USER MANUAL

IMC-1000M(S)

Industrial Gigabit Ethernet OAM/IP
Web Smart Media Converter

CTC UNION TECHNOLOGIES CO., LTD.

CTC Union Technologies Co., Ltd.
Far Eastern Vienna Technology Center
(Neihu Technology Park)
8F, No. 60 Zhouzi St., Neihu, Taipei 114,
Taiwan

T +886-2-26591021
F +886-2-26590237
E sales@ctcu.com
marketing@ctcu.com
techsupport@ctcu.com
H www.ctcu.com

IMC-1000M(S) Operation Manual

Industrial Gigabit Ethernet OAM/IP Web Smart Media Converter

Version 1.1 December 23, 2013 (Update Release)

This Manual supports the following models:

IMC-1000M : 1x1000Base-FX + 1x10/100/1000Base-TX
IMC-1000M-E : 1x1000Base-FX + 1x10/100/1000Base-TX, wide temperature
IMC-1000MS : 1x100/1000Base-FX (SFP) + 1x10/100/1000Base-TX
IMC-1000MS-E : 1x100/1000Base-FX (SFP) + 1x10/100/1000Base-TX, wide temperature

ISO 9001 Quality System Certified

Legal

The information in this publication has been carefully checked and is believed to be entirely accurate at the time of publication. CTC Union Technologies assumes no responsibility, however, for possible errors or omissions, or for any consequences resulting from the use of the information contained herein. CTC Union Technologies reserves the right to make changes in its products or product specifications with the intent to improve function or design at any time and without notice and is not required to update this documentation to reflect such changes.

CTC Union Technologies makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does CTC Union assume any liability arising out of the application or use of any product and specifically disclaims any and all liability, including without limitation any consequential or incidental damages.

CTC Union products are not designed, intended, or authorized for use in systems or applications intended to support or sustain life, or for any other application in which the failure of the product could create a situation where personal injury or death may occur. Should the Buyer purchase or use a CTC Union product for any such unintended or unauthorized application, the Buyer shall indemnify and hold CTC Union Technologies and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, either directly or indirectly, any claim of personal injury or death that may be associated with such unintended or unauthorized use, even if such claim alleges that CTC Union Technologies was negligent regarding the design or manufacture of said product.

TRADEMARKS

Microsoft is a registered trademark of Microsoft Corp.
HyperTerminal™ is a registered trademark of Hilgraeve Inc.

FCC WARNING:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual may cause harmful interference in which case the user will be required to correct the interference at his own expense. NOTICE: (1) The changes or modifications not expressively approved by the party responsible for compliance could void the user's authority to operate the equipment. (2) Shielded interface cables and AC power cord, if any, must be used in order to comply with the emission limits.

CISPR PUB.22 Class A COMPLIANCE:

This device complies with EMC directive of the European Community and meets or exceeds the following technical standard. EN 55022 - Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment. This device complies with CISPR Class A.

CE NOTICE

Marking by the symbol CE indicates compliance of this equipment to the EMC and LVD directives of the European Community. Such marking is indicative that this equipment meets or exceeds the following technical standards: EN 55022:2006, Class A, EN55024:1998+A1:2001+A2:2003, and EN60950-1:2001

Table of Contents

Chapter 1 Introduction

1.1 Welcome

Thank you for choosing **IMC-1000M(S)** Industrial Gigabit Ethernet OAM/IP Web Smart Media Converter. Throughout this document, the two different models of this family will be referred to as **IMC-1000MS** or in an abbreviated form as just **1000MS**. If you would like to skip right to the installation of the industrial grade converter, proceed to Chapter 2.

This manual is used to explain the hardware installation procedures and operation of **IMC-1000MS**, and present its capabilities and specifications. This manual is divided into 3 chapters, the Introduction, Installation, and Provisioning Chapters.

Installers should carefully read the Chapters 1&2, Introduction and Installation. The divisions in that manual are intended for use by personnel to answer questions in general areas. Planners and potential purchasers may read the Introduction to determine the suitability of the product to its intended use; Operating Personnel would use the Web Based Management Chapters and Appendices to become familiar with the settings. Network Administrators should read the chapters on Web Based Management and Trouble Shooting to become familiar with the diagnostic capabilities, network settings and management strategies.

1.2 Product Description

IMC-1000MS is an industrial grade electrical to optical media converter for Gigabit Ethernet. There are two models, one with fixed optical transceiver (**1000M**) and one supporting pluggable SFP transceiver (**1000MS**). These converters sport embedded stand-alone Web based management over IP networks as well as IEEE802.3ah OAM for remote in-band management.

IMC-1000MS is an IEEE802.3ah OAM compliant copper to fiber Gigabit Ethernet solution housed in rugged DIN rail or wall mountable enclosure. These converters are designed for harsh environments, such as industrial networking and intelligent transportation systems (ITS) and are also suitable for many military and utility market applications where environmental conditions exceed commercial product specifications. Standard operating temperature range models (-10 to 60°C) and wide operating temperature range models (-20 to 75°C) fulfill the special needs of industrial automation applications. These devices are designed to make conversion between 10/100/1000Base-TX and 100/1000Base-FX with SC, ST connector (**IMC-1000M**) or SFP LC connector (**IMC-1000MS**). When deployed as a stand-alone solution, this industrial media converter incorporates an easy to use Web user interface for operation, administration and maintenance of both local and remotely connected **IMC-1000MS** converters. By offering 802.3ah OAM compliance, this converter can be linked to any 802.3ah compliant fiber switch and support loop back and dying gasp functions. When used as a remote converter for our centrally controlled and managed **FRM220** managed rack, all functions of this converter can be remotely controlled and monitored via in-band management, including band-width control, duplex, speed, VLAN configuration and more.

1.3 Product Features

- Redundant dual DC inputs
- IP30 rugged metal housing
- Wide temperature model supported (-20C~75C)
- Auto-Cross over for MDI/MDIX at UTP port
- Auto-Negotiation or Forced Manual mode for UTP port
- Supports Dual Rate (100/1000) SFP for selectable Fast or Gigabit speed on fiber
- Supports 802.3X flow control Enable or Disable
- Supports Jumbo Frames up to 9600 bytes
- Supports 16 Tag VLAN Groups
- Supports 802.1Q tagging
- Ingress/Egress Bandwidth control with 64K granularity
- Supports 802.3ah-OAM loop back and dying gasp (remote power failure detection)
- Supports firmware upgrade via Web
- Supports Digital Diagnostics (DOM) for supported SFP
- Includes RMON counters
- Supports password setting for authentication
- Supports Link Fault Pass Through (LFP) Function
- Supports Auto Laser Shutdown (ALS) Function
- Supports DHCP client for automatic TCP/IP configuration
- Supports in-band remote management from **FRM220** rack management

IMC-1000MS SFP socket supports a wide range of standard SFP modules to address any network situation.

Single-mode, Multi-mode, Multi-rate, Dual Rate (100/1000), Single fiber bi-directional, Coarse and Dense Wave Division Multiplexing (CWDM and DWDM) and Copper media

WARNING: Fiber optic equipment may emit laser or infrared light that can injure your eyes. Never look into an optical fiber or connector port. Always assume that fiber optic cables are connected to an active laser light source.

1.4 Specifications

- Optical Interface
- Connector — SFP cage (**1000MS**) or Duplex SC, ST, FC (**1000M**)
- Data rate — 100/1000Base-FX (125Mbps/1.25GMbps optical rate) Dual Rate Support
- Duplex mode — Full duplex on fiber
- Fiber — Depends on SFP
- Distance — Depends on SFP
- Wavelength — Depends on SFP
- Electrical Interface
- Connector — RJ-45, shielded
- Data rate — auto, 10Mbps (10Base), 100Mbps (100Base), or 1000Mbps (1000Base)
- Duplex mode — auto, Full or Half
- Cable — Cat 5e or better
- Distance — 100Meters maximum
- Indications — LED (PWR, FX Link, LAN Link, LAN Speed)
- Power — Dual Inputs for redundancy
- Input — 12/24/48VDC, 9.6~60VCD absolute
- Consumption — <5W
- Dimensions — 155 x 88 x 23mm (D x W x H)
- Weight — 110g
- Temperature — Operating: -10 ~ 60°C (standard), -20~75°C (extended range)
  Storage: -20 ~ 85°C
- Humidity — 10 ~ 90% non-condensing
- Certification — CE (EMI/LVD), FCC, RoHS Compliant
- MTBF — 75000 hrs

1.5 Management Features

Once configured for TCP/IP access, these units support a Web Smart GUI for intuitive setting via point & click.

