converter switch support both in-band and out-of-band management. In-band refers to managing the converter switch through the front panel network ports. Out-of-band means going through the front RS-232 DB-9 port. Available options are listed below:

- Local Console Management
- Telnet Management
- SNMP Management

Local Console Management

Local Console Management is done through the RS-232 DB-9 console port located at the front of the converter switch. Direct RS-232 cable connection between the PC and the converter switch is required for this type of management.

Telnet Management

Telnet is done through the network. Once the converter switch is on the network with proper configuration, you can use Telnet to log in and monitor the status remotely.

SNMP Management

SNMP is also done over the network. Besides standard MIB (Management Information Bases), an additional private MIB is also provided for SNMP-based network management system to compile & control.

1.2 Management Software & Interfaces

Following list the choices of management software and interfaces:

- Converter switch Console Program
- SNMP-based management software

Console Program

The converter switch has a built-in, menu-driven interface called the Console Program that you can use to:

- Configure the system
- Monitor the status
- Reset the system

You can use this Console Program as your only management system. However, other network management option – SNMP based management system is also available.

You can access the text-mode Console Program locally by connecting a VT100 terminal - or a workstation running VT100 emulation software - to the converter switch RS-232 DB-9 console port directly. Or, you can use Telnet to login and access the Console Program through network connection remotely.

SNMP Management Systems

You can use standard SNMP based network management system to manage the converter switch through the network remotely.

When you use a SNMP based network management system, the converter switch becomes one of the managed devices (network elements) in that system. The converter switch management module contains an SNMP agent that will respond to the requests from the SNMP based network management system. These requests, which you can control, can vary from getting system information to setting the device attribute values.

The converter switch private MIB is provided for installation into your SNMP based network management system.

1.3 Management Preparations

After you have decided how to manage your converter switch, you need to make the cable connection, determine the converter switch IP address and, in some cases, install MIB shipped with your converter switch.

Connecting the converter switch

It is extremely important that cables have the correct pin arrangement and that the proper cables be used when connecting converter switch to another switches, hubs, workstations, …etc.

100Base-FX Fiber Port

1x100Base-FX Fiber port is located at the front of the converter switch. This port is primarily used for up-link connection and will always operate at 100M/Full Duplex mode. Duplex SC or WDM Simplex SC types of connectors are available. Use proper multimode or single-mode optical fiber to connect this port with other Fast Ethernet Fiber port.

10/100Base-TX RJ-45 Ports

3x10/100Base-TX RJ-45 ports are also located at the front of the converter switch. These RJ-45 ports allow user to connect their traditional copper based Ethernet/Fast Ethernet devices into network. All these ports support auto-negotiation and MDI/MDIX auto-crossover, i.e. either crossover or straight through CAT-5 cable may be used.

RS-232 DB-9 Port

The RS-232 DB-9 port is located at the front of the converter switch. This DB-9 port is used for local, out-of-band management. Since this DB-9 port of the converter switch is DTE, a null modem is also required to connect the converter switch and the PC. By connecting this DB-9 port, user can configure & check the converter switch even the network is down.

IP Addresses

IP addresses have the format n.n.n.n, for example 168.168.1.100.

IP addresses are made up of two parts:

- The first part (168.168 in the example) refers as network address identifies the network on which the device resides. Network addresses are assigned by three allocation organizations. Depending on your location, each allocation organization assigns a globally unique network number to each network that wishes to connect to the Internet.

- The second part (8.100 in the example) identifies the device within the network. Assigning unique device numbers is your responsibility. If you are unsure of the IP addresses allocated to you, consult the allocation organization from which your IP addresses were obtained.

Remember that no two devices on a network can have the same address. If you connect to the outside, you must change all the arbitrary IP addresses to comply with those you have been allocated by the allocation organization. If you do not do this, your outside communications will not operate.

A subnet mask is a filtering system for IP addresses. It allows you to further subdivide your network. You must use the proper subnet mask for proper operation of a network with subnets defined.

MIB for Network Management Systems

Private MIB (Management Information Bases) is provided for managing the converter switch through the SNMP based network management system. You must install the private MIB into your SNMP based network management system first.

The MIB file is shipped together with the converter switch. The file name extension is ".mib", which SNMP based compiler can read.

2. CONSOLE PROGRAM

This chapter describes how to use your converter switch Console Program, specifically in:

- Local Console Management (out-of-band)
- Telnet Management (in-band)
- Configuring the system
- Resetting the system

The interface and options are the same with Local Console and Telnet Management. The difference is the type of connection and the port that is used to manage the converter switch.

2.1 Local Console Management

Local Console Management is always done through the RS-232 DB-9 port and requires a direct connection between the converter switch and a PC. This type of management is very useful especially when the network is down and the converter switch cannot be reached by any other means.

You also need to use the Local Console Management to setup the converter switch network configuration for the first time. You can setup the IP address and change the default configuration to desired setting to enable Telnet or SNMP services.

Follow these steps to begin a management session using Local Console Management:

1. Attach the serial cable the RS-232 DB-9 port located at the front of the converter switch with a null modem.
2. Attach the other end to the serial port of a PC or workstation.
3. Run a terminal emulation program using the following settings:

    - **Emulation** VT-100/ANSI compatible
    - **BPS** 9600
    - **Data bits** 8
    - **Parity** None
    - **Stop bits** 1
    - **Flow Control** None
    - **Enable** Terminal keys

4. Press Enter to reach the Main menu.

2.2 Remote Console Management - Telnet

You can manage the converter switch via Telnet session. However, you must first assign a unique IP address to the converter switch before doing so. Use the Local Console to log into the converter switch and set up the IP address for the first time.

Follow these steps to manage the converter switch through Telnet session:

1. Use Local Console to set up the assigned IP parameters of the converter switch,

    - IP address
    - Subnet Mask
    - Default gateway IP address, if required

2. Run Telnet.
3. Log into the converter switch to reach the Main menu.

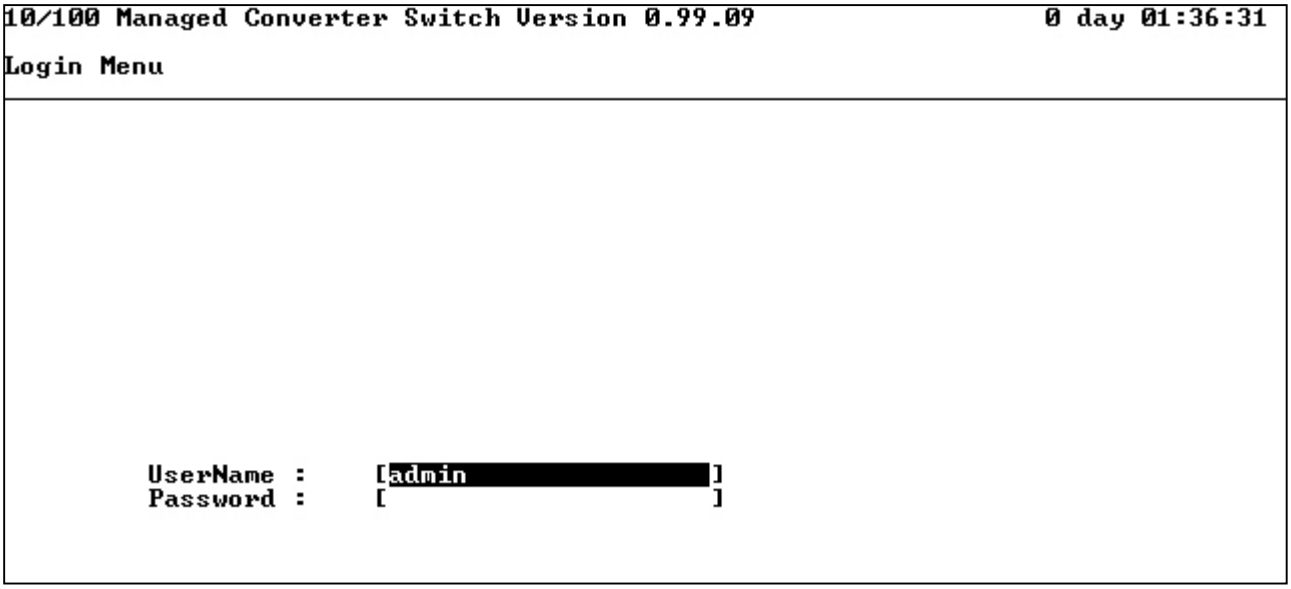
Limitations

When using Telnet, keep the following in mind:

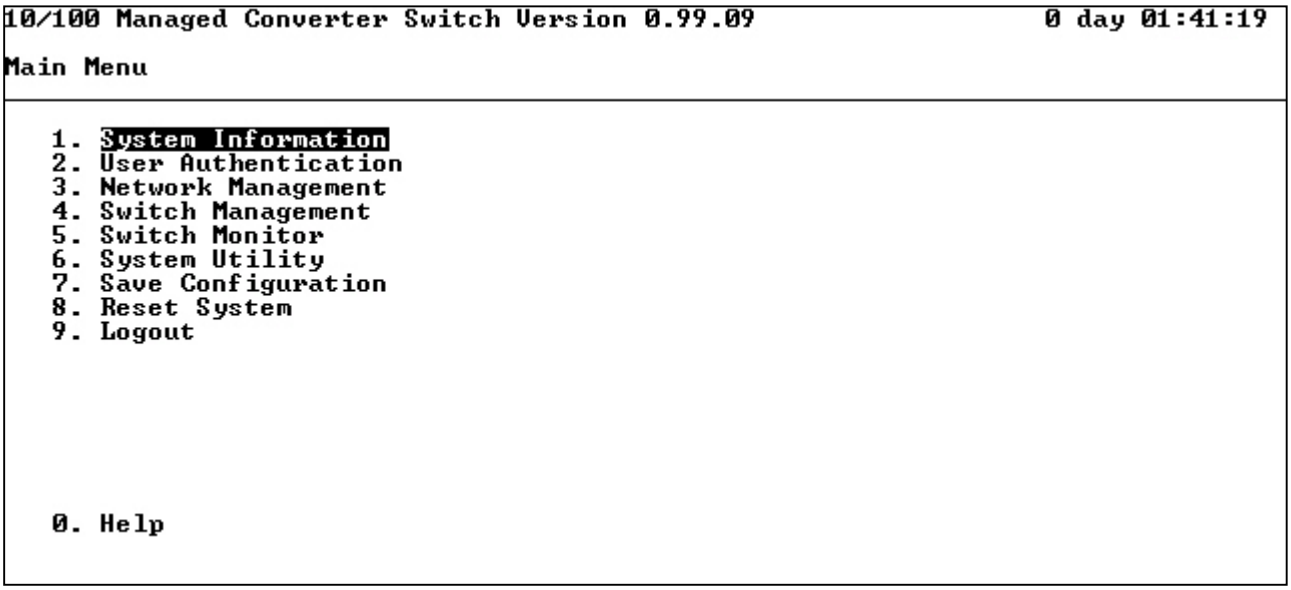
- Only two active Telnet sessions can access the converter switch at one time.

2.3 Console Program Overview

Once you gain the access, a Login Console appear as following,



Enter the user name and password then press ENTER to login to the Console Program main menu,



Press Tab or ↑ or ↓ or Number directly to select.

1. **System Information:** Name the converter switch, specify the location and check the current version information.

2. **User Authentication:** View the registered user list. Add a new user or remove an existing user.

3. **Network Management:** Set up or view the IP address and related information of the converter switch required for network management application.

4. **Switch Management:** Setup switch/port configuration, VLAN configuration and other functions.

5. **Switch Monitor:** View the operation status and traffic statistics of the ports.

6. **System Utility:** Ping, Firmware Upgrade, Load Factory Setting, …etc.

7. **Save Configuration:** Save all change to the system.

8. **Reset System:** Reset converter switch.

9. **Logout:** Logout from the console program.

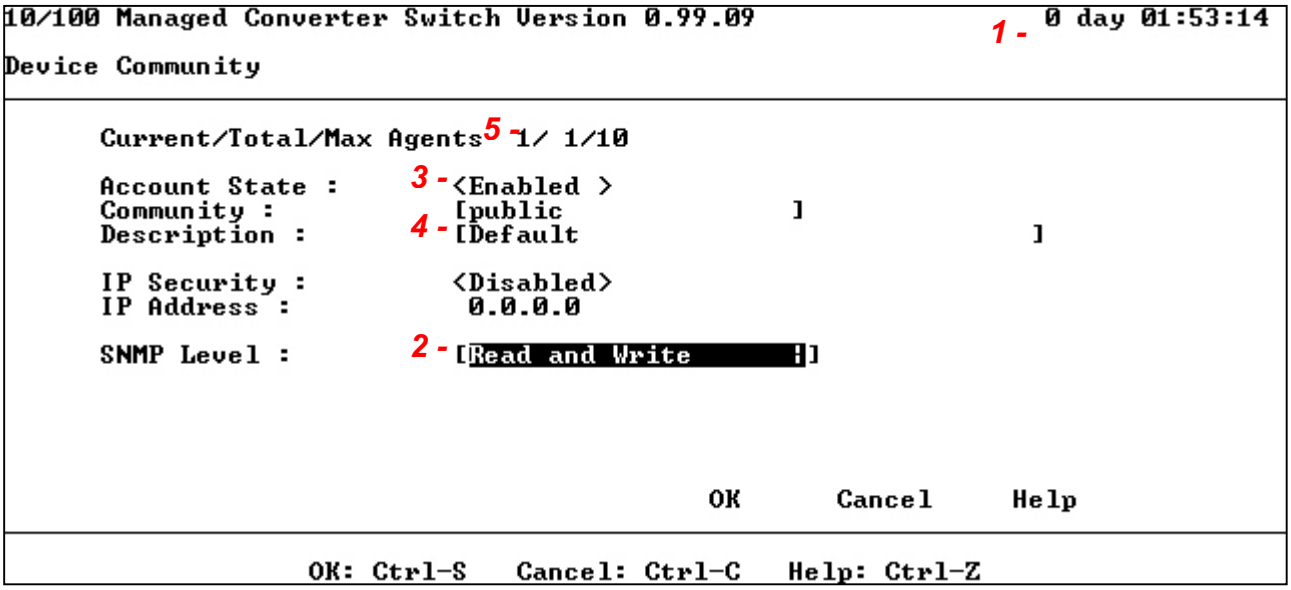
0. **Help:** List the console operation keys.

2.4 Navigating the Console Program Screens

To do this…	Use this key…
Highlight an option in menu.	Tab and ↑ or ↓ or press number directly
Select a highlighted option.	Enter
Pull Down Menu in a choice field.	Spacebar
Select within Pull Down Menu in a choice field.	↑ or ↓
Toggle between available options in a choice field.	Spacebar
Move to the next entry field or command.	Tab
Move one line up to the previous field. ˜	<–
Move one line down to the next field.	–>
Exit current screen	ESC

Field Types

A typical console program screen contains several types of fields, as shown in below figure.



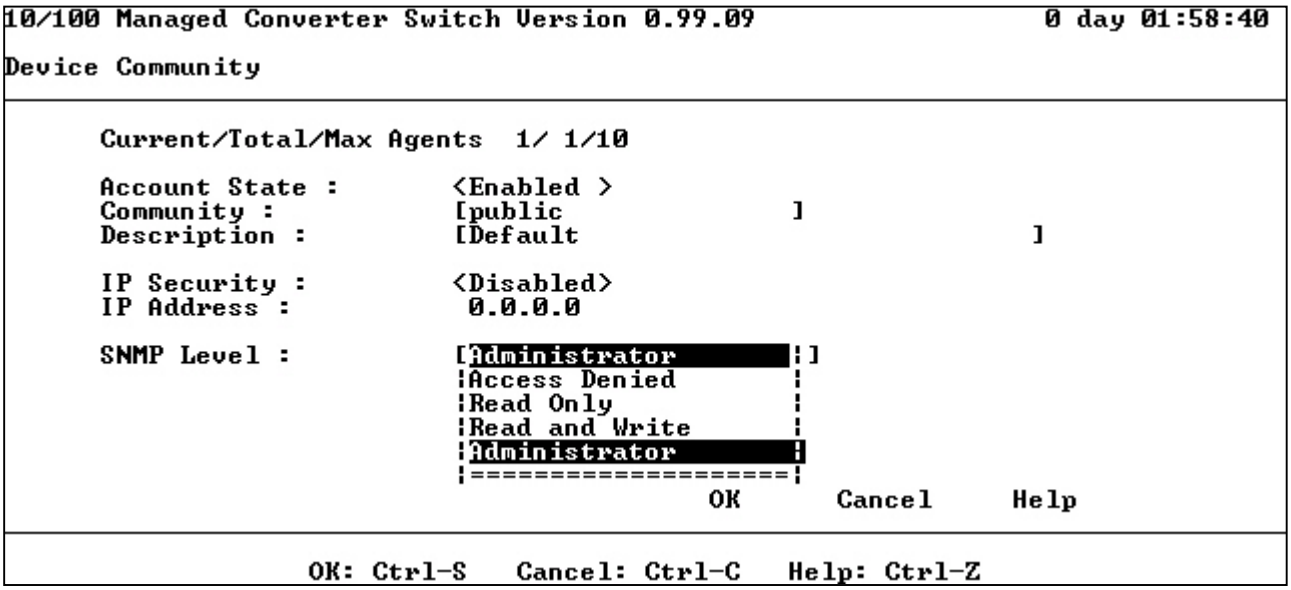
1. Timer: X day XX:XX:XX

Timer is view-only, shows how long the switch has been up since it was turned on or reset.

2. Pull Down Menu: [XXXX |]

Pull down menu is used if there are more than 2 selections, for example: **Port Number**

Press Spacebar will display the pull down menu as below.



Use ↑ or ↓ move to desired selection and then press Spacebar to select.