1.6 Panel

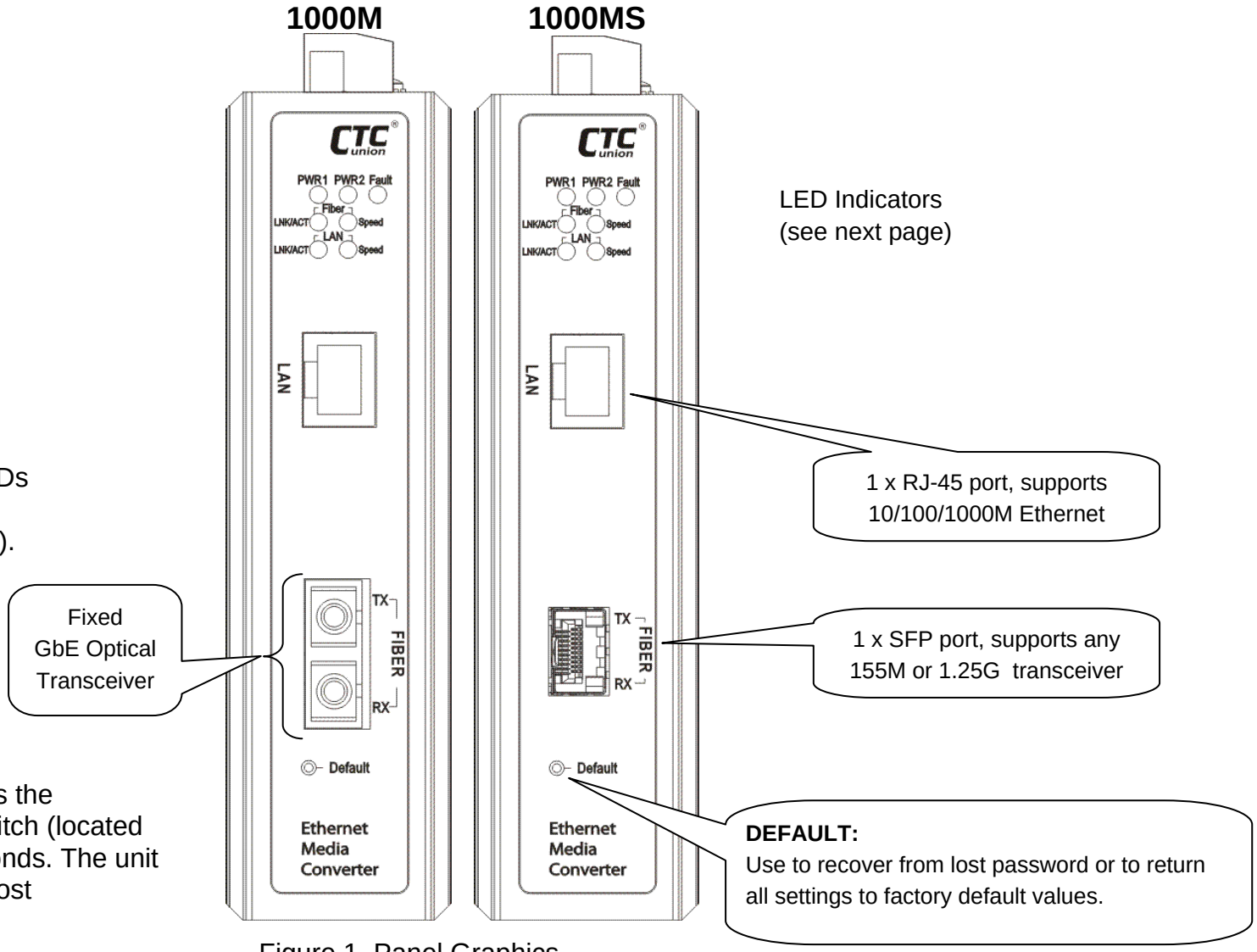


Figure 1. Panel Graphics

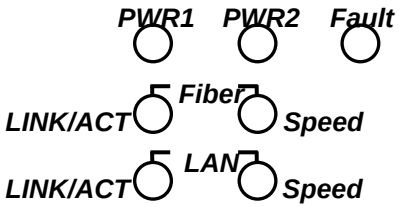
The LAN Speed and Fiber Speed LEDs use dual color to indicate speed. Green indicates Fast Ethernet (100M). Amber indicates Gigabit Speed. When off, the LAN Speed LED indicates 10M speed.

Factory reset procedure
Apply power to **1000M(S)**.
Allow 30 seconds to fully boot.
Using a pencil or ball-point pen, press the 'DEFAULT' recessed push-button switch (located on the face plate) and hold for 6 seconds. The unit will be restored to factory default almost immediately. The defaults are:

IP=10.1.1.1
netmask=255.255.255.0
GW=10.1.1.254
password reset to 'admin'

1.7 LED Indicators

IMC-1000M and **IMC-1000MS** have LEDs on the front face that report the condition of power, Fiber link & Speed, LAN link & Speed as well as power or link fault.



IMC-1000M(S) LED Indicators

PWR1: This green LED will light if power is connected and active at the PWR1 terminal connection.

PWR2: This green LED will light if power is connected and active at the PWR2 terminal connection.

Fault: This red LED will light if there is a power, fiber or TP fault condition.

Fiber LINK/ACT: This green LED will light when the fiber port has an optical link and flash when there is data traffic.

Fiber Speed: This two color LED will indicate the fiber speed setting. Green indicates 100M, while amber color indicates 1000M fiber speed.

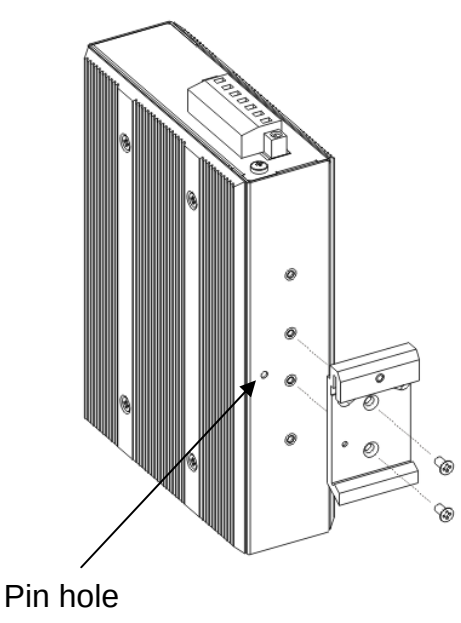
LAN LINK/ACT: This green LED will light when the LAN port has a link and will flash when there is Ethernet traffic.

LAN Speed: This two color LED will indicate the UTP (LAN) speed. Green indicates 100M, while amber color indicates 1000M UTP speed. If not lit, a LAN speed of 10M is indicated.

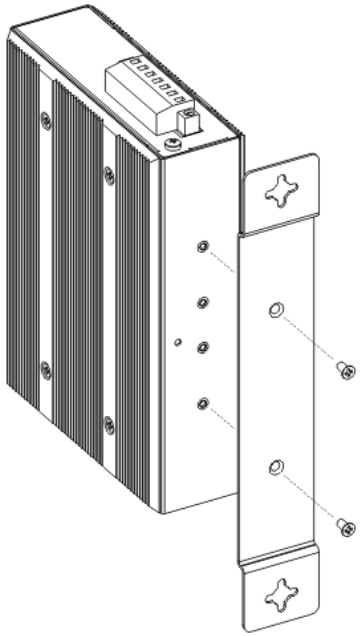
Chapter 2 Installation

2.1 Mounting Options

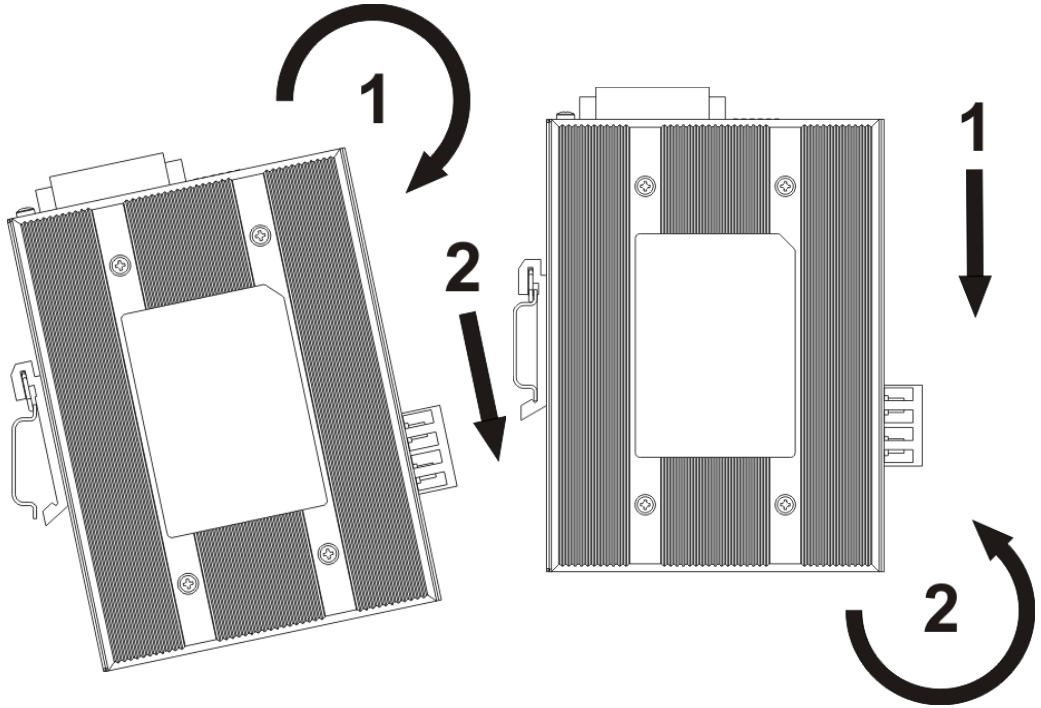
IMC-1000M(S) comes with both wall mount and DIN rail hardware brackets. When installing the DIN rail bracket, be sure to correctly align the orientation pin.



DIN Rail



Wall Mount

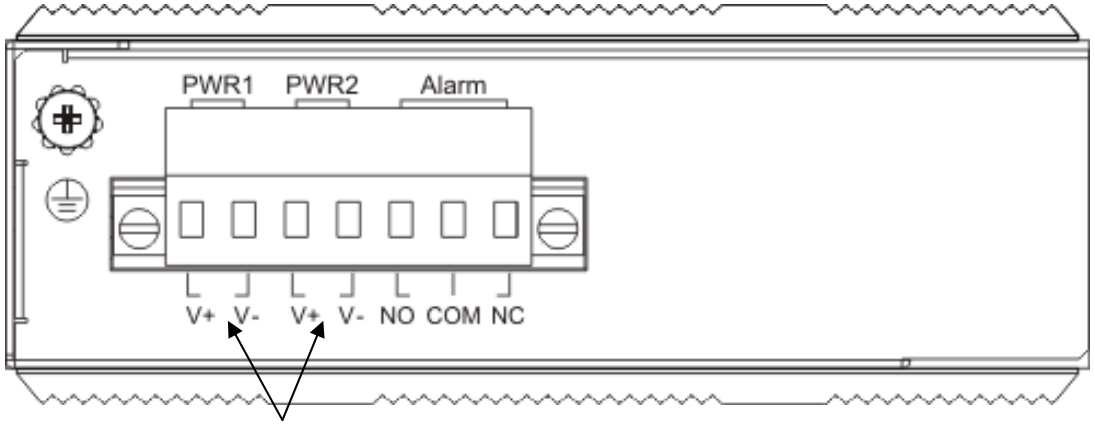


mounting un-mounting

IMC-1000M(S) with DIN Rail bracket has a steel spring in the upper rail of the bracket. This spring is compressed for mounting and un-mounting by applying downward force.