3. Toggle Option: < XXXX >

A Toggle option contains 2 selections, for example: **Account State**

Press Spacebar to select between **< Enabled > & < Disabled >**

4. Editing Field: [XXXX]

Options may be edited directly, for example: **Community**

Use Backspace to delete default setting and enter new content directly.

5. View Only Field: XXXX

No options available and is view only,

For example: Current number of each registered user.

6. OK

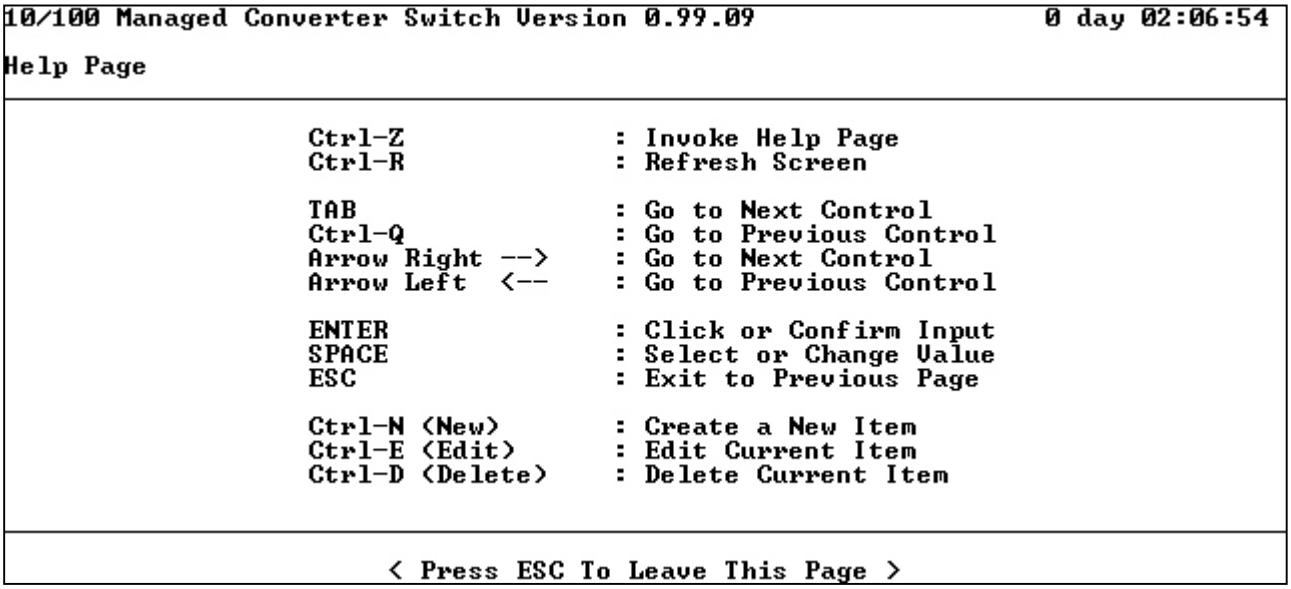
Press OK to accept change and quit the current menu.

7. Cancel

Press Cancel to skip the change and quit the current menu.

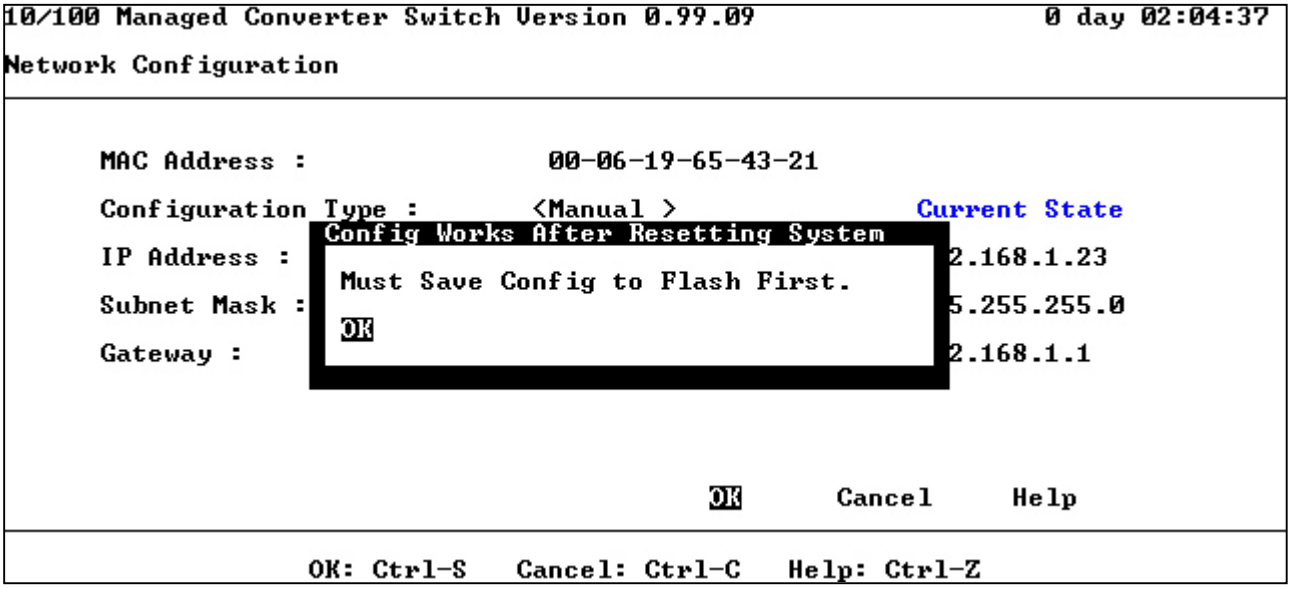
8. Help

Press Help to view On-Line help as below,



NOTICE:

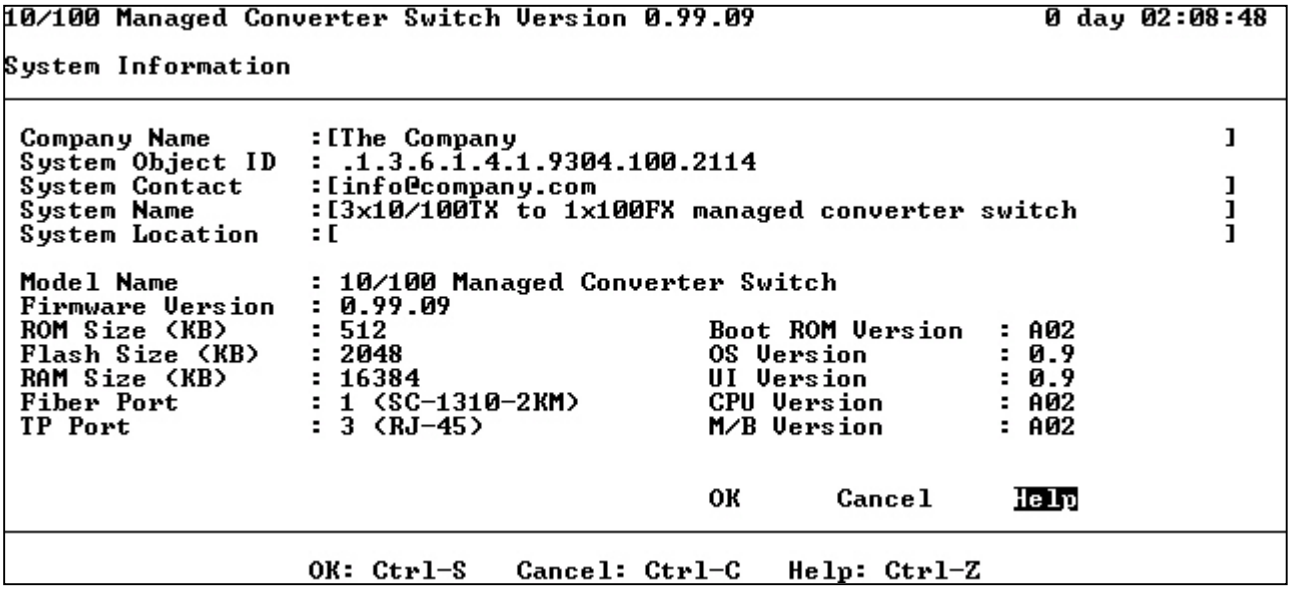
Some of the configuration setting change will require system reset to take effect, a pop up message displayed below will issued to alert the user.



This pop up message alerts user that the configuration change will take effect after reset. However, before perform System Reset, user must save the configuration change first.

2.5 System Information

Select **System Information** in the Console Program Main menu, following screen appears.



Company Name: Enter a company name for this converter switch, up to 55 alphanumeric characters.

System Object ID: View only field, predefined System OID.

System Contact: Enter contact information for this converter switch, up to 55 alphanumeric characters.

System Name: Enter a unique name for this converter switch, up to 55 alphanumeric characters. Use a descriptive name to identify the converter switch in relation to your network, for example “Backbone 1”. This name is mainly used for reference purpose only.

System Location: Enter a brief description of the converter switch location, up to 55 alphanumeric characters. Like the name, the location is for reference only, for example “13th Floor”.

Model Name: View only field shows the product model name.

Firmware Version: View only field shows the product firmware version.

ROM size <KB>: View only field shows the product ROM size.

FLASH size <KB>: View only field shows the product FALSH size.

RAM size <KB>: View only field shows the product RAM size.

Fiber Port: View only field shows the fiber port number and fiber port perimeters.
- 1310 fiber transceiver operation wavelength (nm)
- SC fiber transceiver connector type
- 2KM fiber transceiver operation length

TP Port: View only field shows the total TP port number.

Boot ROM Version: View only field shows the Boot ROM version.

OS Version View only field shows the OS version.

UI Version View only field shows the User Interface program version.

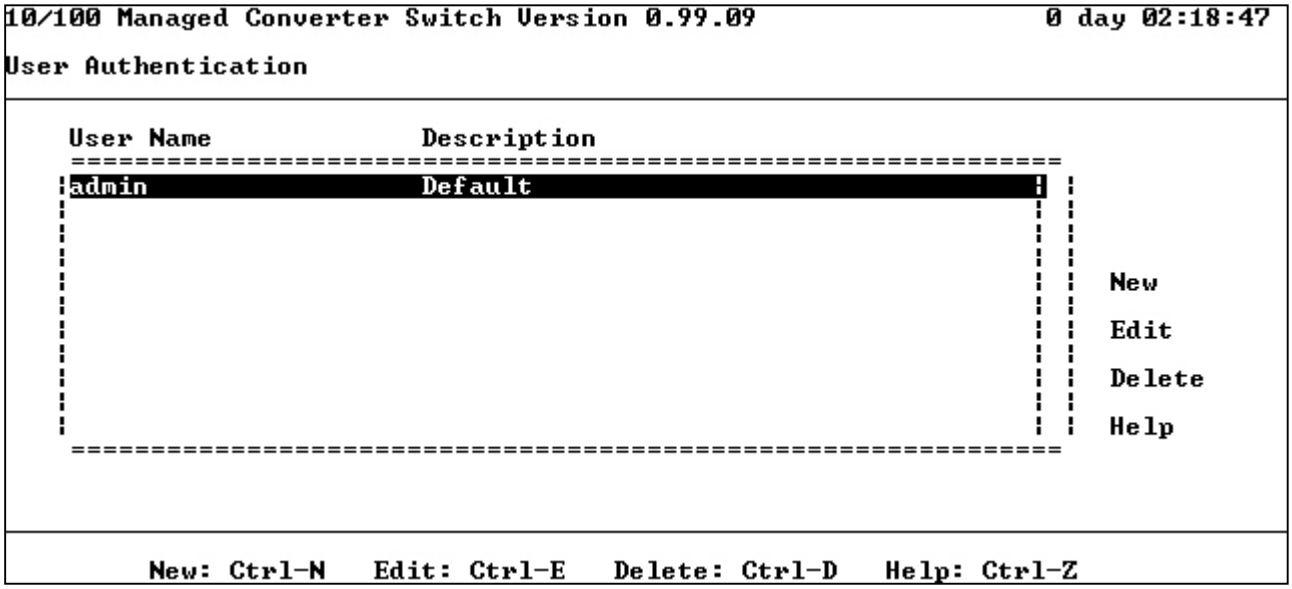
CPU Version View only field shows the CPU version.

M/B Version View only field shows the Main board version.

2.6 User Authentication

To prevent any un-authorized operation, only registered users are allowed to operate the converter switch. Any user want to operate the converter switch need to register into the user list first.

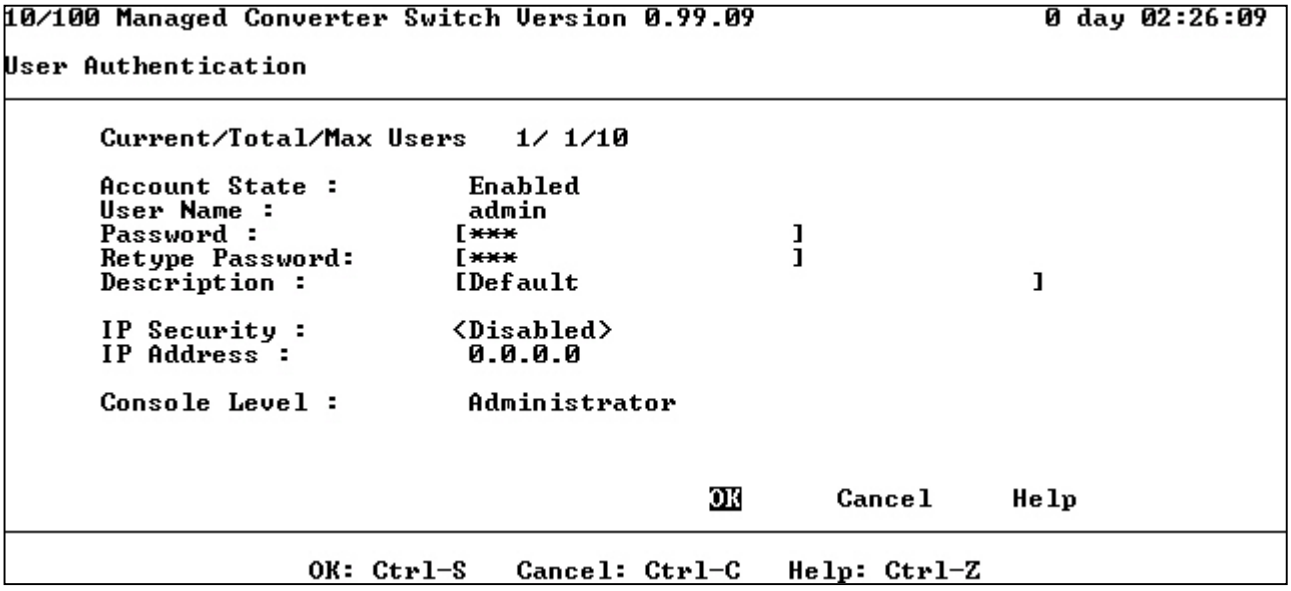
To view or change current registered users, select **2. User Authentication** from the main menu, following screen appears.



Up to 10 Users maybe set.

Use **Delete** to remove a registered user.
Press **New** to add a new user.
Press **Edit** to view the current user setting.

Following screen appears,



Current/Total/Max Users: View only field. Specify:

Current:	Current registered user number.
Total:	Total registered user number.
Max Users:	Maximum available registered user number, default 10.

Account State: Press Spacebar to Enable or Disable this User Account.

User Name: Specified the authorized user login name, up to 20 alphanumeric characters.

Password: Enter desired user password, up to 20 alphanumeric characters.

Retype Password: Enter password again for double check.

Description: Enter a unique description for the User, up to 35 alphanumeric characters. This is mainly for reference purpose only.

IP Security: Press Spacebar to Enable or Disable the IP security function.

If Enabled, user may access the converter switch only through the management station which has exact IP address specified in below IP address field.
If Disabled, user may access the converter switch through any management station.

IP Address: Specify the IP address used for IP Security function.

Console Level: Use ↑ or ↓ to select desired privilege for the console operation

Available operation privileges,

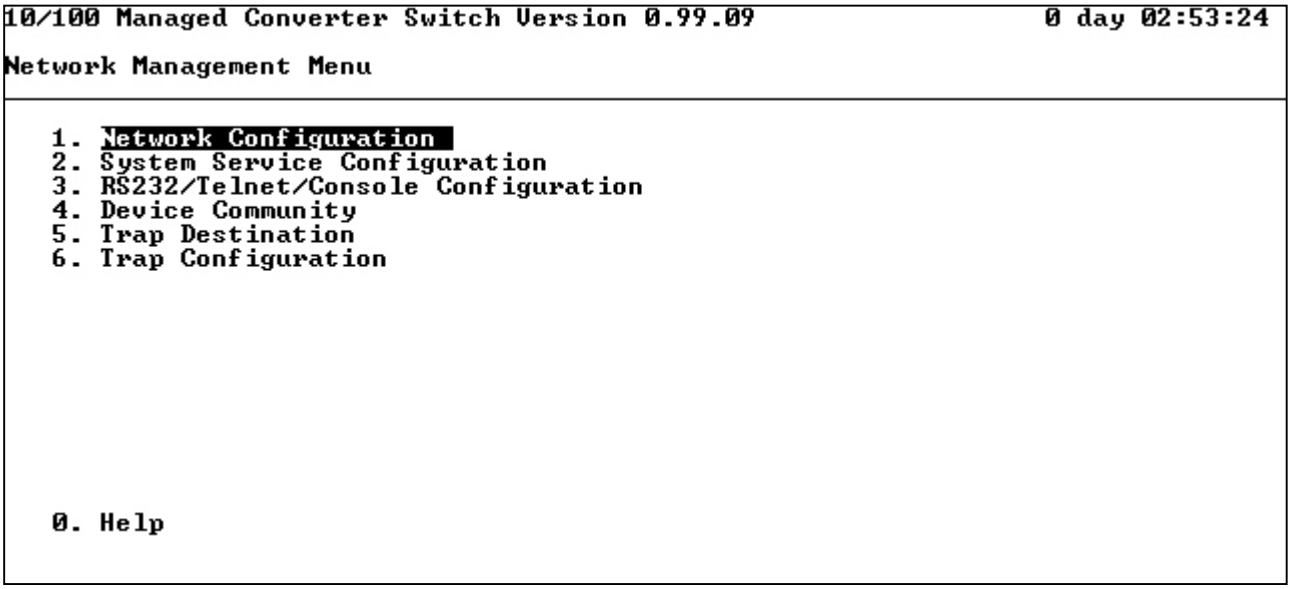
Administrator	Full access right include maintain user account & system information, load factory setting, …etc.
Read & Write	Full access right but cannot modify user account & system information, cannot load factory setting
Read Only	Allow to view only.
Access Denied	Complete forbid to access.

NOTICE:

To prevent un-caution operation, a user cannot Delete, Modify User Name or Enable/Disable himself.

2.7 Network Management

In order to enable network management of the converter switch, proper network configuration is required. To do this, select option **Network Management** from the Console main menu, following screen appears.



1. **Network Configuration:** Setup the required IP configuration of the converter switch.

2. **System Service Management:** Enable or Disable the specified network services.

3. **RS232/Telnet/Console Configuration:** View the RS-232 port setting, specified Telnet & Console services.

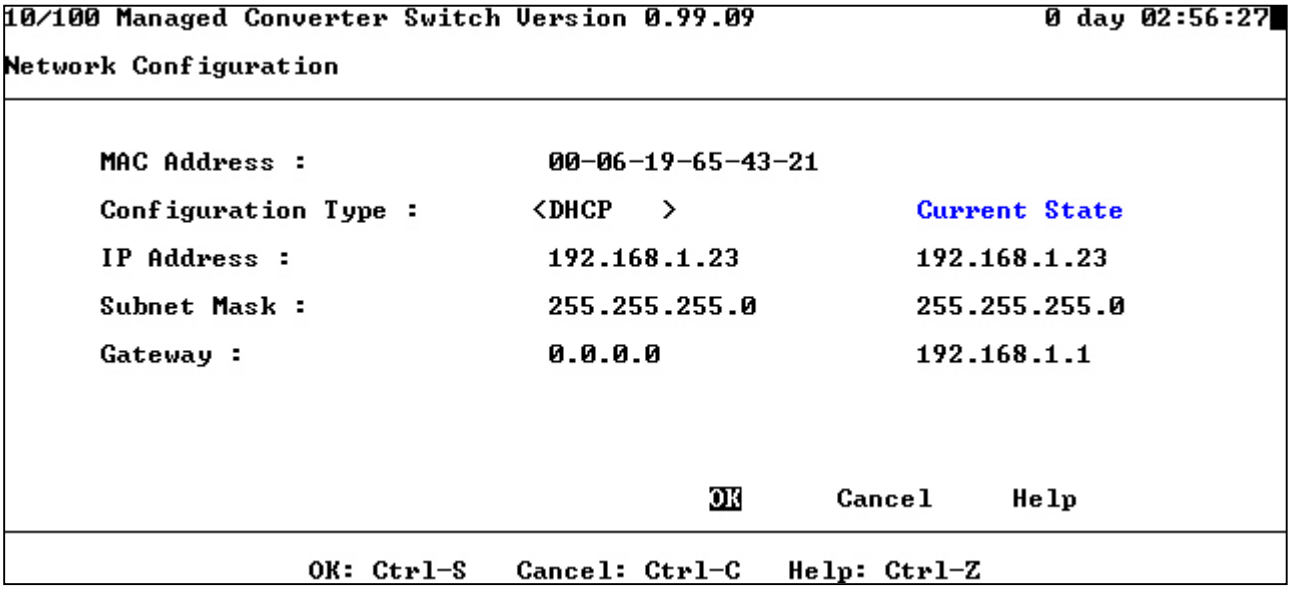
4. **Device Community:** View the registered SNMP community name list. Add a new community name or remove an existing community name.

5. **Trap Destination:** View the registered SNMP trap destination list. Add a new trap destination or remove an existing trap destination.

6. **Trap Configuration:** View the converter switch trap configuration. Enable or disable a specified trap.

2.7.1 Network Configuration

Select option **Network Configuration** from the Network Management menu, following screen appears.



MAC Address: This view-only field shows the unique and permanent MAC address assigned to the converter switch. You cannot change the converter switch MAC address.

Configuration Type: Press Spacebar to select using "DHCP" or "Manual". If select "**DHCP"** and a DHCP server also available on the network, the converter switch will automatic get the IP address from the DHCP server. If select the "**Manual"** mode, user need to specify the IP address, Subnet Mask & Gateway.

IP Address: Enter the unique IP address of this converter switch. You can use the default IP address or specify a new one if there is address duplication or the address does not match your network.

Subnet Mask: Specify the subnet mask to use with the converter switch IP address. The default subnet mask values for the three Internet address classes are as follows:

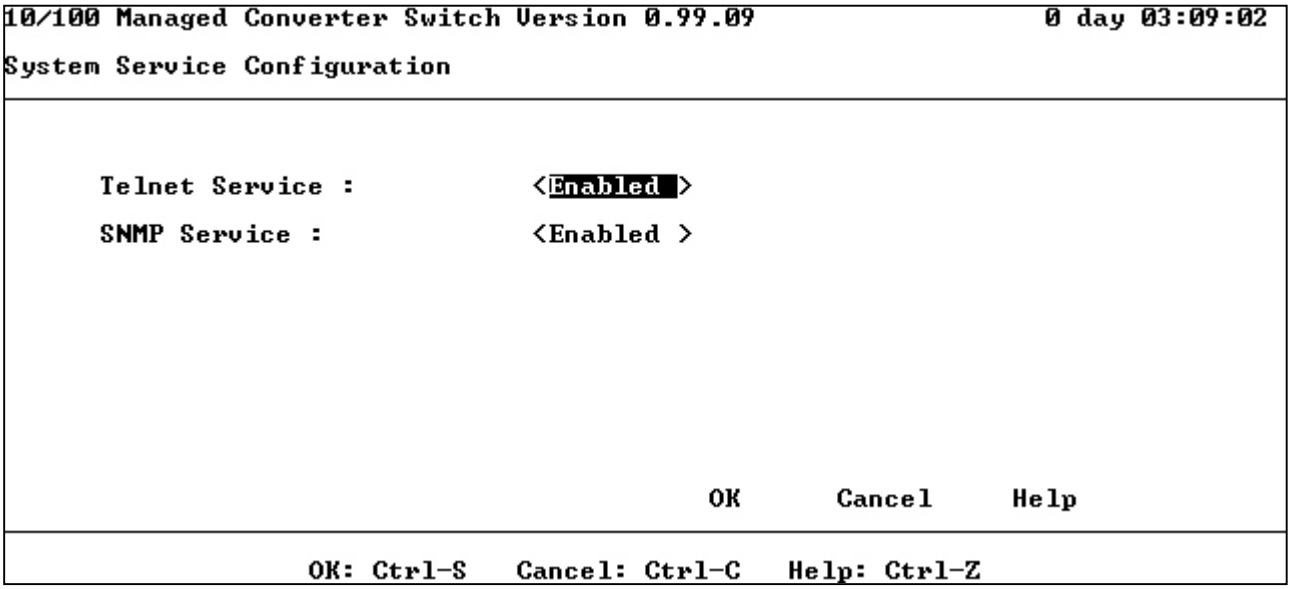
- Class A: 255.0.0.0
- Class B: 255.255.0.0
- Class C: 255.255.255.0

Gateway: Specify the IP address of a gateway or a router, which is responsible for the delivery of the IP packets sent by the converter switch. This address is required if the converter switch and the network management station are on different networks or subnets. The default value of this parameter is 0.0.0.0, which means no gateway exists and the network management station and converter switch are on the same network.

Current State: This view only field shows currently assigned (by DHCP or manual) IP address, Subnet Mask & Gateway of the converter switch.

2.7.2 System Service Management

Select option **System Service Management** from the Network Management menu, following screen appears.

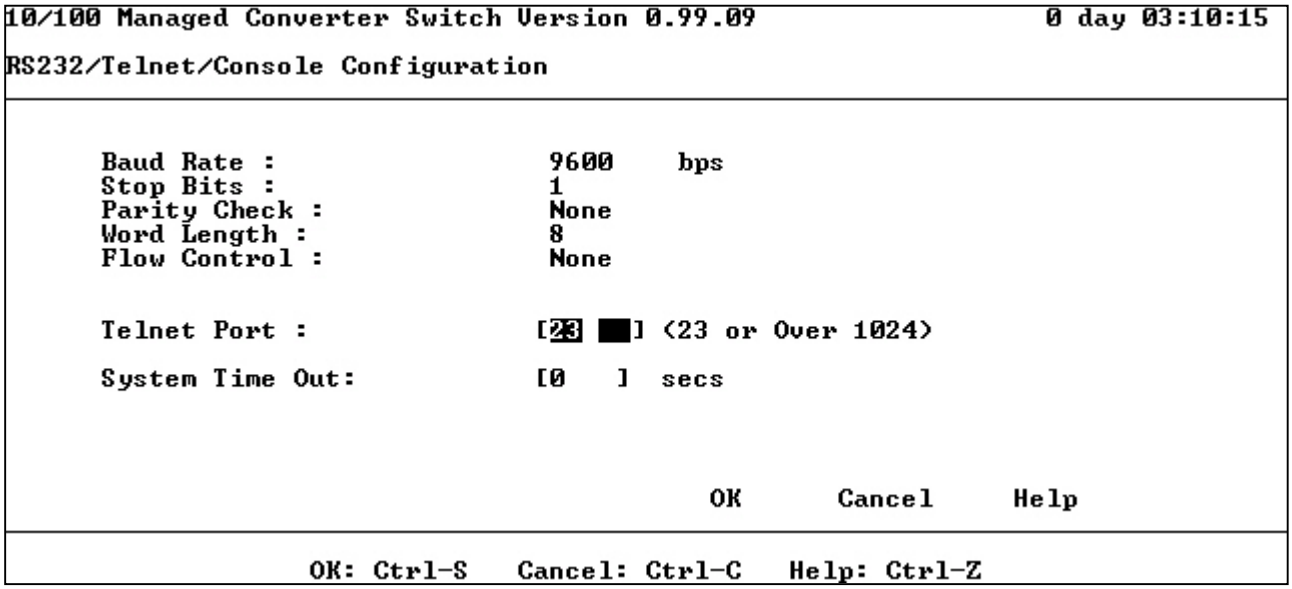


Telnet Service: Press Spacebar to Enable or Disable the Telnet service.

SNMP Service: Press Spacebar to Enable or Disable the SNMP service.

2.7.3 RS232/Telnet/Console Configuration

Select option **RS232/Telnet/Console Configuration** from the Network Management menu, following screen appears.



Baud Rate: 9600 bps, RS-232 setting, view only field.

Stop Bits: 1, RS-232 setting, view only field.

Parity Check: None, RS-232 setting, view only field.

Word Length: 8, RS-232 setting, view only field.

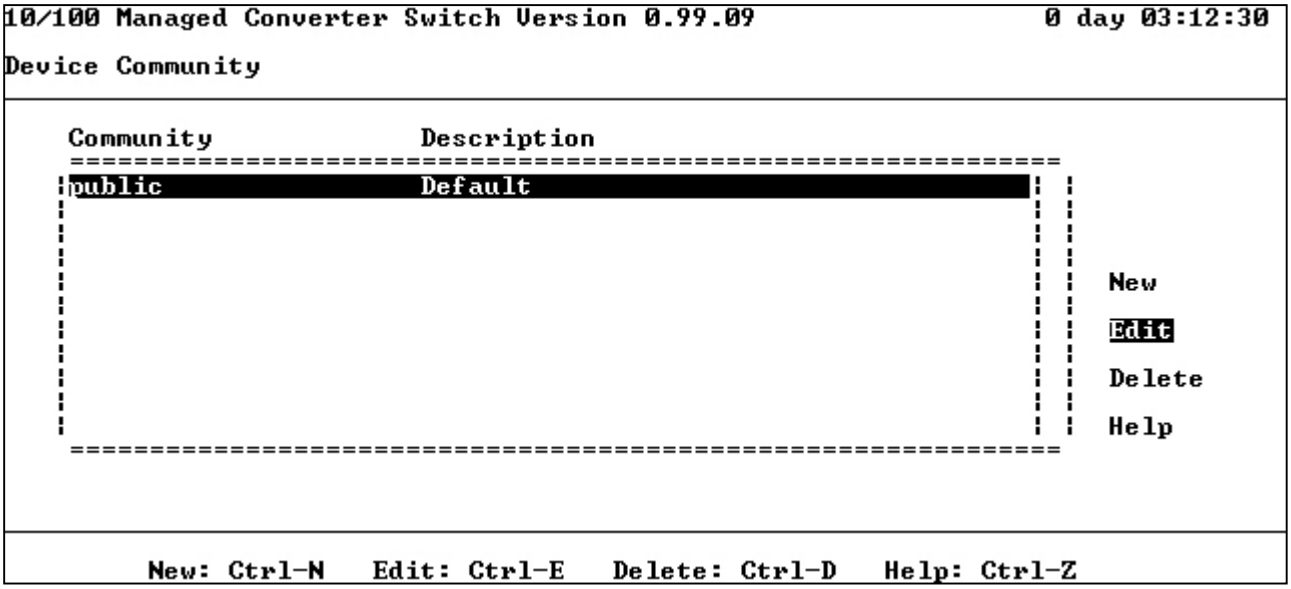
Flow Control: None, RS-232 setting, view only field.

Telnet Port: Specified the desired TCP port number for the Telnet console. Default TCP port number of the Telnet is 23.

System Time Out: Specified the desired times that the converter switch will wait before cut off an inactive console/telnet connection.
Specified "0" mean never cut off an inactive connection.

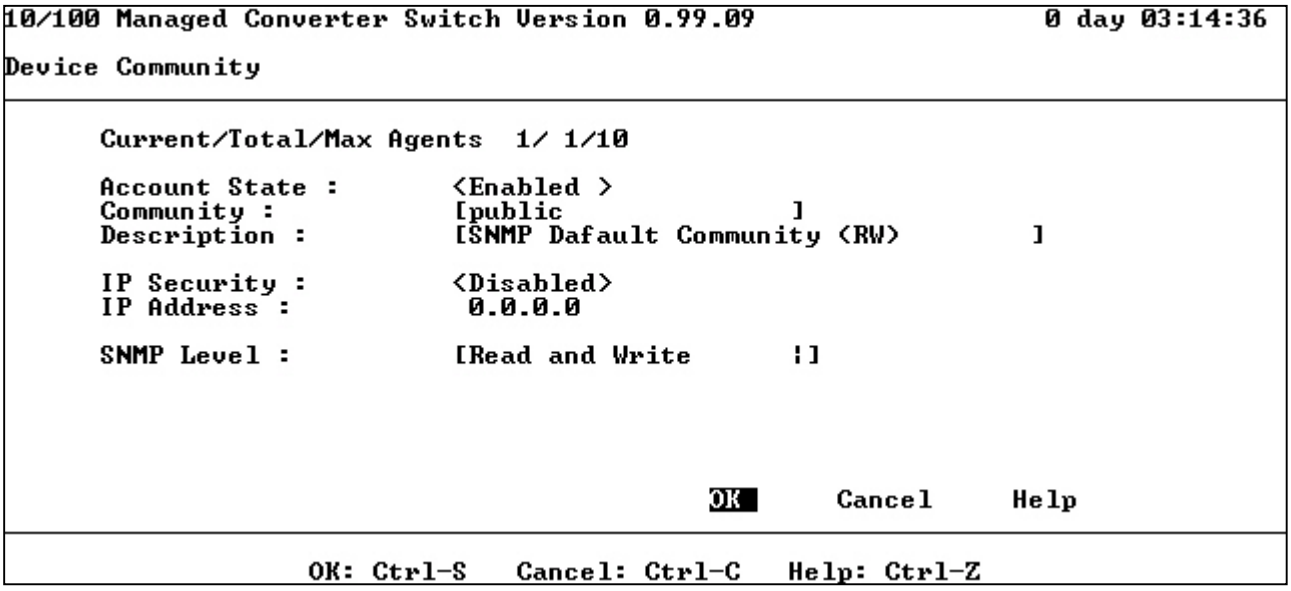
2.7.4 Device Community

Select option **Device Community** from the Network Management menu, following screen appears.



Up to 10 Device Community maybe set.

Use **Delete** to remove a registered community.
Press **New** to add a new community.
Press **Edit** to view the current community setting.
Following screen appears,



Current/Total/Max Agents: View only field. Specify:

Current:	Current registered community number.
Total:	Total registered community user number.
Max Users:	Maximum available registered community number, default 10.

Account State: Press Spacebar to Enable or Disable this Community Account.

Community: Specified the authorized SNMP community name, up to 20 alphanumeric characters.

Description: Enter a unique description for this community name, up to 35 alphanumeric characters. This is mainly for reference purpose only.

IP Security: Press Spacebar to Enable or Disable the IP security function.

If Enabled, Community may access the converter switch only through the management station, which has exact IP address specified in below IP address field.
If Disabled, Community may access the converter switch through any management station.

IP Address: Specify the IP address used for IP Security function.

SNMP Level: Use ↑ or ↓ to select desired privilege for the SNMP operation

Available operation privileges,

Administrator Full access right include maintain user account & system information, load factory setting, …etc.