2.2 Electrical Installation

Power & Alarm

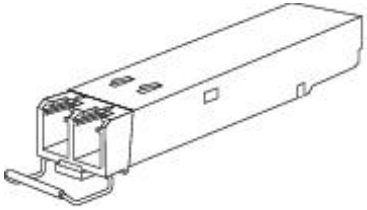


9.6 ~ 60VDC
Dual Inputs

A removable terminal block provides both power and alarm connections. Power can be provided through the dual inputs from separate sources. One electrical relay can be wired into an alarm circuit. From the common pin (COM), the relay can be connected as Normally Open (NO) or Normally Closed (NC). The alarm is triggered by programmable events of either link loss for optical or electrical or both. The relay is able to support a maximum current carrying capacity of 1A@24VDC.

2.3 Installation of SFP Modules

CTC Union supplied SFP modules are of the Bale Clasp type. The bale clasp pluggable module has a bale clasp that secures the module into the SFP cage and has a handle to aid in removing the module.



Bale Clasp type SFP

2.3.1 Inserting a Bale Clasp SFP Module into the Cage

Step 1 Close the bale clasp upward before inserting the pluggable module.
Step 2 Line up the SFP module with the port, and slide it into the cage. Seat it. Attach fiber cable.

2.3.2 Removing a Bale Clasp SFP Module

Step 1 Remove fiber cable. Open the bale clasp on the SFP module. Press the clasp downward with your index finger.
Step 2 Grasp the SFP module between your thumb and index finger and carefully remove it from the SFP cage.

Follow all ESD precautions when handling SFP modules.

Chapter 3 Web Based Provisioning

3.1 Introduction

In an effort to make Networking devices easier to configure, many devices can now be configured via a Web Page, which should be familiar to all Internet users.

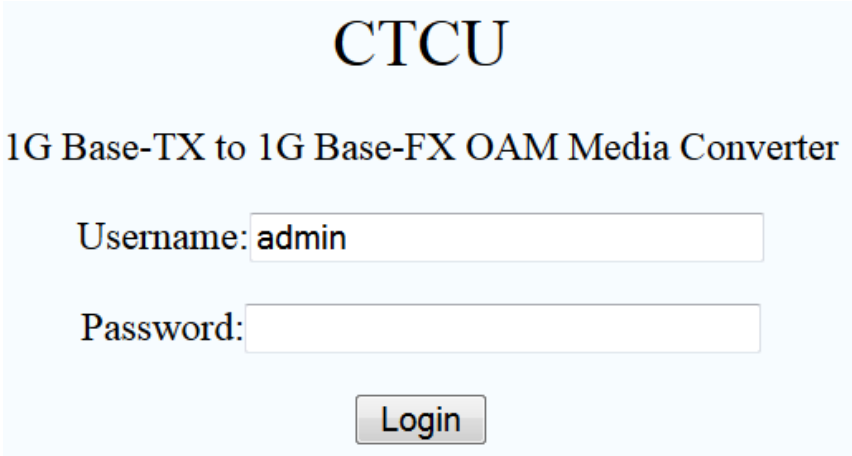
The web page is accessed by the Default IP Address of the device from a Web Browser such as Internet Explorer or Firefox in the following way:

http://10.1.1.1/ (Assuming the device has Default IP Address of 10.1.1.1)

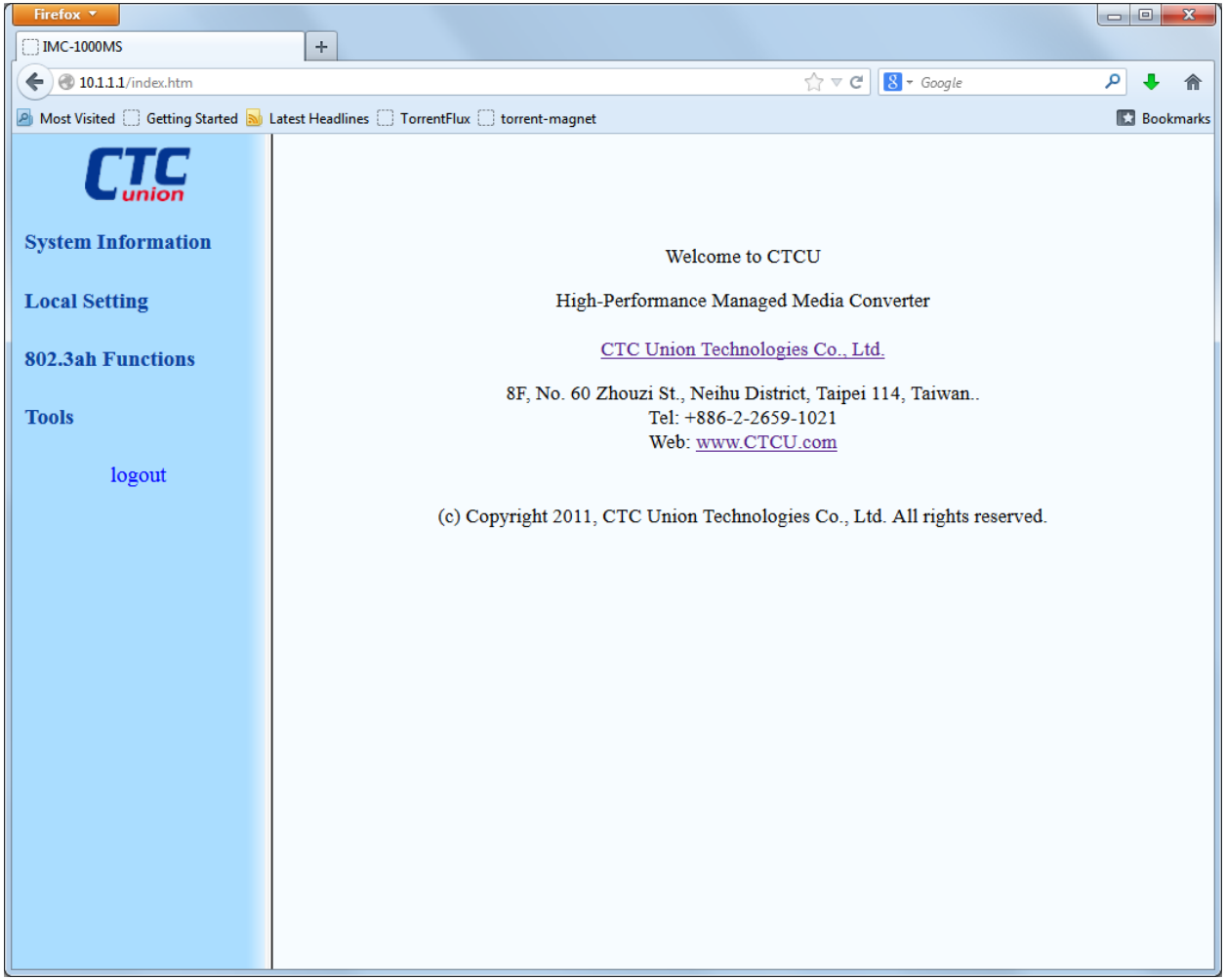
Before accessing this device by web browser, the IP address must be known or it must be reset or changed to be used on the desired network. Please refer to Chapter 1, section 1.6 for the factory reset procedure. For initial configuration, you must set your PC to the default IP subnet and access this device that way. Then you can change the IP address through the web interface.

3.2 Web Login Page

Access the device via a web browser.
Enter the password 'admin' and click "Login".



3.3 Web Main Page



3.4 System Information

3.4.1 Network Information

The information displayed on this page gives specific device, network information, and port status for the local 1000MS and for any remote that is accessible via IEEE802.3ah OAM in-band management.

Local Device Information

MAC Address	00:02:ab:11:22:44
Software Version	1.000
IP Address	10.1.1.1
Gateway	10.1.1.254
Subnet Mask	255.255.255.0
Description	IMC-1000MS
Power 1	OK
Power 2	FAIL

Remote Device Information

MAC Address	00:02:ab:11:22:23
Software Version	1.000
IP Address	10.1.1.8
Gateway	10.1.1.254
Subnet Mask	255.255.255.0
Description	IMC-1000M
Power 1	OK
Power 2	FAIL

Local Port Status

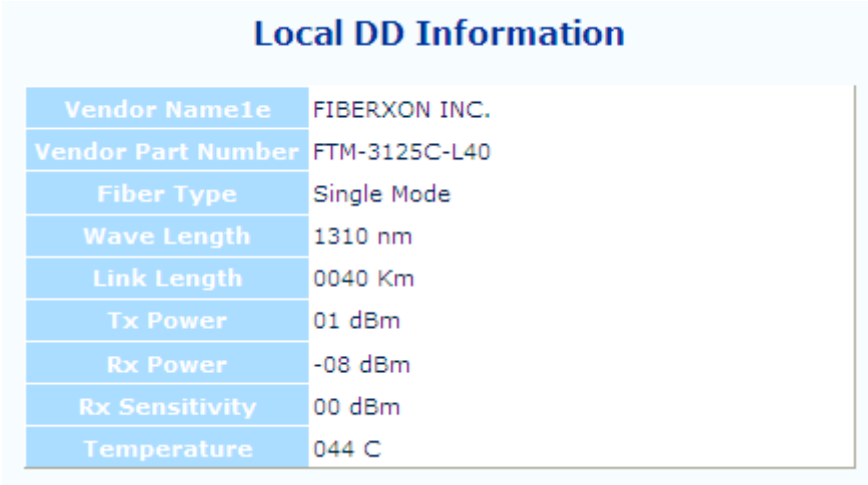
Ports	**TP**	**FX**
Link Status	Up	Up
Speed	100M	100M
Duplex mode	Full	Full
Flow control	Enable	Disable
Auto negotiation	Auto	Force

Remote Port Status

Ports	**TP**	**FX**
Link Status	Down	Up
Speed	10M	100M
Duplex mode	Half	Full
Flow control	Enable	Disable
Auto negotiation	Auto	Force

3.4.2 DD Information

The DD or DDOM information is read from the MSA compliant SFP module and can be displayed via the web user interface.