Read & Write Full access right but cannot modify user account & system information, cannot load factory setting.

Read Only Allow to view only.

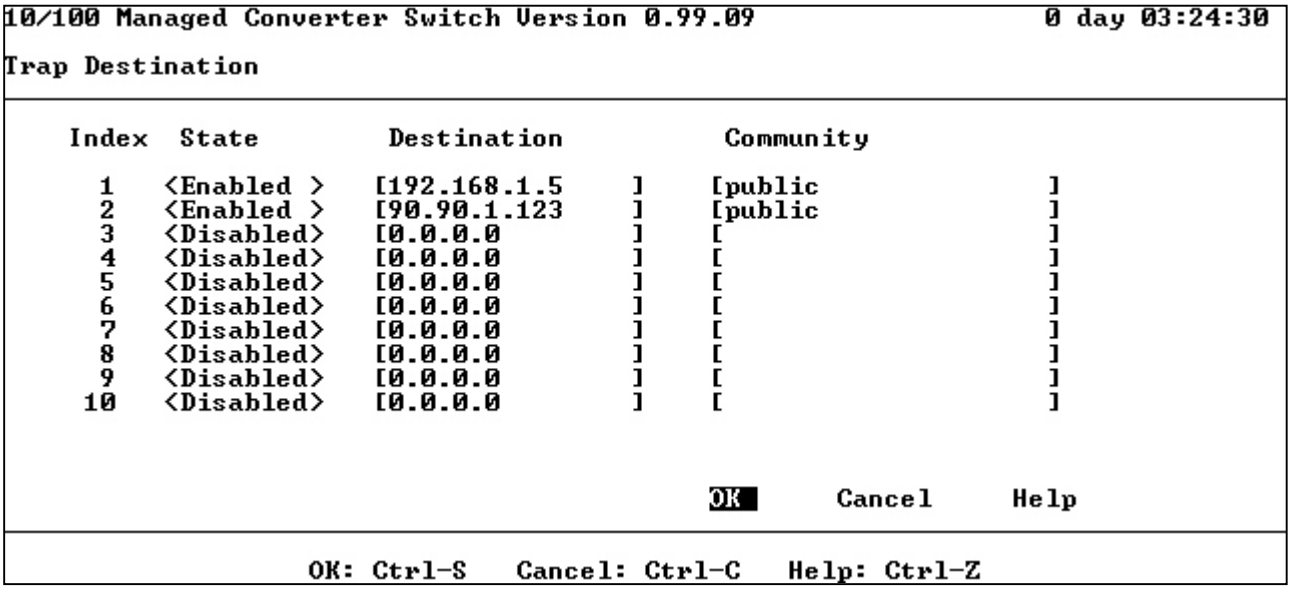
Access Denied Complete forbid to access.

NOTICE:

If the community browses the converter switch without proper access right, the converter switch will respond empty. For example, if a community only had Read & Write privilege then it cannot browse converter switch User table.

2.7.5 Trap Destination

Select option **Trap destination** from the Network Management menu, following screen appears.



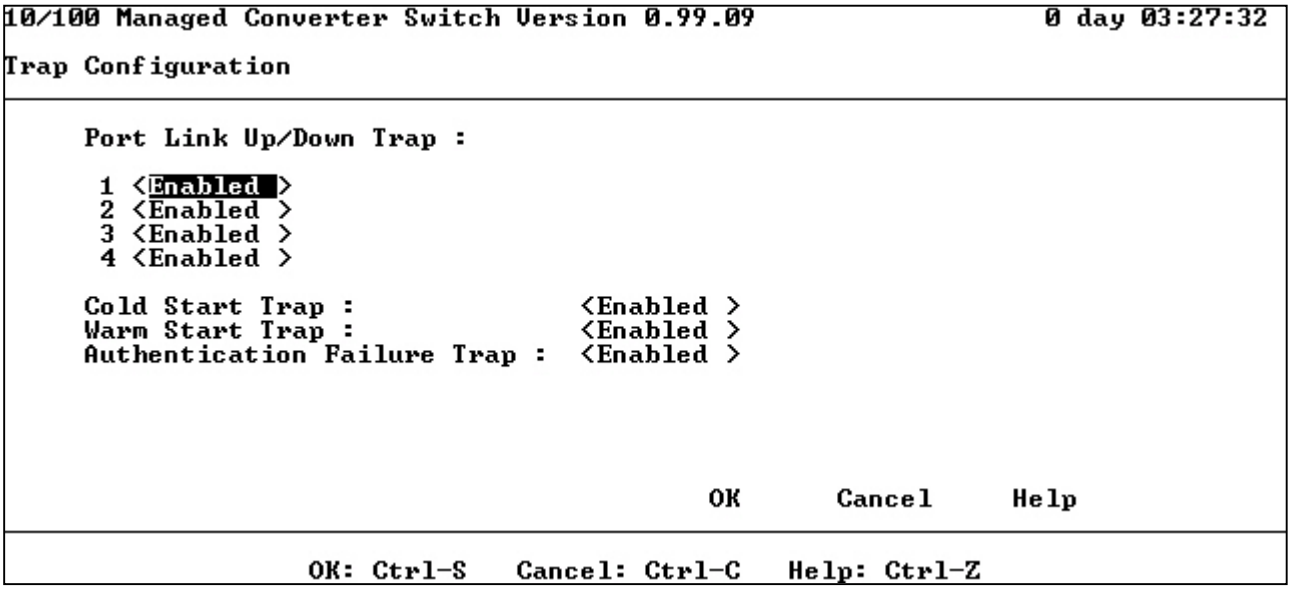
State: Enable or Disable to send Trap to the specified destination.

Destination: Enter the specified IP address of the network management system that will receive the trap.

Community: Enter the community name of the network management system.

2.7.6 Trap Configuration

Select option **Trap Configuration** from the Network Management menu, following screen appears.



Port Link Up/Down Trap: Enable or Disable the converter switch to send port link up/link down trap.

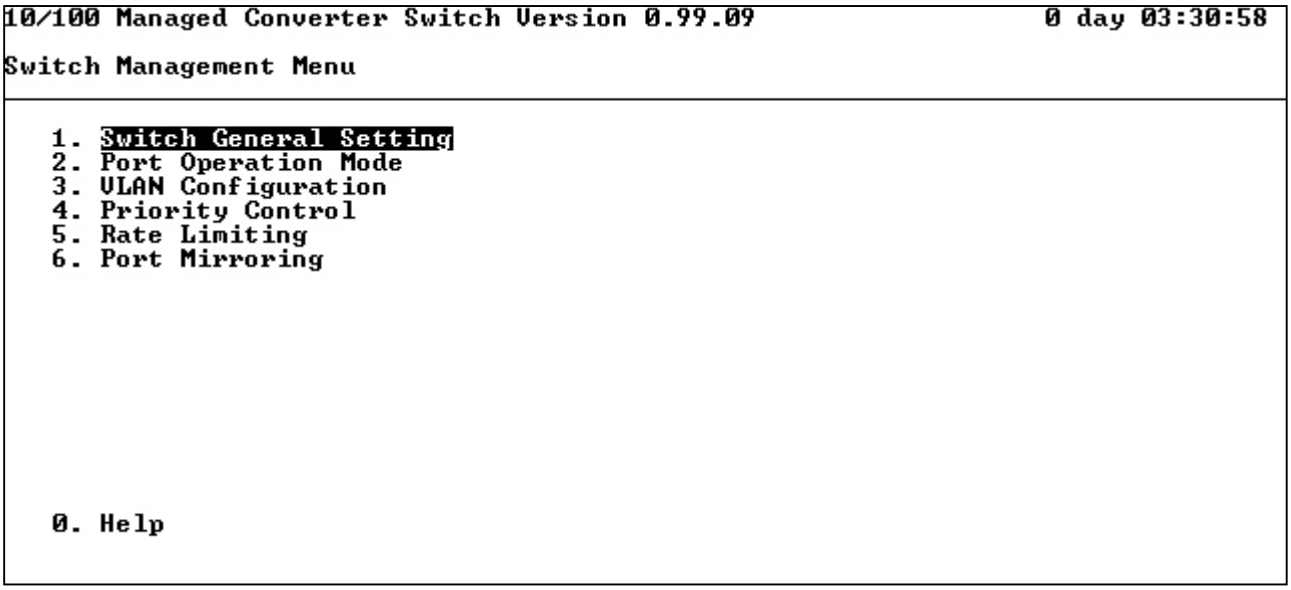
Cold Start Trap: Enable or Disable the converter switch to send Cold Start trap after power on.

Warm Start Trap: Enable or Disable the converter switch to send Warm Start trap after system reset.

Authentication Failure Trap: Enable or Disable the converter switch to send Authentication Failure trap after any unauthorized login attempt.

2.8 Switch Management

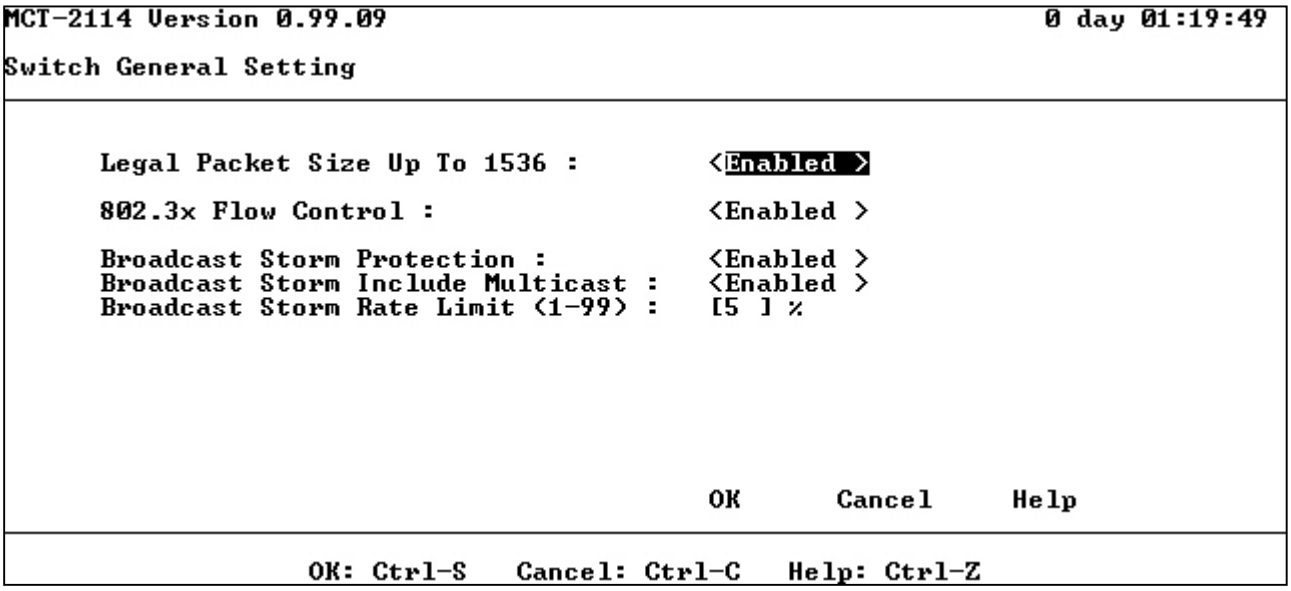
In order to manage the converter switch and setup required switching function, select option **Switch Management** from the Console main menu, following screen appears.



1. **Switch General Setting:** Setup acceptable frame size and flow control, …etc.
2. **Port Operation Mode:** Enable/Disable Port and setup Port Speed, …etc.
3. **VLAN Configuration:** Enable/Disable VLAN and setup VLAN configuration, …etc.
4. **Priority Control:** Enable/Disable Priority and setup Priority configuration, …etc.
5. **Rate Limiting:** Enable/Disable Rate Control and setup Rate control configuration.
6. **Port Mirroring:** Enable/Disable port mirroring and setup port mirroring configuration.

2.8.1 Switch General Setting

Select option **Switch General Setting** from the Switch Management menu, following screen appears.



Legal Packet Size Up to 1536: Press Spacebar to Enable or Disable this function.

If Enabled, acceptable frame size is up to 1536 Bytes.
If Disabled, acceptable frame size is up to 1522/1518 Bytes (with/without VLAN Tag).

802.3x Flow Control: Press Spacebar to Enable or Disable Flow control function.

Broadcast Storm Protection: Press Spacebar to Enable or Disable the Broadcast Storm Protection functions.

Broadcast Storm Include Multicast: Press Spacebar to Enable or Disable the take account of Multicast frame as Broadcast frame when Broadcast Storm Protection Active.

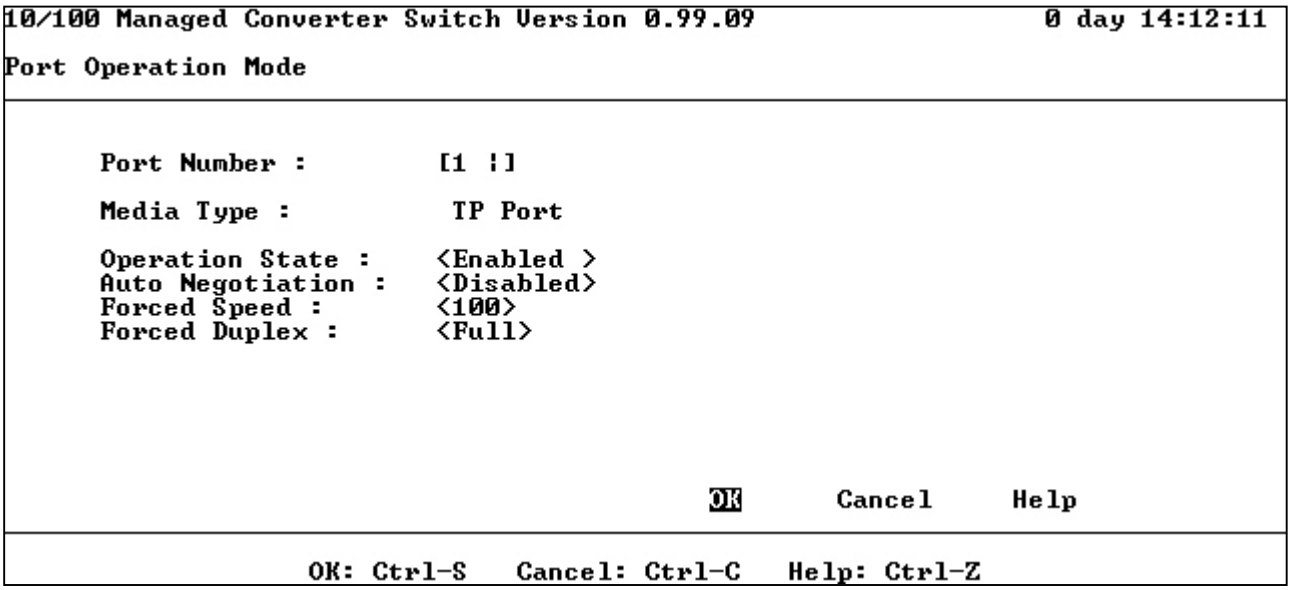
Broadcast Storm Rate Limit (1-99%): Enter the utilization rate of the broadcast frames. Broadcast storm Protection function will active when the threshold is reached.

Broadcast Storm

Broadcast Storm refers broadcast packets flooded and/or looped on a network causing noticeable performance degradation or even networks failure. Broadcast Storm can be caused by network loops, malfunctioning NIC, bad cable connections, and applications or protocols that generate broadcast traffic, among others. Network administrators usually use routers to divide the Broadcast Domain and prevent Broadcast storm occurrence.
Converter switch is able to limit the Broadcast Domain easier and cheaper than router by setting VLAN. Further, built-in broadcast storm sensors and filters allow converter switch provide even better protection to against Broadcast Storm. Broadcast Storm filter will active when the Broadcast Storm Rate Limit is reached.

2.8.2 Port Operation Mode

Select option **Port Operation Mode** from the Switch Management menu, following screen appears.



Port Number: Use ↑ or ↓ to move to desired port.

Media Type: View only field, indicate current port media.

Operation State: Press Spacebar to Enable or Disable the selected port.

Auto Negotiation: Press Spacebar to Enable or Disable RJ-45 Twisted Pair Port Auto Negotiation function.

Forced Speed: If Auto Negotiation is Disable, Press Spacebar to select the speed.

Forced Duplex: If Auto Negotiation is Disable, Press Spacebar to select the duplex mode.

Notice

Fiber port is always forced to operate at 100M, Full Duplex mode.