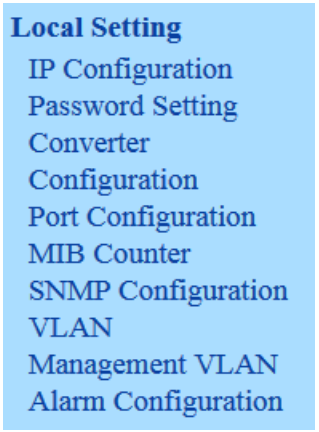


Local DD Information

Vendor Name1e	FIBERXON INC.
Vendor Part Number	FTM-3125C-L40
Fiber Type	Single Mode
Wave Length	1310 nm
Link Length	0040 Km
Tx Power	01 dBm
Rx Power	-08 dBm
Rx Sensitivity	00 dBm
Temperature	044 C

3.5 Local Settings

The following is a listing of the local settings that can be performed via the web interface for the **IMC-1000M(S)** industrial media converter. We will go through the settings here, one by one, in detail.

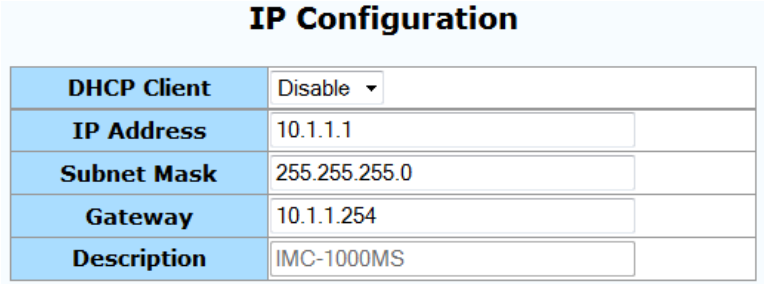


Local Setting

- IP Configuration
- Password Setting
- Converter Configuration
- Port Configuration
- MIB Counter
- SNMP Configuration
- VLAN
- Management VLAN
- Alarm Configuration

3.5.1 IP Configuration

Use this screen to set the TCP/IP configuration for the local unit. Note, that if you change the IP address you could lose remote management for this device. Remember to save settings under the “Tools” menu.



The above shows the factory default TCP/IP settings for **IMC-1000MS**.

DHCP Client, when enabled, will allow the **IMC-1000MS** to automatically get the IP configuration settings from the network's Dynamic Host Configuration Protocol server. When setting this device with static IP, make sure this is disabled (disabled is the default).

IP Address is the dotted/decimal format for the IPv4 address to remotely manage this device.

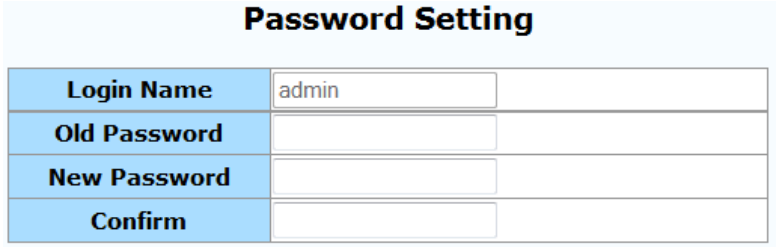
The **Subnet Mask** defines the type of subnet the device will be on. The proper subnet setting will be defined by the network administrator.

The **Gateway** is the default path for any packets NOT belonging to the local subnet. This IP address is the address of the router on your network. It is also entered as a dotted/decimal IPv4 format address. If the device will only be managed on the local subnet, setting a gateway address is optional.

After applying settings, do not forget to save the configuration under the ‘Tools’ menu so that the settings are permanent.

3.5.2 Password Setting

This function is used to modify the default password for the device. The password is required so that only authorized users have access to the management of the **IMC-1000MS**.

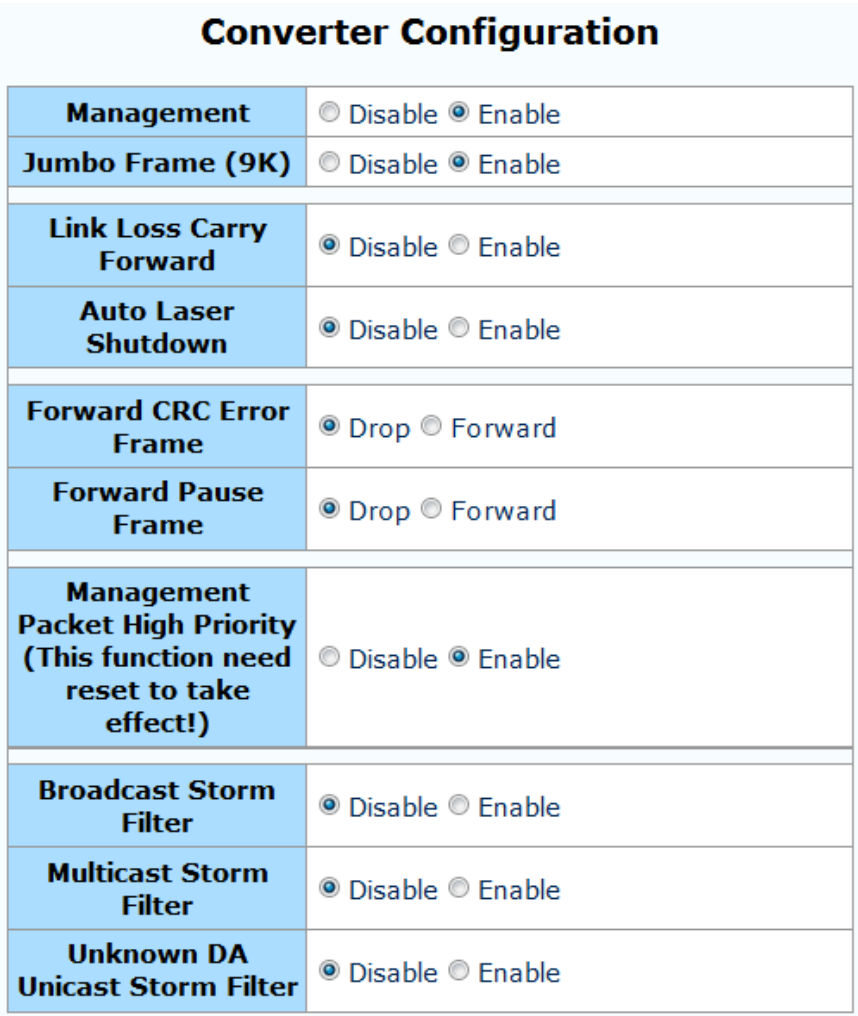


Key in the current password and type in the new password twice, then click the “Apply” button.

After applying settings, do not forget to save the configuration under the ‘Tools’ menu so that the settings are permanent.

3.5.3 Converter Configuration

The Converter configuration menu includes special features of **IMC-1000MS**.



Converter Configuration

Management	○ Disable ◉ Enable
Jumbo Frame (9K)	○ Disable ◉ Enable
Link Loss Carry Forward	◉ Disable ○ Enable
Auto Laser Shutdown	◉ Disable ○ Enable
Forward CRC Error Frame	◉ Drop ○ Forward
Forward Pause Frame	◉ Drop ○ Forward
Management Packet High Priority (This function need reset to take effect!)	○ Disable ◉ Enable
Broadcast Storm Filter	◉ Disable ○ Enable
Multicast Storm Filter	◉ Disable ○ Enable
Unknown DA Unicast Storm Filter	◉ Disable ○ Enable

All of these special functions will be explained on the following two pages. Select the proper radio buttons and then click the “Apply” button. Remember to save settings under the “Tools” menu.

The remote **Management** functions of the converter can be disabled. Once disabled and saved, regardless of the 802.3ah OAM settings, the remote management feature is disabled. When management is enabled, the remote management feature will be available.

This converter is capable of supporting **Jumbo Frames** (9k byte packets) when this option is enabled. Note that in order to support jumbo frames, the TP speed and duplex must match the FX. i.e., 1000M/Full. Jumbo Frames are not typically used on a normal network, since most devices are not able to handle them and they would be truncated. Most PCs, servers, switches, DSL and WiFi do not support jumbo frames. Jumbo frames can only work on a pure Jumbo frame network, which currently only exists in data centers for server-to-server or server-to-storage connections and on some education back bone networks. Jumbo frames will always be considered to be illegal, non-standard Ethernet packets, according to IEEE802.3. In most cases, the call for jumbo frame support is just marketing hype.

Link Loss Carry Forward or Link Fault Pass through (**LFP**) allows a link condition to be passed from fiber to TP or from TP to fiber. This function is disabled by default.

Auto Laser Shutdown (ALS) is an optical safety mechanism which will shutoff laser transmission if the transceiver experiences a loss of receive signal. This function is disabled by default.