2.8.3 VLAN Configuration

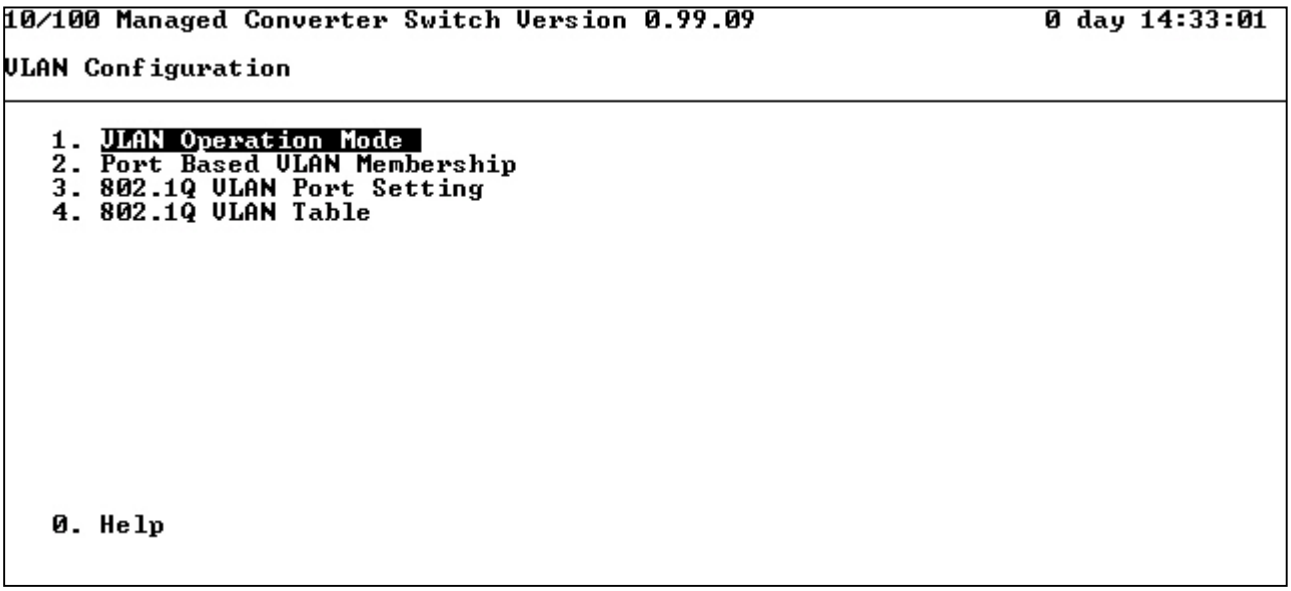
A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLAN can be used to combine any collection of LAN segments into a group that appears as a single LAN. VLAN also logically segment the network into different broadcast domains. All broadcast, multicast, and unknown packets entering the Switch on a particular VLAN will only be forwarded to the stations or ports that are members of that VLAN.

VLAN can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains. A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Another benefit of VLAN is that you can change the network topology without physically moving stations or changing cable connections. Stations can be 'moved' to another VLAN and thus communicate with its members and share its resources, simply by changing the port VLAN settings from one VLAN to another VLAN. This allows VLAN to accommodate network moves, changes and additions with the utmost flexibility.

The converter switch support 2 types of VLAN:

- Port Based
- 802.1Q Tag Base

Select option **VLAN Configuration** from the Switch Management menu, following screen appears.



1. **VLAN Operation Mode:** Enable/Disable VLAN function.

2. **Port Based VLAN Membership:** Setup Port Based VLAN configuration.

3. **802.1Q VLAN Port Setting:** Setup Port PVID, Tagged/Untagged, …etc.

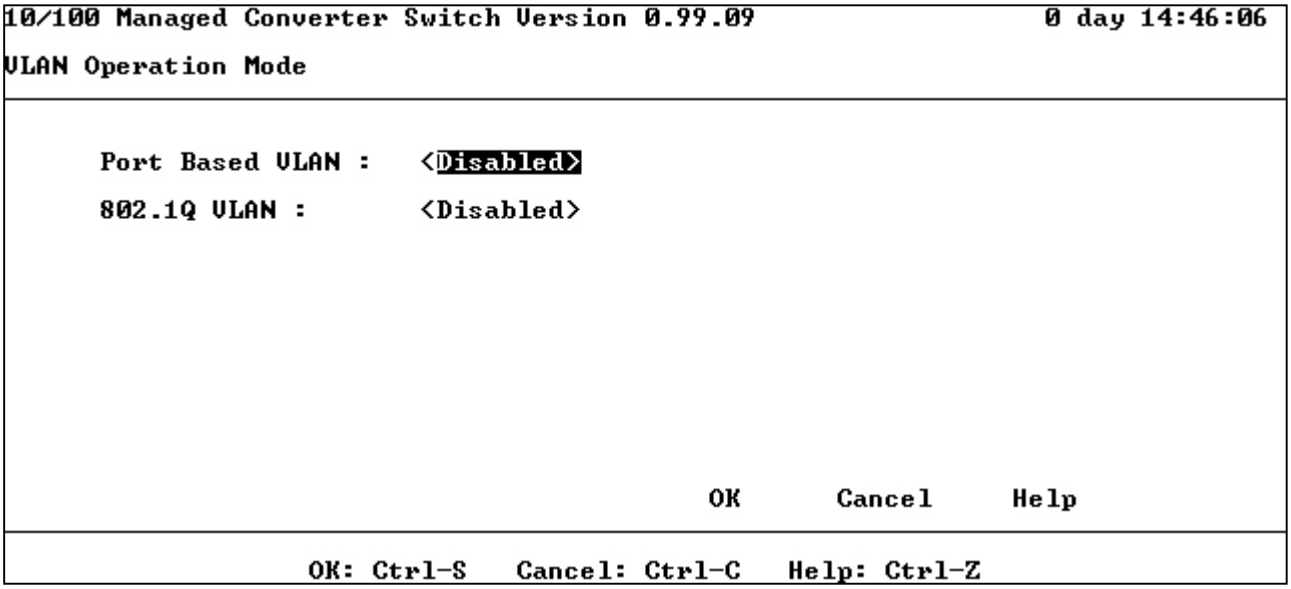
4. **802.1Q VLAN Table:** Setup 802.1Q VLAN VID, membership, …etc.

2.8.3.1 VLAN Operation Mode

The converter switch support 2 types of VLAN:

- Port Based
- 802.1Q Tag Base.

To Enable the VLAN function, first switch to **VLAN Configuration** screen then select **VLAN Operation Mode** and following screen appears,



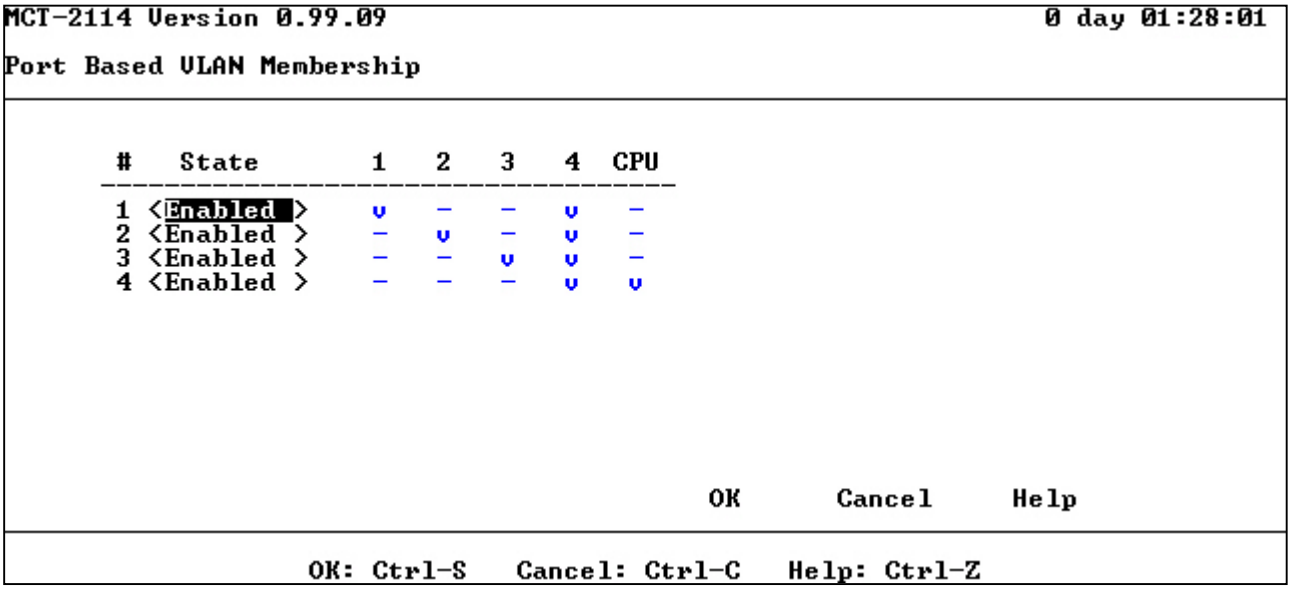
Port Based VLAN: Press Spacebar to Enable or Disable the Port Based VLAN function.

802.1Q: Press Spacebar to Enable or Disable the 802.1Q VLAN function.

2.8.3.2 Port Based VLAN Membership

Port-based VLAN can effectively segment one network into several Broadcast Domains, Broadcast/Multicast and unknown packets will be limited to within the VLAN. Port Based VLAN is uncomplicated and fairly rigid in implementation, it is best used for network administrators who wish to quickly and easily setup VLAN in order to isolate the effect of broadcast packets on their network

Select **Port Based VLAN Membership** from **VLAN Configuration** menu and following screen appears,



The converter switch supports 4 Port Based VLAN.

1 <Enable>: Toggle to Enable or Disable the selected Port Based VLAN.

Port Based VLAN Members:

1	2	3	4	CPU
V	V	V	V	-

Use <- or -> to move between the ports (Management Module refer as CPU),
Press Spacebar to toggle and assigned the membership.

"V" This port is this Port Based VLAN member.

"-" This port is not this Port Based VLAN member.

NOTICE

1. The built in management module of the converter switch is refer as CPU. For in-band management, network management port and CPU shall belong to the same Port Based VLAN.
2. Port Based VLAN can co-locate with 802.1Q VLAN. Further, Port Based VLAN has higher priority than 802.1Q VLAN.

2.8.3.3 802.1Q VLAN Port Setting

Port Based VLAN is simple to implement and use, but it cannot deploy cross switches VLAN. The 802.1Q protocol was developed in order to provide the solution. By tagging VLAN membership information to Ethernet frames, the IEEE 802.1Q can help a network administrator to break up large switched networks into smaller segments so that broadcast and multicast traffic won't grab too much of the available bandwidth, as well as providing a higher level of security between segments of internal networks.

The 802.1Q frame format is shown below,

PRE	SFD	DA	SA	TCI	P	C	VID	T/L	Payload	FCS

PRE	Preamble	62 bits Used to synchronize traffic
SFD	Start Frame Delimiter	2 bits Marks the beginning of the header
DA	Destination Address	6 bytes The MAC address of the destination
SA	Source Address	6 bytes The MAC address of the source
TCI	Tag Control Info	2 bytes set to 8100 for 802.1p and Q tags
P	Priority	3 bits Indicates 802.1p priority level 0-7
C	Canonical Indicator	1 bit Indicates if the MAC addresses are in Canonical format - Ethernet set to "0"
VID	VLAN Identifier	12 bits Indicates the VLAN (0-4095)
T/L	Type/Length Field	2 bytes Ethernet II "type" or 802.3 "length"
Payload		< or = 1500 bytes User data
FCS	Frame Check Sequence	4 bytes Cyclical Redundancy Check

Important VLAN Concepts for Configuration

There are two key components to understanding:

- The Default Port VLAN ID (**PVID**), which specifies the VLAN to which the switch will assign **unlabeled** traffic from that port;
- The VLAN ID (**VID**), which specify the set of VLAN from which a given port is allowed to receive, and to which allowed to send **labeled** packets.

Both variables can be assigned to a switch port, but there are important differences between them. An administrator can only assign one PVID to each switch port (since the 802.1Q protocol assigns any single packet to just one VLAN). The PVID defines the default VLAN ID tag that a switch will add to un-tagged frames it receives on that port (ingress traffic).

On the other hand, a port can be defined as a member of multiple VLAN (multiple VID). These VID constitute an access list for the port. The access list can be used to filter tagged ingress traffic (the switch will drop a packet tagged as belonging in one VLAN if the port on which it was received is not a member of that VLAN). The switch also consults the access list to filter packets it sends to that port (egress traffic). Packets will not be forwarded out the port if they unless they belong to one of the VLAN in which the port is a member.
The differences between **Ingress** and **Egress** configurations can provide network segmentation while still allowing resources to be shared across more than one VLAN.

Important VLAN Definitions

Ingress

The point at which a frame is received on a switch and the switching decisions must be made. The switch examines the VID (if present) in the received frames header and decides whether and where to forward the frame. If the received frame is untagged, the switch will tag the frame with the PVID for the port on which it was received. It will then use traditional Ethernet bridging algorithms to determine the port to which the packet should be forwarded.

Next it checks to see if each destination port is on the same VLAN as the PVID and can thus transmit the frame. If the destination port is a member of the VLAN used by the ingress port, the frame will be forwarded. If the received frame is tagged with VLAN information, the switch checks its address table to see whether the destination port is a member of the same VLAN. Assuming both ports are members of the tagged VLAN, the frame will be forwarded.

Ingress Filtering

The process of checking an incoming frame and comparing its VID to the ingress port VLAN memberships is known as Ingress Filtering.

On the switch, it can be either *enabled* or *disabled* on a port-by-port basis.

1. An **untagged** frame is received, the **ingress** port **PVID** is applied to the frame.
2. If a **tagged** frame is received, the **VID** in the frame tag is used.

If Ingress Filtering is *enabled* and, the switch will first determine,

1. If the **ingress** port itself is a member of the frame VLAN and can thus receive the frame.
2. If the **ingress** port is not a member of the frame VLAN, the frame is dropped.
3. If it is a member of that VLAN, the switch then checks its address table to see whether the destination port is a member of the same VLAN. Assuming both ports are members of that VLAN, the frame will be forwarded.

Administrators should take care to make sure that each port **PVID** is setup, or incoming frames may be dropped if **Ingress Filtering** is enabled. If **Ingress Filtering** is *disabled*, it will not compare the incoming frame **VID** against the **ingress** port VLAN membership; it will only check its address table to see whether the destination VLAN exists.

1. If the VLAN is unknown, it will be dropped.
2. If the VLAN and the destination MAC address are known, the frame will be forwarded.
3. If the VLAN is known and the destination MAC address is unknown, the frame will be flooded to all ports in the VLAN.

Egress

The point at which frames are being transmitted out of a switch and tagging decisions must be made. When an administrator configures each port VLAN membership (allows egress for a specific VLAN), another configuration option is whether to transmit tagged or untagged frames on that port.

1. If an egress port is connected to an 802.1Q-compliant switch or end system, tagging should be enabled so the other device can utilize the VLAN and priority tags.
2. If an egress port is connected to a non-compliant switch or end-station, the tags should be stripped off and the frame transmitted untagged so that the receiving device can read the normal Ethernet frame.

Tagging

Every port on an 802.1Q compliant switch can be configured as *tagging* or *untagging.*

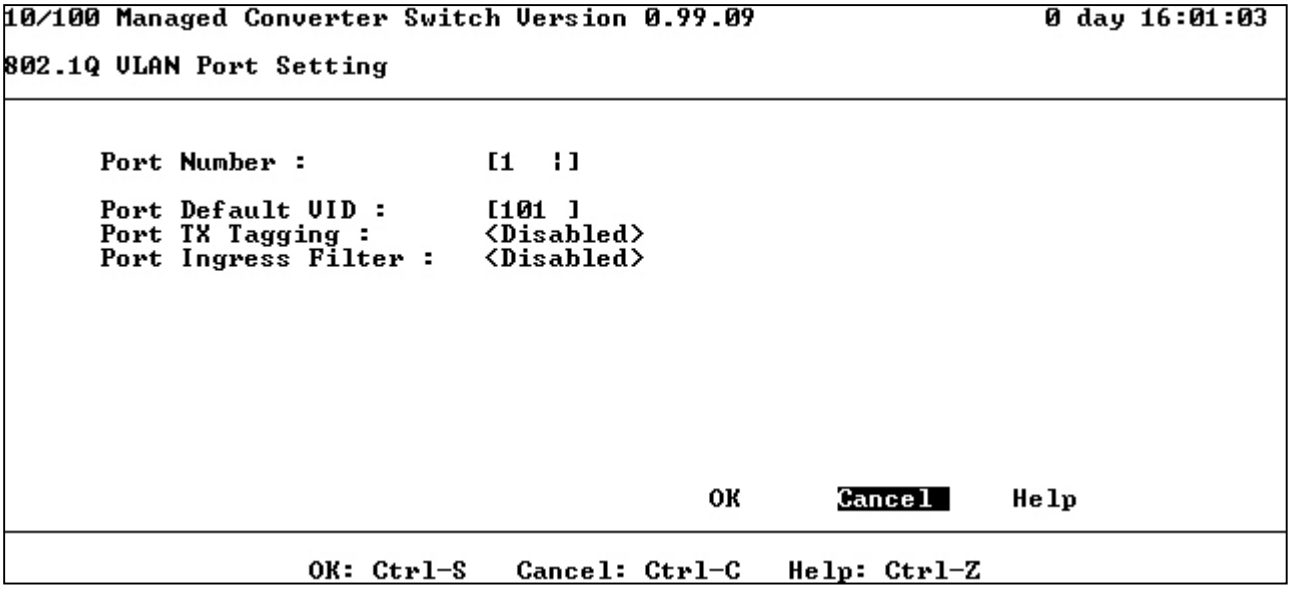
Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into and out of it. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. The VLAN information in the tag can then be used by other 802.1Q compliant devices on the network to make packet forwarding decisions.

Untagging

Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into and out of those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Setup Port for 802.1Q VLAN

To setup port for 802.1Q VLAN, first switch to **VLAN configuration** screen and then select **802.1Q VLAN Port Setting,** following screen appears,



Port Number: Use ↑ or ↓ to move to desired port.

Port Default VID: Enter the pre-assigned PVID.

When port is receiving an untagged frame, a VLAN Tag (VID = PVID) will be attached.

Port TX Tagging: Press Spacebar to Enable or Disable the Tagging function.

If Disabled, all output frames will be untagged frames.
If Enabled, all output frames will be tagged frames.

If the port is attached to a device that is not IEEE 802.1Q VLAN compliant, then the port should set to Untagged.