Forward CRC Frame option is disabled by default. The normal behavior of a switch is to read the entire Ethernet frame (store), calculate the check sum and compare to the FCS in the packet. If the checksum matches, the packet is transmitted (&forward). If the checksum does not match, the switch considers the packet to have CRC error and drops it. If this option is enabled, the packet with CRC error will still be forwarded instead of being dropped.

The option **Forward Pause Frame** allows pause frame forwarding to occur when enabled. Pause frames are special broadcast frames defined in IEEE802.3X. Normally pause frames are used by the switch to throttle packets through a bottle neck rather than drop excess packets (for example, if **1000M** data stream is exiting a lower speed 100M port). Normally, the pause frames are not forwarded between interfaces in the switch. In many cases, pause frames are considered problematic. Therefore, their forwarding is disabled by default in this converter.

Management Packet High Priority is a function which is enabled by default. Unless VLAN is enabled, this function is meaningless. The packet priority is included as 3 bit priority in the VLAN tag. Management packets will be assigned highest priority so that even in the presence of high traffic throughput, this converter can still be easily managed.

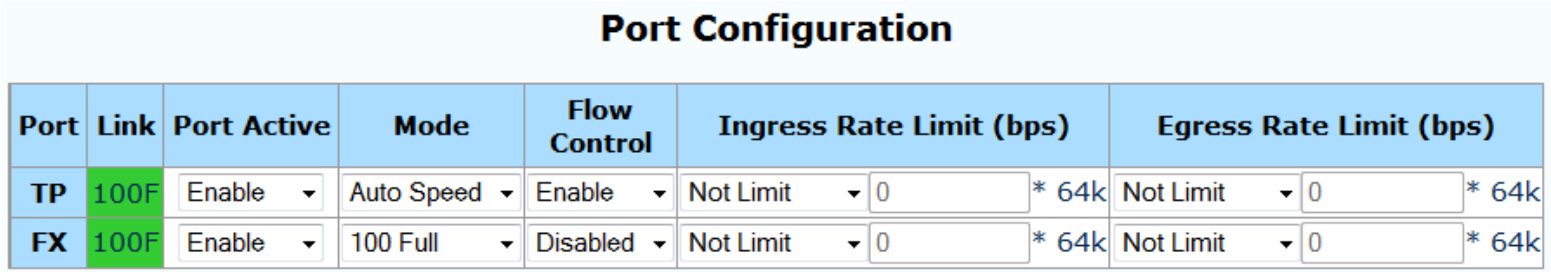
Broadcast Storm is a condition where either a loop exists on the network or an Ethernet transceiver is bad and exhibiting jabber. In addition there are the deliberate attempts to bring a network down through virus and denial of service routines. When enabled, the **Broadcast Storm Filter** will recognize and block the forwarding of these broadcasts.

Multicast storms happen when application participants request retransmits of information they have missed in the multicast stream. There are many applications, like video streaming, IP based punch clocks, IP based surveillance trackers and camera, that come with multicast or some broadcast based protocol turned on by default. The **Multicast Storm Filter** can be enabled to filter these unwanted effects.

The **Unknown DA Unicast Storm Filter** can be used to filter the Unicast broadcasts whose objective is to cause deny-of-service. Some Trojans and virus start scanning multicast IP ranges causing excess broadcasts and reducing network performance.

3.5.4 Port Configuration

This screen is for the configuration of the electrical Ethernet port (TP) and the optical port (FX).



Port Configuration

Port	Link	Port Active	Mode	Flow Control	Ingress Rate Limit (bps)	Egress Rate Limit (bps)
TP	100F	Enable	Auto Speed	Enable	Not Limit 0 * 64k	Not Limit 0 * 64k
FX	100F	Enable	100 Full	Disabled	Not Limit 0 * 64k	Not Limit 0 * 64k

Both the TP and FX **Port Active** are enabled by default. If a port is disabled, all transmission through this port will be stopped. The **1000M**'s LAN or Fiber Link LED will be extinguished if the port is made inactive. However, any connected device will still detect an Ethernet link.

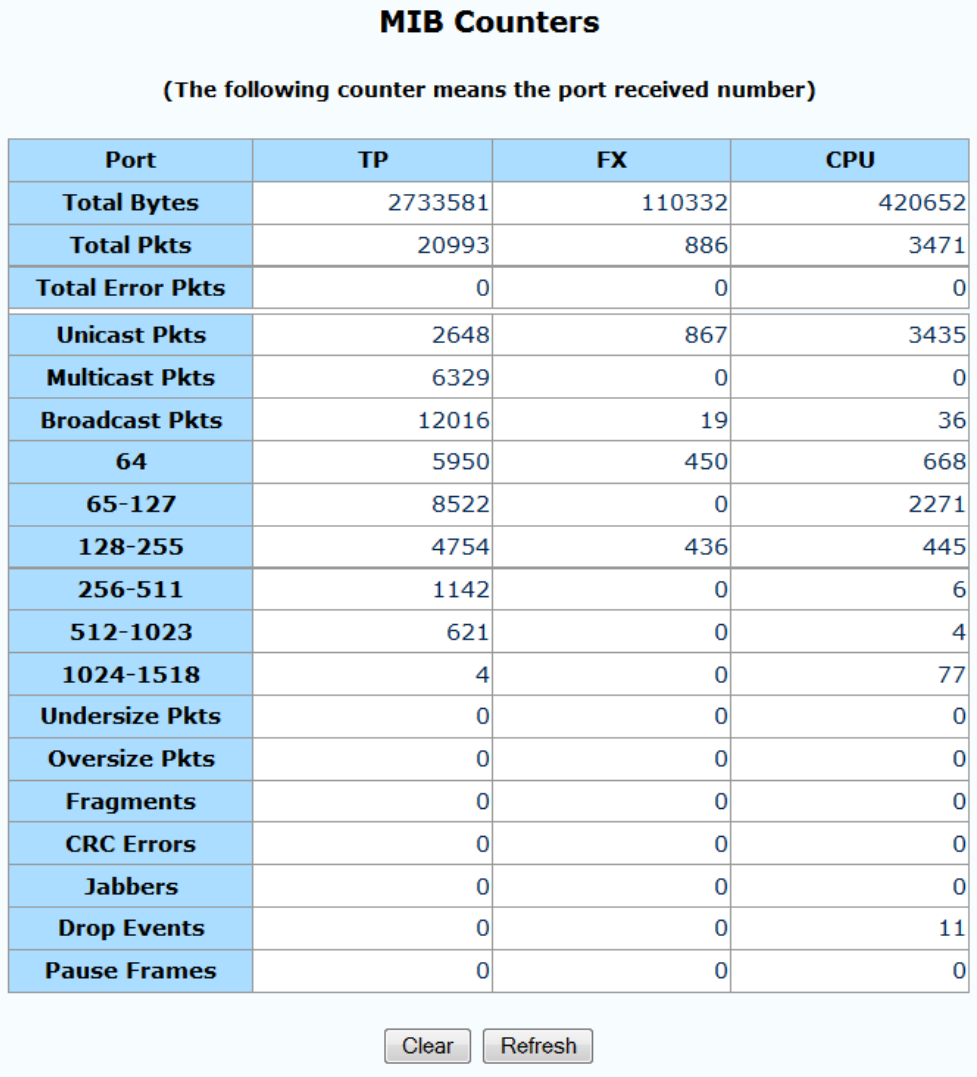
The UTP port **Mode** supports auto-**negotiation** per IEEE802.3u as well as manual forced mode setting of **Speed** (10/100/1000) and **Duplex** (Half/Full). In 802.3u, speed can be auto detected, however the Duplex mode MUST be negotiated. When an 802.3u compliant device is configured in auto negotiation mode, failure to negotiate Duplex (for example, if connected to legacy equipment or to equipment configured in forced mode) will result in the Auto device assuming a Half-Duplex operating mode. Do not connect forced Full mode Ethernet ports to an auto device as this will result in a Duplex-Mismatch.

The FX port will be able to auto detect speed (100M or 1000M) although there is no standard for fiber speed and duplex negotiation. Therefore, it is important that at least one device on the fiber link be manually configured for speed. In the example here, the device is manually configured for fiber speed of 100M.

Ethernet **Flow Control** (IEEE802.3X) is a mechanism for temporarily stopping the transmission of data on Ethernet family computer networks. It can work in conjunction with rate limiting to avoid dropped packets from TCP. Flow control should also be used with care and with full knowledge of its effect when used to pause traffic coming from a switch.

The **rate limiting** is adjustable for both ingress (packets received into the TP or FX port) and egress (packets transmitted from the TP or FX port) in granularity of 64k. By default, rate limiting is disabled. Once enabled, the rate limit can be set in nx64k rates where n=1 to 16000. Entering an "n" value of zero (0) will again disable the rate limiting.

3.5.5 MIB Counters



MIB Counters

(The following counter means the port received number)

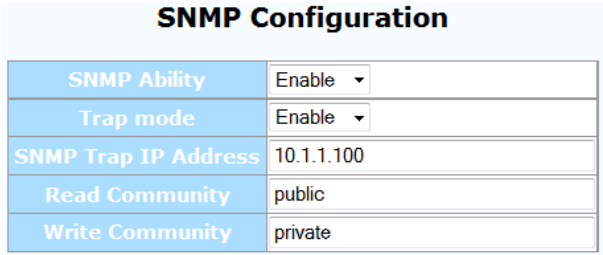
Port	TP	FX	CPU
Total Bytes	2733581	110332	420652
Total Pkts	20993	886	3471
Total Error Pkts	0	0	0
Unicast Pkts	2648	867	3435
Multicast Pkts	6329	0	0
Broadcast Pkts	12016	19	36
64	5950	450	668
65-127	8522	0	2271
128-255	4754	436	445
256-511	1142	0	6
512-1023	621	0	4
1024-1518	4	0	77
Undersize Pkts	0	0	0
Oversize Pkts	0	0	0
Fragments	0	0	0
CRC Errors	0	0	0
Jabbers	0	0	0
Drop Events	0	0	11
Pause Frames	0	0	0

Clear Refresh

The counters have an accumulation of received bytes and packets for each port (UTP, Fiber and Management). The distribution of those packets is further delineated into packet types (Unicast, Multicast, Broadcast) and packet sizes. Also counted are illegal packets and dropped events. This display can be refreshed or the counters cleared by clicking the appropriate buttons.

3.5.6 SNMP Configuration

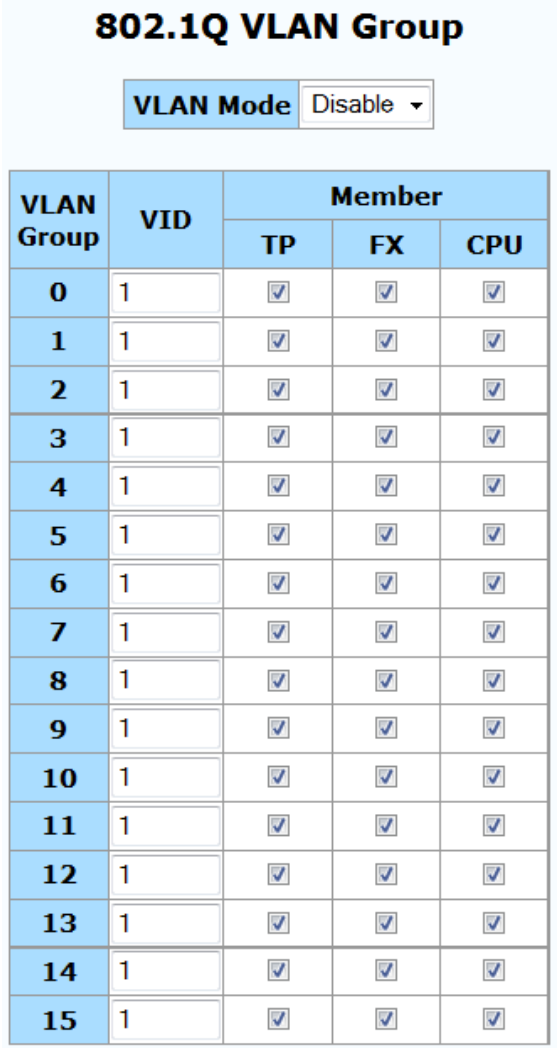
SNMP or Simple Network Management Protocol is an industry standard, ISO layer 7 application, for management of network devices. The SNMP deployed in the **IMC-1000MS** is SNMPv1. By default, SNMP is disabled.



In the example above, SNMP has been enabled along with trap mode. SNMP traps will be sent, unsolicited, to the trap server at the configured IP address (10.1.1.100 in the example). The community strings further control authentication for the SNMP 'get' and 'set' operations.

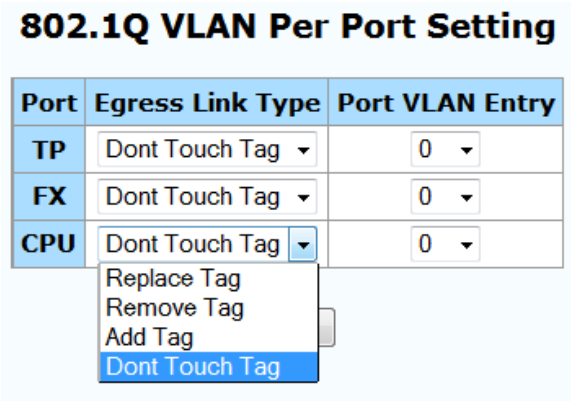
3.6.7 VLAN

3.6.7.1 VLAN Group



By default, this device is VLAN unaware, making it completely transparent to VLAN tags. In most application, this device only acts as a media converter and therefore the device should be transparent. **IMC-1000MS** does support up to 16 VLAN groups. By using the check boxes for each port, the ingress access to different VIDs can be controlled here for TP, FX and management.

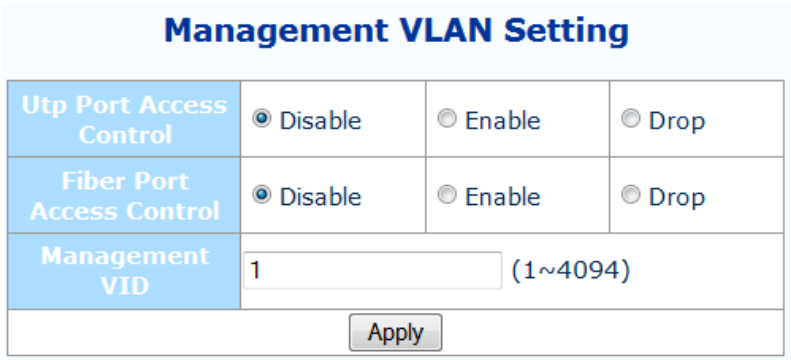
3.6.7.2 VLAN Per Port Configuration



Within the **IMC-1000MS** there are actually three different ports, the external copper and fiber ports, plus the internal CPU port (management). The VLAN Per Port Setting page deals with how frames exit (egress) the copper, fiber and CPU (management). These are the **Frame Egress Type**. The following operations may be performed to the outgoing frames: **<1>: Replace Tag** The switch will remove VLAN tags from packets then add new tags to them. The inserted tag is defined in ”Port VLAN Entry”. **<2>: Remove Tag** The switch will remove VLAN tags from packets, if they are tagged. The switch will not modify packets received without tags **<3>: Add Tag** The switch will add VLAN tags to packets, if they are not tagged when these packets are output on this port. The switch will not add tags to packets already tagged. The inserted tag is defined in ”Port VLAN Entry”. **<4>: Don't Touch Tag** Do not insert or remove VLAN tags to/from packet which is output on this port.

3.6.8 Management VLAN Setting

This function is independent of any other VLAN group or per port settings. The settings here provide a very quick method to configure how access to management is controlled.



There are three control 'states' defined as follows:
Disable : This means that the "access control" is not enabled. When set to disable, management is allowed in the respective port. By default, both the TP and FX ports allow full management using untagged packets.
Enable : The access control for the effected port is now enabled. Only packets tagged with the assigned "Management VID" are allowed for management of the **1000MS**.
Drop : No management is allowed from this port connection. If, for example, the TP port is set for 'Drop', then there will be no way to manage this device when connected to the UTP port. The management is effectively blocked on that port. This dropped setting might be used in an application where only management arriving from the FX port is desired and all management from TP is blocked.

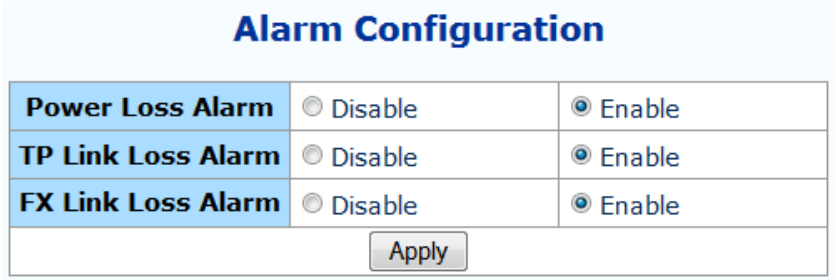
Caution : The "Apply" button is immediate and persistent. An incorrect setting here could result in 'loss of management' when applying that setting. For example, if you are managing the device via the UTP connection, select 'Drop' for the UTP port and then click 'Apply', management will be immediately lost. In fact, the device will no longer reply to 'ping' at its IP address. Simply rebooting the device will not be enough to recover. To regain management control, either access management from the fiber side, or reset the device to factory default and start over again.

3.6.9 Alarm Configuration

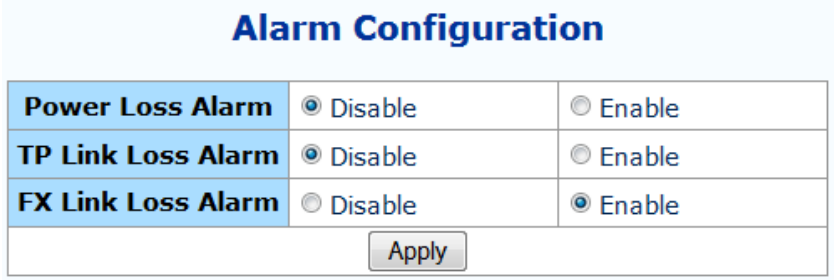
IMC-1000MS has an alarm relay with NO (normally open) and NC (normally closed) relay contacts which are available at the terminal block on the top of the unit. When there is an alarm condition (the RED alarm LED is lit) the NC relay will be closed. When there is no alarm condition (the RED alarm LED is off) the NO relay will be closed. If the device has no power, the NC relay will also be in a closed state (alarm active).

The programming here of the alarm serves two functions. First, the alarm indication of LED and the relay state are controlled by fault conditions of power, UTP link and/or Fiber link. Second, if SNMP is enabled, traps will be generated only on those alarm conditions that are configured.

In the default configuration, all sources for alarm are enabled. Settings are applied immediately.



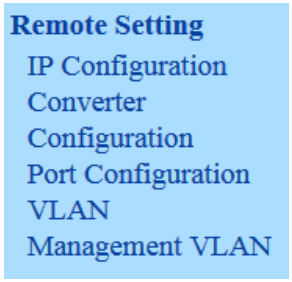
Example configuration:



An alarm will be triggered (and SNMP trap sent) only in the event of a loss of fiber link.