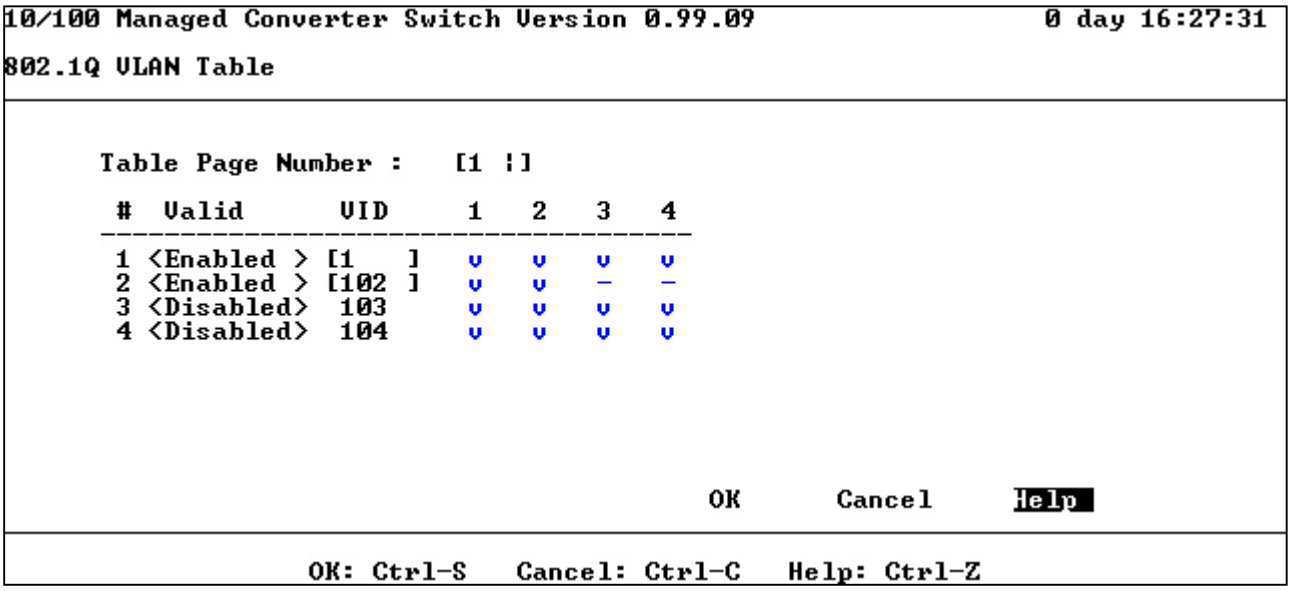
Port Ingress Filter: Press Spacebar to Enable or Disable the Ingress Filter function.

If Enabled,
When a packet arrives, the port will check the VID of the packet and its own VLAN membership. If the port also belongs to that VLAN, the frame will receive and forward. If the port is not a member of the VLAN, the packet will be discarded.

If Disabled,
When a packet arrives, the port will not check the VID of the packet and its own VLAN membership.

2.8.3.4 802.1Q VLAN Table

To setup 802.1Q VLAN, first switch to **VLAN configuration** screen and then select **802.1Q VLAN Table,** following screen appears,



The converter switch supports 16 802.1Q VLAN.

Table Page Number: Use ↑ or ↓ to move between pages, total 4 pages.

 # 1, 2, 3, 4: Index of the defined 802.1Q VLAN.

Valid: Press Spacebar to Enabled or Disabled this VLAN.

VID: Enter the assigned VID of this VLAN.

VLAN Members:

1	2	3	4
V	V	V	-

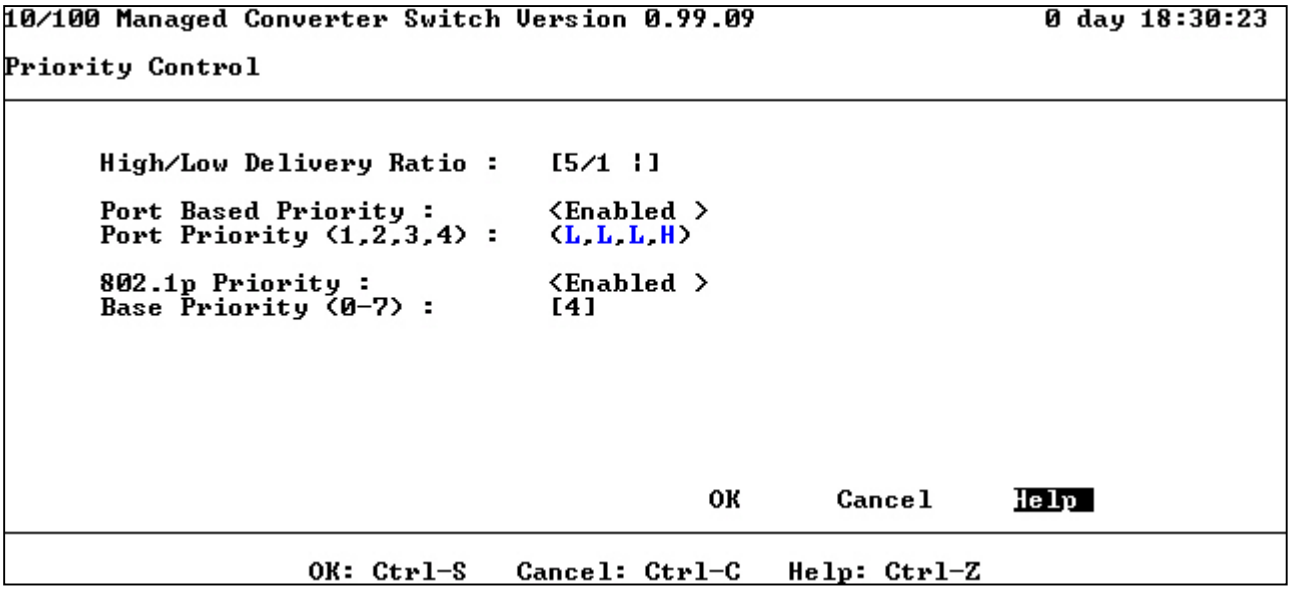
Use <- or -> to move between the ports,
Press Spacebar to toggle and assigned the membership.

"V" This port is this 802.1Q VID VLAN member.

"-" This port is this 802.1Q VID VLAN member.

2.8.4 Priority Control

The converter switch support both Port Based and 802.1P Based Priority functions, select option **Priority Control** from the Switch Management menu, following screen appears,



High/Low Delivery Ratio: Use ↑ or ↓ to select desired High/Low priority queue processing ratio. Available options are 2/1, 5/1, 10/1 and most.

High/Low Priority Queue

If Enable priority control function, the converter switch internal packet queue can be further divided into High and Low Priority Queues. The High/Low Delivery Ratio is used to decide how to process packets within these queues. Ratio 2/1 mean it will deliver 2 packets within the High Priority Queue first than deliver 1 packet within the Low Priority Queue.

Port Based Priority: Press Spacebar to Enable or Disable the Port Based Priority function.

Port Priority (1, 2, 3, 4): (L, L, L, H)

Use <- or -> to move between the ports,
Press Spacebar to toggle and assigned the port priority.

H High Priority, received frames will put into High Priority Queue

L Low Priority, received frames will put into Low Priority Queue

802.1P Priority: Press Spacebar to Enable or Disable the 802.1P Priority function. If Enable, VLAN Tag 3 bits priority field will be used to determine the delivery priority.

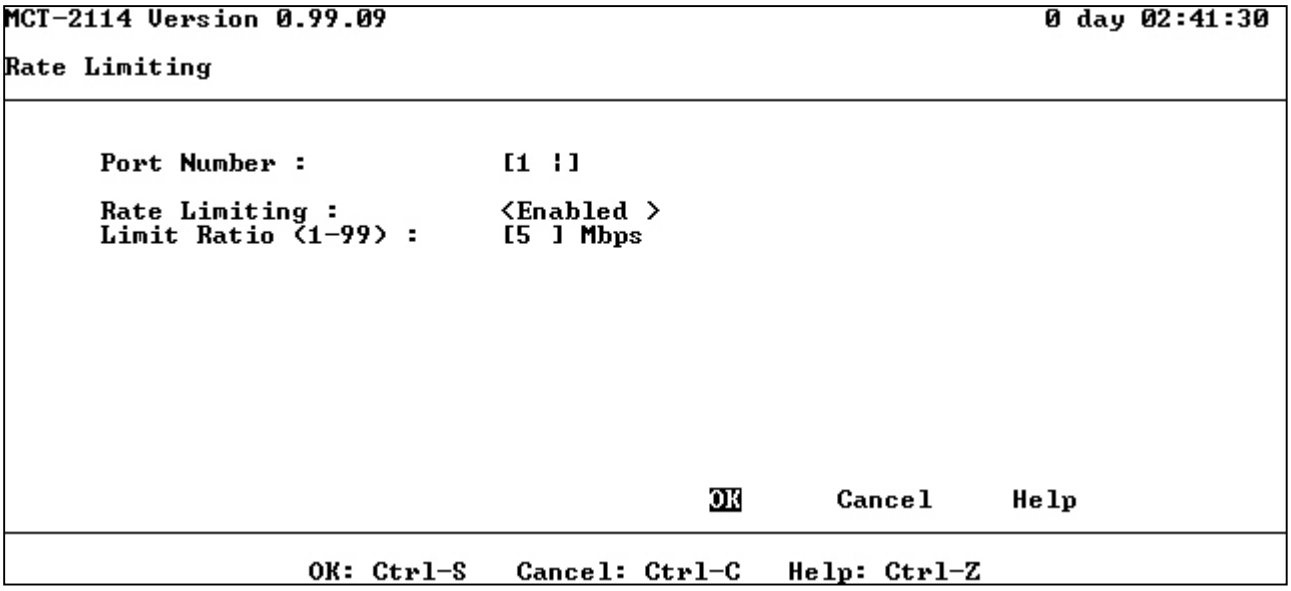
If Enable, 802.1P priority will over Port Based Priority.

Base Priority (0 - 7): Specified the threshold for 802.1P Priority Control, received frames with equal or higher priority will be put into High Priority Queue.

2.8.5 Rate Limiting

The converter switch support advanced Rate Control function to each port. When rate limit function is enabled, a port will only process specified amount of traffic. All traffic excess the rate control limitation will be discarded.

To setup Rate Limiting, select option **Rate Limiting** from the Switch Management menu, following screen appears,



Port Number: Use ↑ or ↓ to select Port for rate control.

Rate Limiting: Press Spacebar to Enable or Disable the selected Port rate control function.

Limit Ratio (1-99): [xxx] Mbps

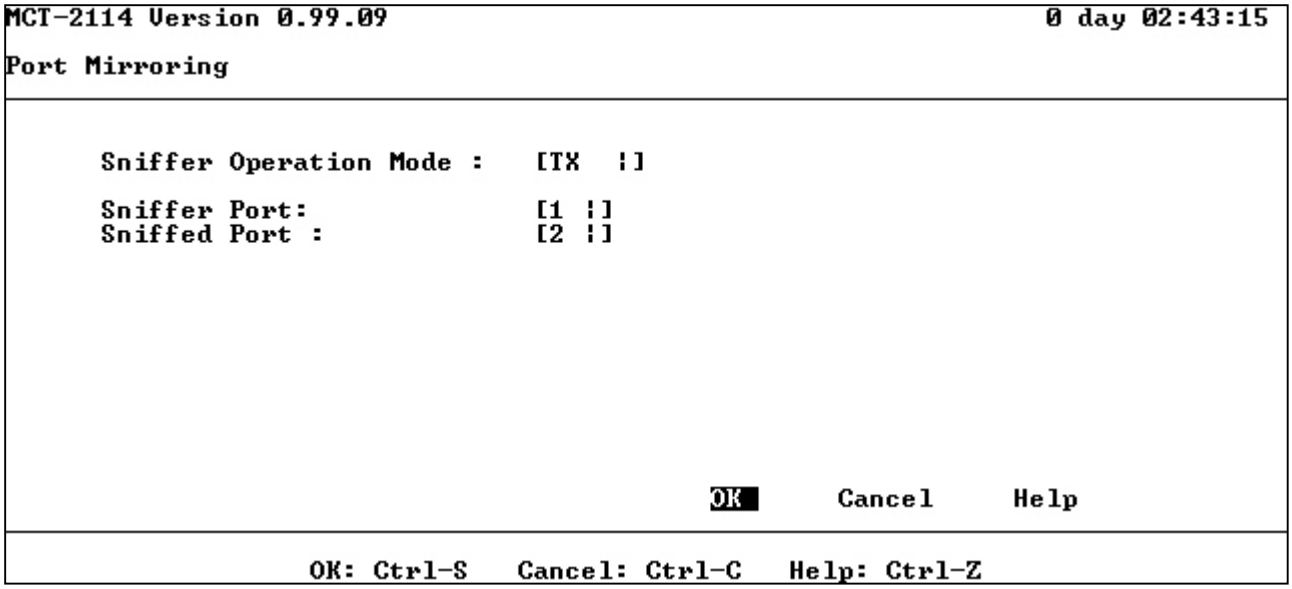
Enter the desired number for rate control.

The Limit Ratio of each port will take effect on both transmit and receive frames.

2.8.6 Port Mirroring

Port mirroring mean all frames transmitted and received on one port can be monitored from another port. You can attach a monitoring device to the mirrored port, such as a protocol analyzer or an RMON probe, to view the details about the frames passing through. This is useful especially for network monitoring and troubleshooting purposes.

Select option **Port Mirroring** from the Switch Management menu, following screen appears.



Sniffer Operation Mode: Use ↑ or ↓ select desired mirroring operation.

Option available,

None The Port Mirroring function is disabled.

TX Only The Sniffer port will monitor the Sniffed port transmit out frames only.

RX Only The Sniffer port will monitor the Sniffed port receive in frames only

Sniffer Port: Use ↑ or ↓ select the port as monitor port.

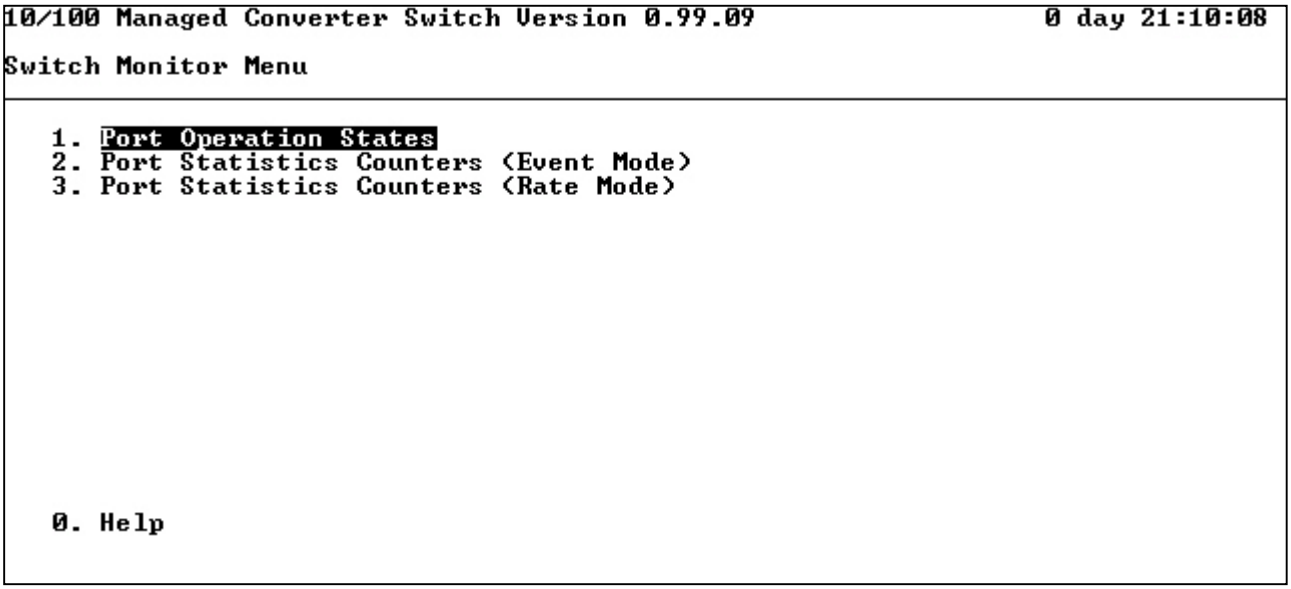
Sniffed Port: Use ↑ or ↓ select the port to be monitored.

Notice

Sniffer and Sniffed ports should work on the same operation mode.

2.9 Switch Monitor

Switch monitor allow user to monitor the real time operation status of the converter switch. User may monitor the port link up status or traffic counters for maintenance or diagnostic purpose. Select option **Switch Monitor** from the Console main menu, following screen appears.



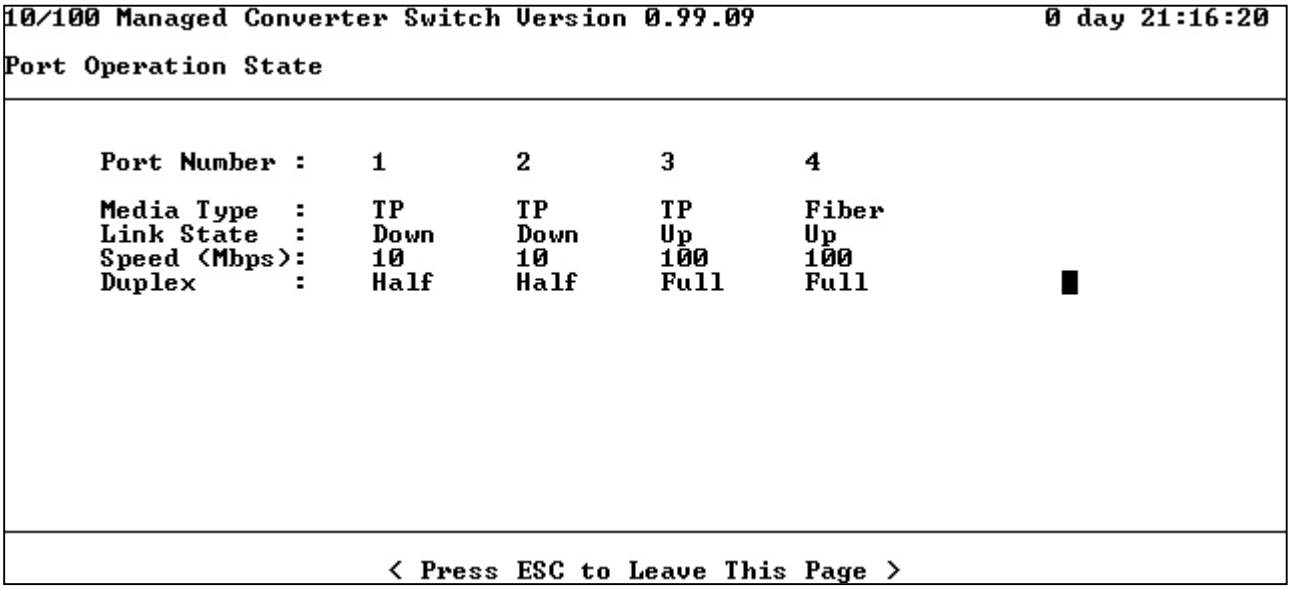
1. **Port Operation States:** View current port speed and duplex, …etc**.**

2. **Port Statistics Counters (Event Mode):** View the traffic condition of port, counters are calculated since the last time that counter was reset or cleared**.**

3. **Port Statistics Counters (Rate Mode):** View the traffic condition of port, counters are calculated base on the number of events per second at which the events happen.

2.9.1 Port Operation State

In order to view the real time port status of the switch, select **Port Operation State** from the Switch Monitor menu, following screen appears,



Port Number: The number of the port.

Media Type: The media type of the port; could be TP or Fiber.

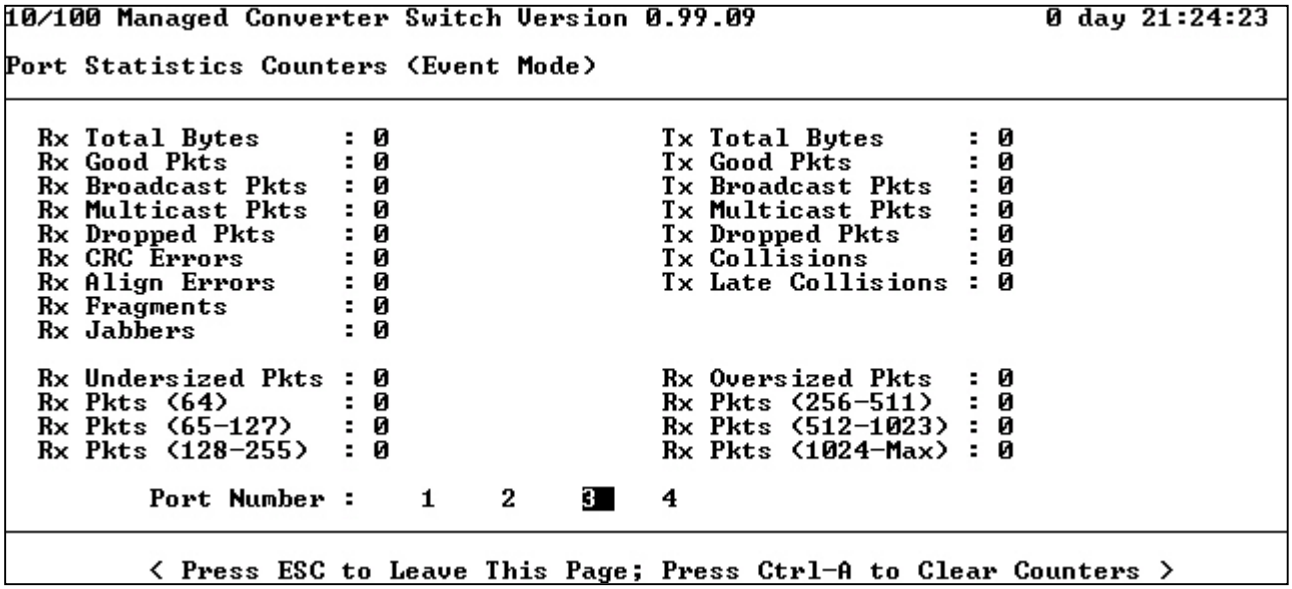
Link State: The current link status of the port, could be Up or Down.

Speed (Mbps): The current operation speed of the port, could be 10 or 100.

Duplex: The current operation Duplex mode of the port, could be Full or Half.

2.9.2 Port Statistics Counters (Event Mode)

Port Statistics Event Mode Counters allow viewing the traffic history of the converter switch, Event Mode counters are calculated since the last time that counter was reset or cleared. Select **Port Statistics Counters (Event Mode)** from the Switch Monitor menu, following screen appears,



Port Number: 1 2 3 4
Use <- & -> arrow keys select the port to view.

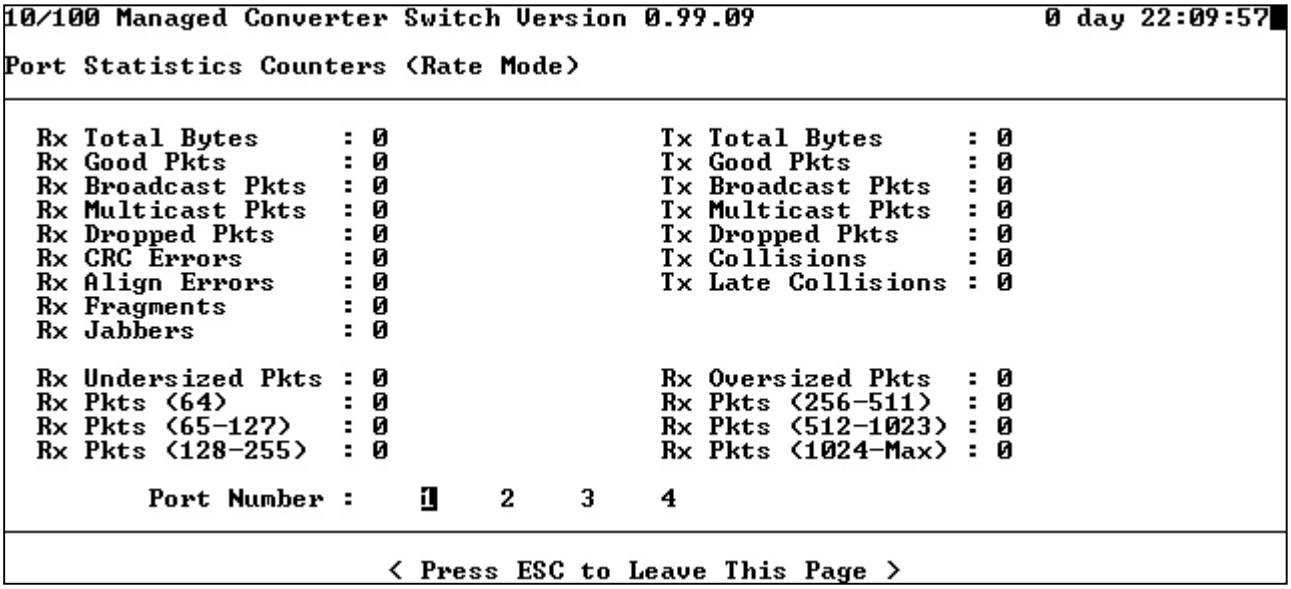
Ctrl-A: Press Ctrl-A will clear all port's counter values back to zero.

RX Total Bytes:	Total bytes of all received packets.
RX Good Pkts:	Total good packets received.
RX Broadcast Pkts:	Total Good Broadcast packets received.
RX Multicast Pkts:	Total Good Multicast packets received.
RX Dropped Pkts:	Total received packets dropped due to resources shortage.
RX CRC Errors:	Total received packets with CRC error.
RX Align Errors:	Total received packets with Alignment error.
RX Fragments:	Total packets received which were less than 64 bytes or packet without SFD and are less than 64 bytes in length.
RX Jabbers:	Total packets received had both Oversize & CRC error.
RX Undersized Pkts:	Total packets received shorter than 64 bytes.
RX Oversized Pkts:	Total packets received longer than maximum frame size.
RX Pkts (64):	Total 64 bytes packets received.
RX Pkts (65 - 127):	Total 65 - 127 bytes packets received.
RX Pkts (128 - 255):	Total 128 - 255 bytes packets received.
RX Pkts (256 - 512):	Total 256 - 512 bytes packets received.
RX Pkts (512 - 1023):	Total 512 - 1023 bytes packets received.
RX Pkts (1024 - Max):	Total 1024 - Maximum Frame size packets received.

TX Total Bytes:	Total bytes of all transmitted packets.
TX Good Pkts:	Total Good packet transmitted.
TX Broadcast Pkts:	Total Broadcast packets transmitted.
TX Multicast Pkts:	Total Multicast (not include Broadcast) packets transmitted.
TX Dropped Pkts:	Total packets not transmitted due to resources shortage.
TX Collisions:	Total collision detected.
TX Late Collisions:	Total late collision detected. Late Collision: Collision occurred after 512 bits time.

2.9.3 Port Statistics Counters (Rate Mode)

Port Statistics Rate Mode Counters allow viewing the real-time traffic condition of the converter switch. Rate mode counters are calculated base on the number of events per second at which the events happen. Select **Port Statistics Counters (Rate Mode)** from the Switch Monitor menu, following screen appears,



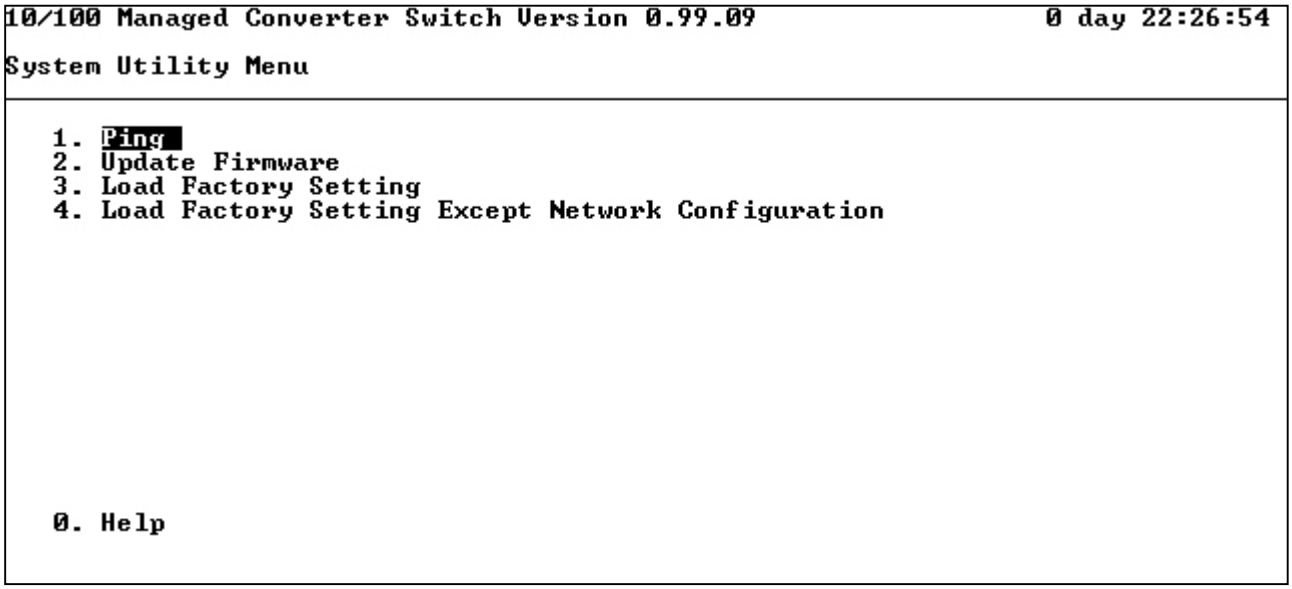
Port Number: 1 2 3 4
Use <- & -> arrow keys select the port to view.

Notice

Please refer Port Statistics Counters (Event Mode) for counters definition.

2.10 System Utility

System Utility allow user easy to operate and maintain the system. Select option **System Utility** from the Console main menu, following screen appears.



1. **Ping:** Ping allow user to ping a specified network device.

2. **Update Firmware:** Allow user to update the latest firmware, save current configuration, or restore previous configuration to the converter switch.

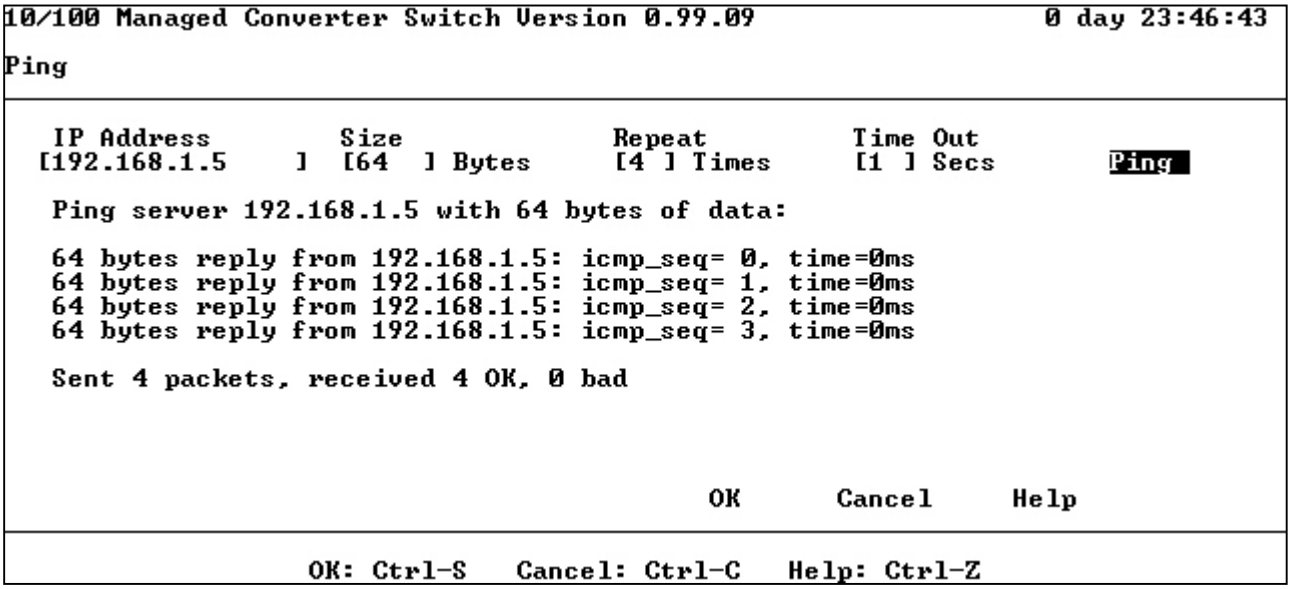
3. **Load Factory Setting:** Load Factory Setting will return the configuration of the converter switch to the factory default settings. The IP and Gateway addresses will also return to the factory default.

4. **Load Factory Setting Except Network Configuration:** Select this will also return the configuration of the converter switch to the factory default settings. However, this will not return the IP and Gateway addresses to the factory default.

2.10.1 Ping

Ping refer to ICMP Echo Request, a device receive the Ping request will respond with an ICMP Echo Reply. The converter switch built in Ping function allow network administrator easily identify the network connection.

Select **Ping** from the System Utility menu, following screen appears,



IP Address: Enter the desired IP address that the converter switch will Ping.

Size: Enter the desired length of the Ping packets.

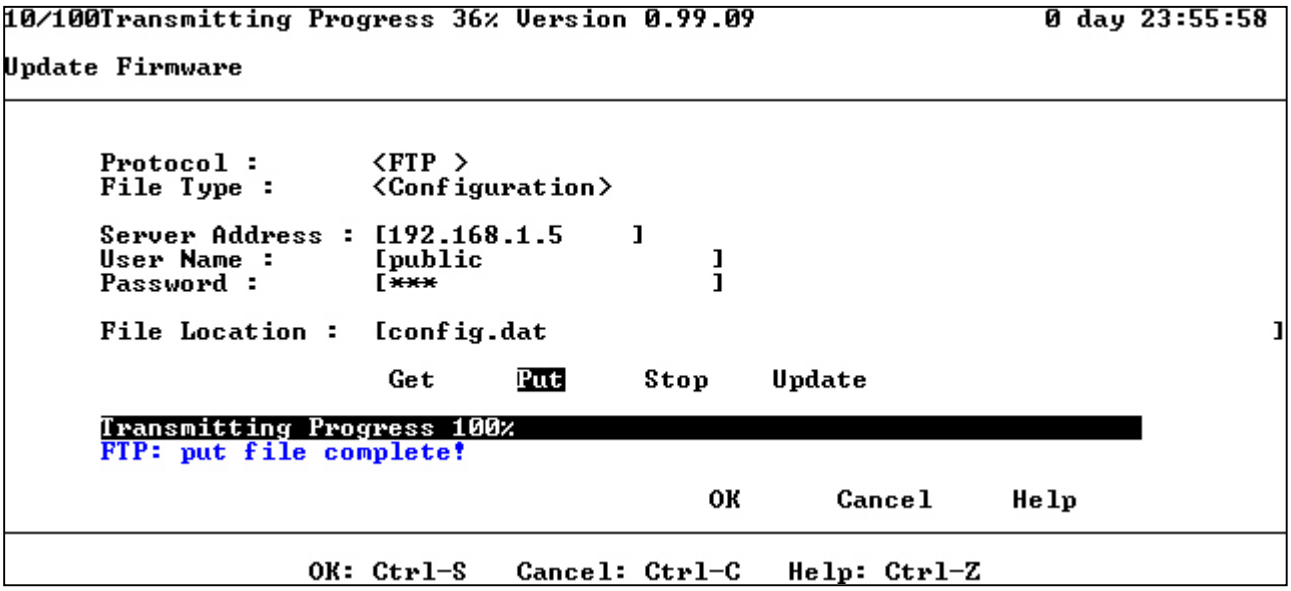
Repeat: Enter the total times of Ping will issued.