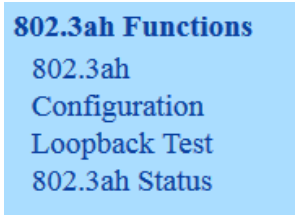
3.7 Remote Settings

When 802.3ah is active in both the local and remote unit (with fiber connection), the in-band management provides an embedded channel to control and configure the remote by using OAM (layer 2) Ethernet packets. The same settings available to the local unit are available under the **Remote Setting** menu, with the exception of password setting, SNMP, Counters and Alarm configuration.

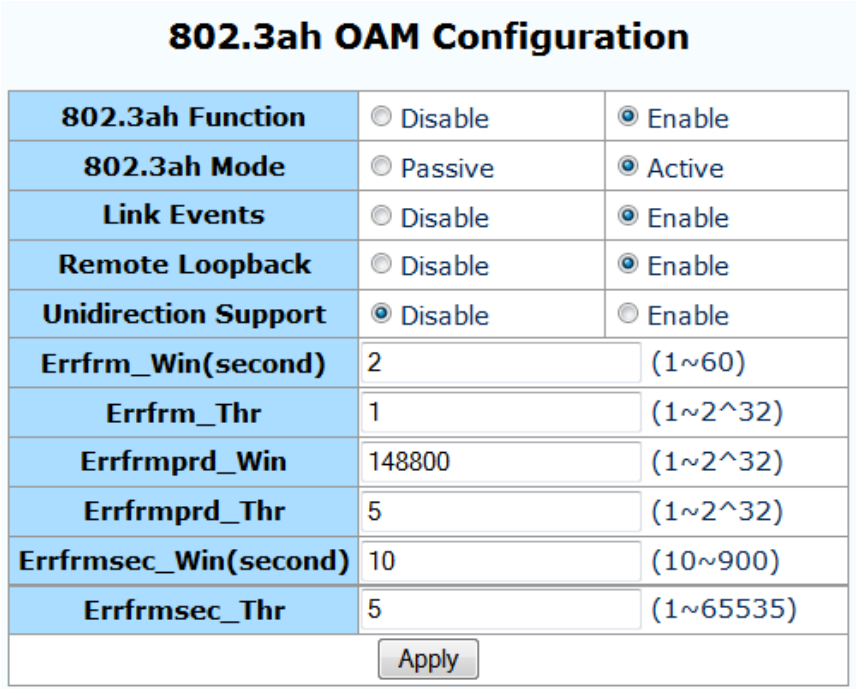


3.8 802.3ah OAM Functions

This converter supports IEEE 802.3ah, an OAM protocol that operates at Ethernet Layer 2 (Data Link layer). OAM provides mechanisms to monitor link operation / health and to improve fault isolation. OAM only works point-to-point over the fiber link. In addition to standard 802.3ah functions like loop back and dying gasp, **IMC-1000MS** also implements OAM to provide complete provisioning of the remote fiber connected converter, without using Layer 3 IP protocol. By using OAM, we can remote manage another fiber connected **1000M(S)** converter, without IP addressing. From this menu we can also perform some basic diagnostics, such as loop back test.

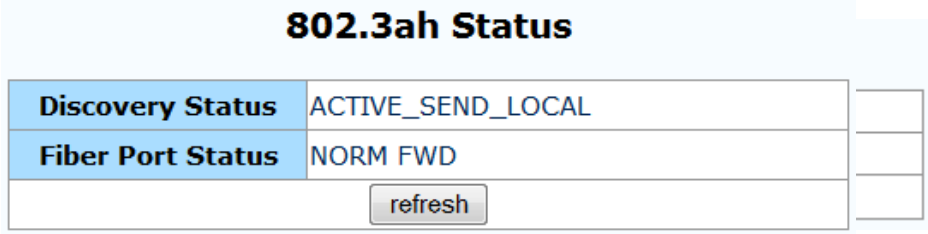


3.8.1 802.3ah Configuration



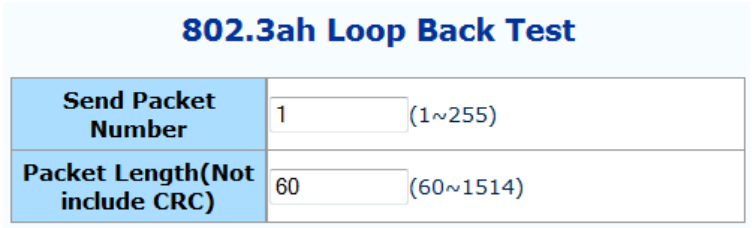
To use the OAM functions, the **802.3ah Function** setting must be enabled. It is not enabled by default. The **802.3ah mode** is used to configure an OAM pair. In a pair, one unit must be 'active', while the other must be 'passive'. We typically place the remote converter (CPE) in 'passive' mode and make the local converter 'active'. 'Passive' is the default setting when 802.3ah function is enabled.

In order to do **Remote Loop Back** test, this option must be enabled in both converters. By default it is enabled.



The normal status when OAM is working is shown above. If OAM is not passing due to fiber disconnect, Discovery Status will be Fault. If OAM is not enabled, this status window will not even be shown.

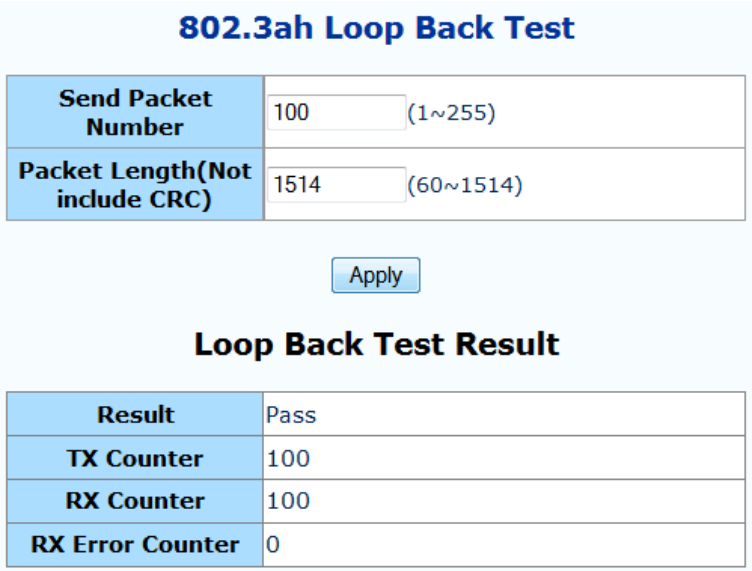
3.8.2 Loop back Test



The loop back test is a non-intrusive test which uses OAM packets and will not affect normal transmissions. The number of OAM frames used (the number of times the loop back is done) is set by the **Send Packet Number**. The default is 1 packet.

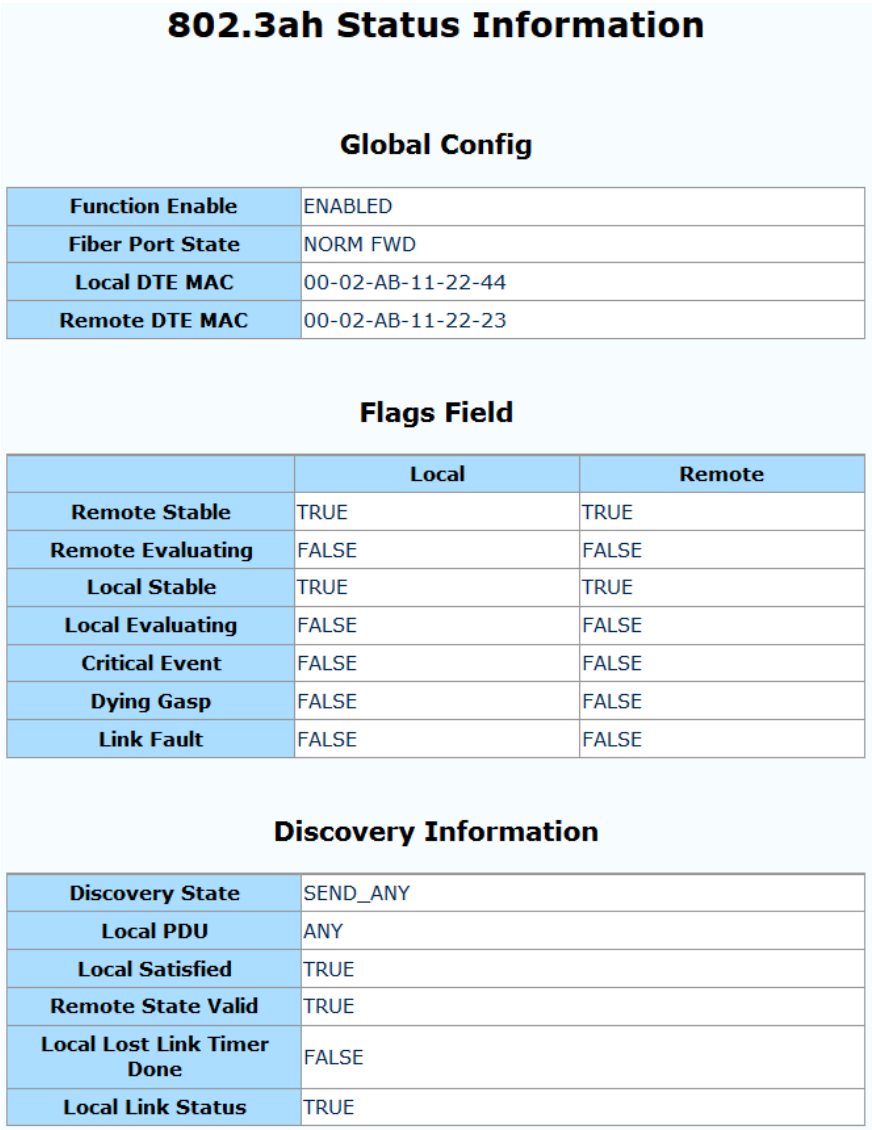
The **Packet Length (Not including CRC)** controls the packet size of the OAM frames used for loop back testing. The default is 60 bytes. The CRC of Ethernet packets uses 4 bytes. Valid Ethernet packets range in size from 64 bytes to 1518 bytes. VLAN tag adds another 4 bytes for a maximum size of 1522 bytes. Any frame size larger than this is technically called a jumbo frame and is not IEEE802.3 compliant.