Time Out: Enter the desired time out value of Ping.

After finish configuration, select **Ping** then press **Enter** to start the Ping process.

2.10.2 Update Firmware

The converter switch has built-in both TFTP and FTP clients. User may save or restore their configuration and update their Firmware on line. Select **Update Firmware** from the System Utility menu, following screen appears,



Protocol: Press Space Bar to select preferred protocol - FTP or TFTP.

File Type: Press Space Bar to select the file to process - Firmware or Configuration.

Server Address: Enter the specified IP address of the File Server.

User Name: Enter the specified User Name for Log In the File Server.

Password: Enter the specified Password for Log In the File Server.

File Location: Enter the specified path & file name within the File Server.

Select **Get** then press **Enter** to start the download process - receive file from the server.
A Transmitting Progress will display during transfer.
A complete message will pop up to advise the user.

Select **Put** then press **Enter** to start the upload process - transmit file to the server.
A Transmitting Progress will display during transfer.
A complete message will pop up to advise the user.

Select **Stop** then press **Enter** to abort current operation.

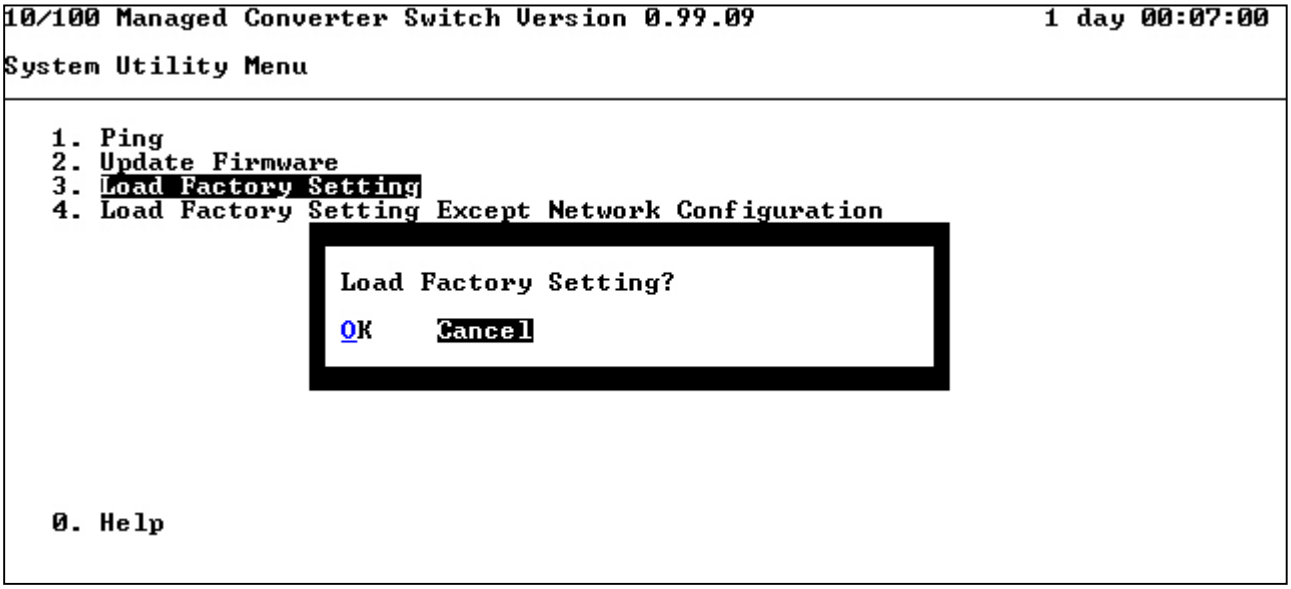
Select **Update** then press **Enter** to instruct the converter switch update existing firmware/configuration to the newest received firmware/configuration. After an Update Success message pop up, the switch will need to reset to take change effect.

2.10.3 Load Factory Setting

Load Factory Setting will return all the configuration of the converter switch to the factory default settings include the IP and Gateway address. Load Factory Setting is useful when network administrator like to re-configure the system.

A system reset is required to put all changes effect after Load Factory Setting.

Select **Load Factory Setting** from the System Utility menu, following screen appears,



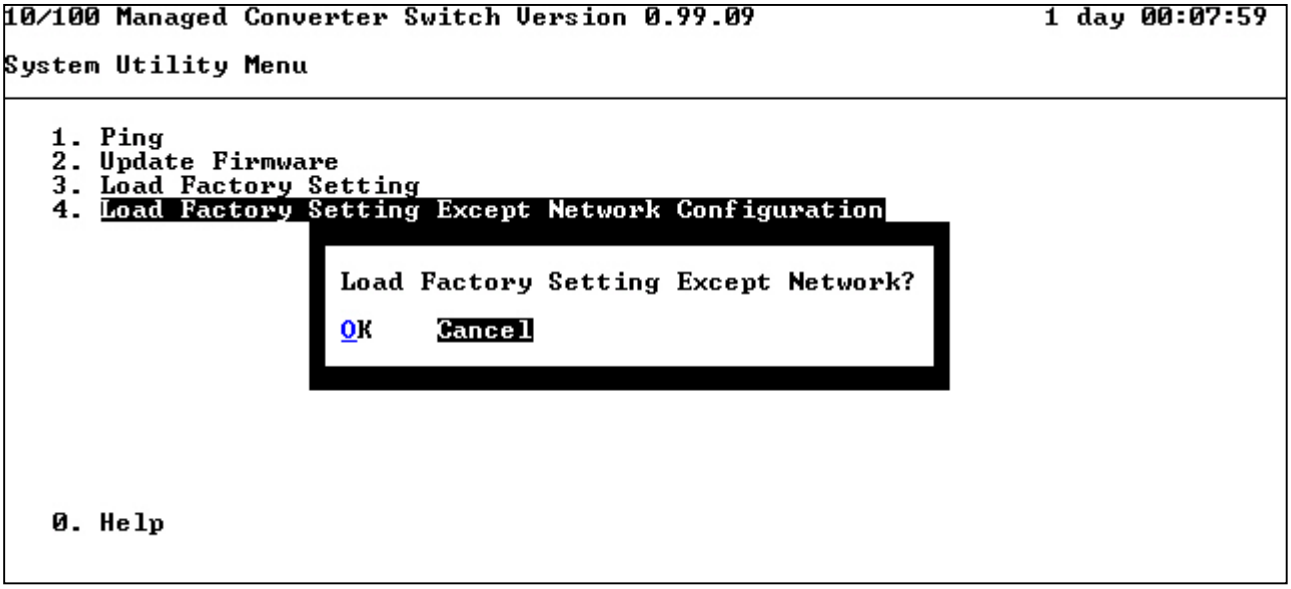
To load Factory Setting, select OK then press **Enter**.

2.10.4 Load Factory Setting Except Network Configuration

Load Factory Setting Except Network Configuration will return all the configuration of the converter switch to the factory default settings. However, IP and Gateway addresses will not return to the factory default.

Load Factory Setting Except Network Configuration is extremely useful when a network administrator need to re-configure the system "REMOTELY". Because traditional Factory Reset will bring network setting back to default and lost all network connection.

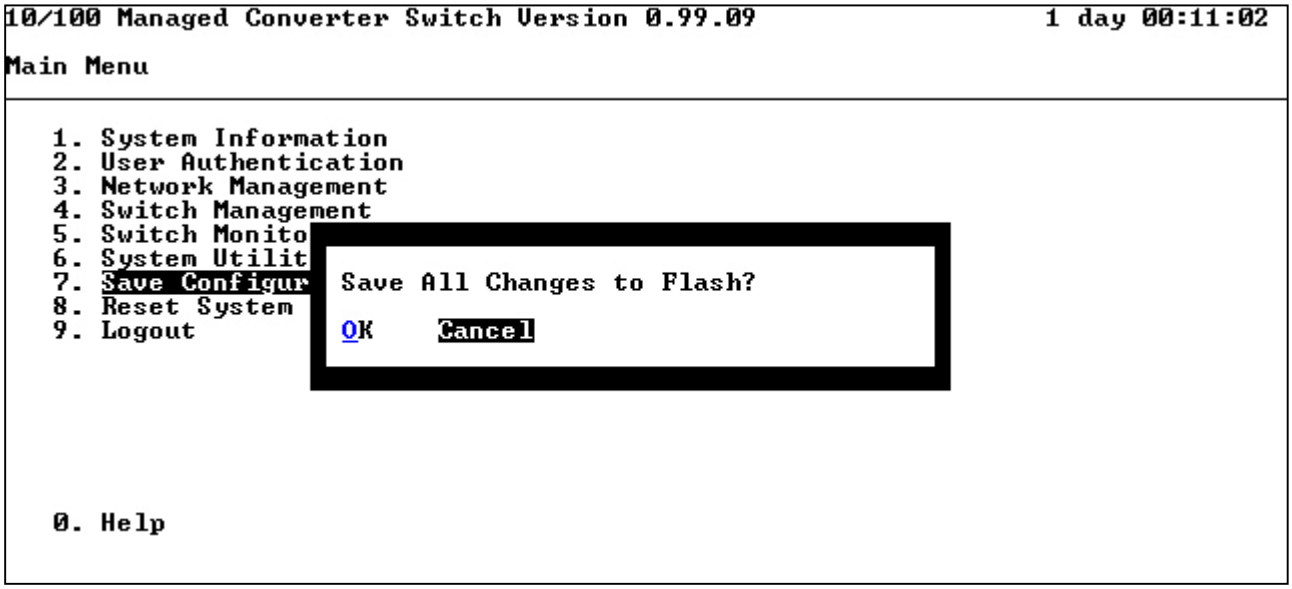
Select **Load Factory Setting Except Network Configuration** from the System Utility menu, following screen appears,



To load Factory Setting Except Network Configuration, select OK then press **Enter**.

2.11 Save Configuration

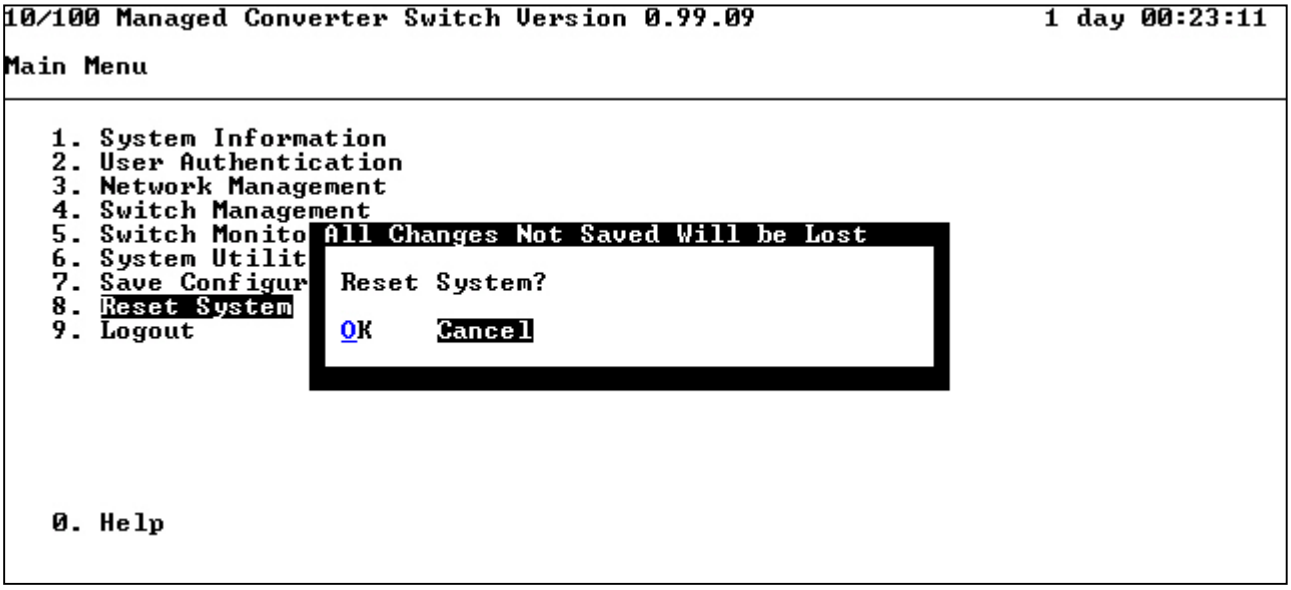
In order to save configuration setting permanently, user need to save configuration first before reset the converter switch. Select **Save Configuration** from the Console main menu, following screen appears.



To save the Configuration, select OK then press **Enter**.

2.12 Reset System

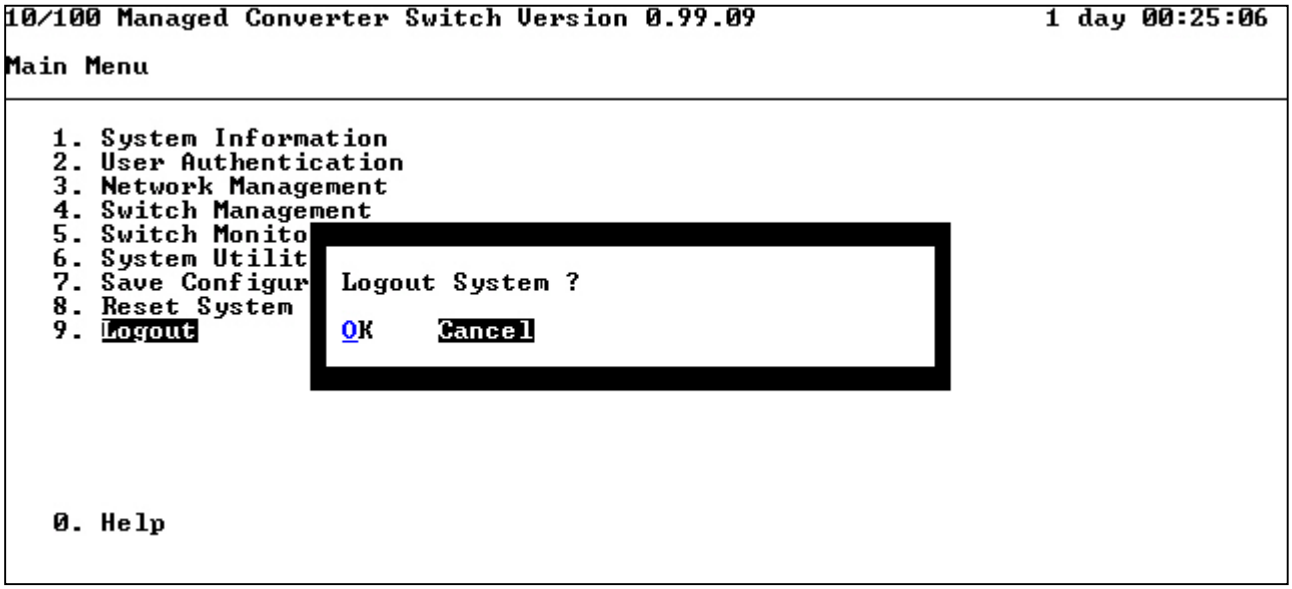
After configuration change, reset system to take change effect. Select **Reset System** from the Console main menu, following screen appears.



To perform System Reset, Select OK then press **Enter**.

2.13 Logout

Console Logout will stop current RS-232 or Telnet connection between the system and the PC. To perform Logout, select option **Logout** from the Console main menu, following screen appears.



To logout, select **OK** then press **ENTER**.

3. SNMP NETWORK MANAGEMENT

The Simple Network Management Protocol (SNMP) is an application-layer protocol that facilitates the exchange of management information between network devices. It is part of the TCP/IP protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth.

SNMP consists following key components,

Managed device is a network node that contains SNMP agent. Managed devices collect and store management information and make this information available to NMS using SNMP. Managed device can be switches/Hub, …,etc.

MIB (Management Information Base) define the complete manageable entries of the managed device. These MIB entries can be either read-only or read-write. For example, the System Version is read-only variables. The Port State Enable or Disable is a read-write variable and a network administrator can not only read but also set its value remotely.

SNMP Agent is a management module resides in the managed device that responds to the SNMP Manager request.

SNMP Manager/NMS executes applications that monitor and control managed devices. NMS provide the bulk of the processing and memory resources required for the complete network management. SNMP Manager often composed by desktop computer/work station and software program such like HP OpenView.

Totally 4 types of operations are used between SNMP Agent & Manager to change the MIB information. These 4 operations all use the UDP/IP protocol to exchange packets.

GET: This command is used by an SNMP Manager to monitor managed devices. The SNMP Manager examines different variables that are maintained by managed devices.

GET Next: This command provides traversal operation and is used by the SNMP Manager to sequentially gather information in variable tables, such as a routing table.

SET: This command is used by an SNMP Manager to control managed devices. The NMS changes the values of variables stored within managed devices.

Trap: Trap is used by the managed device to asynchronously report a specified event to the SNMP Manager. When certain types of events occur, a managed device will send a trap to alert the SNMP Manager.

The system built-in management module also supports SNMP management. User must install the MIB file before using the SNMP based network management system. The MIB file is on a diskette that accompanies the system. The file name extension is .mib, which SNMP based compiler can read.

Please refer to the appropriate documentation for instructions on installing the system private MIB.