The **Loop Back Test Start** is accomplished by clicking the “Apply” button.



802.3ah is a slow protocol with a maximum throughput of 10 packets per second. The test above takes about 10 seconds for 100 packets.

3.8.3 802.3ah Status



802.3ah Status Information

Global Config

Function Enable	ENABLED
Fiber Port State	NORM FWD
Local DTE MAC	00-02-AB-11-22-44
Remote DTE MAC	00-02-AB-11-22-23

Flags Field

	Local	**Remote**
Remote Stable	TRUE	TRUE
Remote Evaluating	FALSE	FALSE
Local Stable	TRUE	TRUE
Local Evaluating	FALSE	FALSE
Critical Event	FALSE	FALSE
Dying Gasp	FALSE	FALSE
Link Fault	FALSE	FALSE

Discovery Information

Discovery State	SEND_ANY
Local PDU	ANY
Local Satisfied	TRUE
Remote State Valid	TRUE
Local Lost Link Timer Done	FALSE
Local Link Status	TRUE

The **Global Config** fields display the state of OAM, if OAM is enabled. We can also see the MAC addresses of the local and remote units in the OAM manageable pair. The **Flags Field** list the results of individual events based on the results of OAM protocol data units (OAMPDUs). Lastly, when two OAM devices start negotiation, there is **Discovery Information** passed between them. The results are shown here.

Information TLV

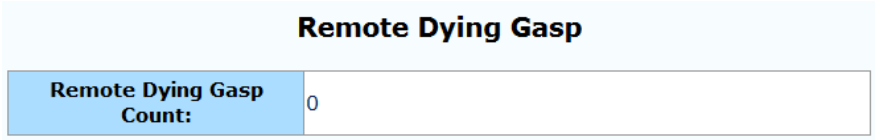
	Local	Remote
State Mux	FWD	FWD
State Par	FWD	FWD
Revision	0x2	0x2
Variable	TRUE	TRUE
Link Events	TRUE	TRUE
Loopback	TRUE	TRUE
Unidir	FALSE	FALSE
Mode	ACTIVE	PASSIVE

Most information carried by OAMPDU is encoded using type-length-value (TLV) format. The first octet (or byte) of the OAMPDU indicates the type. This type is used to let the OAM client know how to decode the bytes containing the information. The next octet carries the length of the information. This display has **TLV information** for both the local and remote OAM units.

Link Event Notification Status

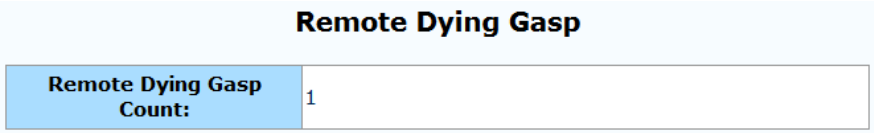
	Local	Remote
Frm Errtal	0	0
Frm Evetal	0	0
Frmprd Errtal	0	0
Frmprd Evetal	0	0
Frmsec Errtal	0	0
Frmsec Evetal	0	0

Ethernet OAM also defines a set of standard event conditions that Ethernet links should monitor in normal operation, and if detected, should be signaled to a peer entity. The **Link Event Notification Status** conditions reflect a degraded, but not yet inoperable, Ethernet connection. These conditions include threshold-crossing alarms on the frequency of symbol errors and frame errors.



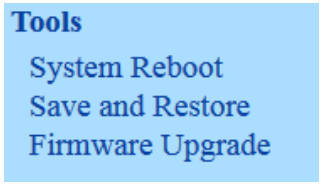
One of the most critical problems in an access network for carriers is differentiating between a simple power failure at the customer premise and an equipment or facility failure. Dying gasp provides this information by having a station indicate to the network that it is having a power failure.

If remote management is lost, we simply need to check the **Remote Dying Gasp Count** register to see if it has been incremented.



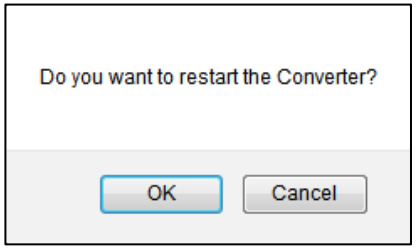
3.9 Tools

The **Tools** menu includes the **System Reboot**, **Save and Restore** settings and **Firmware Upgrade** functions.



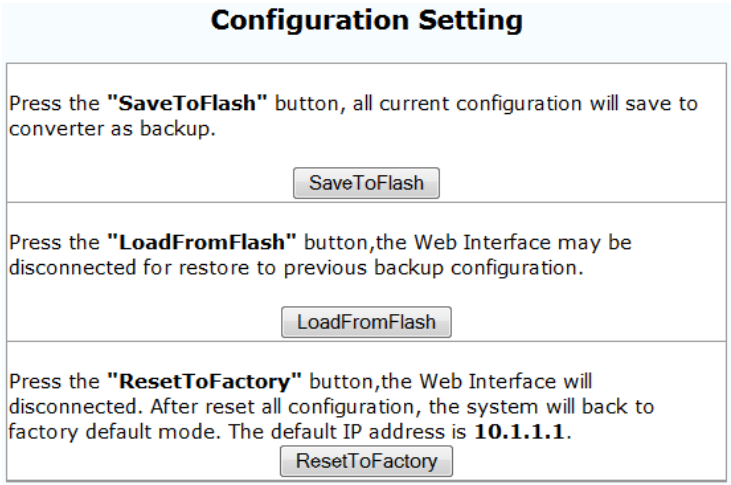
3.9.1 System Reboot

When the converter is rebooted, all counters and registers are cleared and the converter starts fresh. If OAM is enabled, the discovery process will start. After selecting the System Reboot menu item, a confirmation dialogue box will pop up. Click “OK” to reboot the converter or click “Cancel” to leave without rebooting. The converter requires about 20~25 seconds to fully reboot.



3.9.2 Save and Restore

After performing configuration of the converter, the settings must be saved. Click the “**Save To Flash**” button to save settings. If you wish to abandon all settings and return to the previous settings before doing configuration, click the “**Load From Flash**” button.

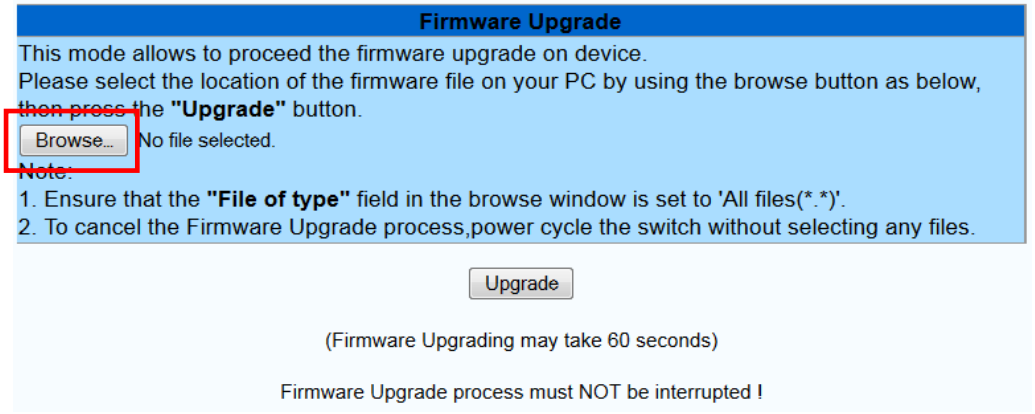


To restore all settings to factory default, click the “**Reset To Factory**” button. The IP address will also be reset, so you might lose management contact with the converter. So, be careful.

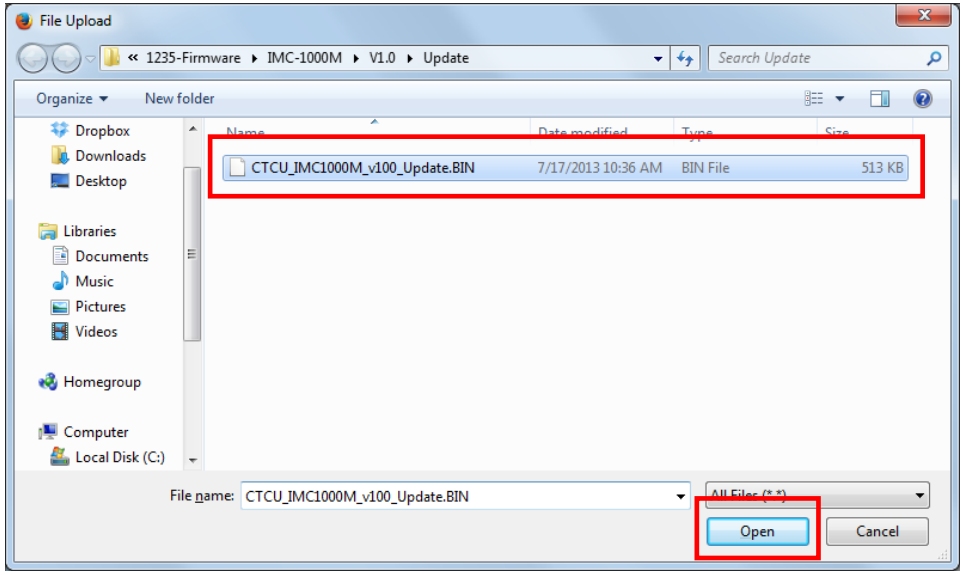
3.9.3 Firmware Upgrade

If bugs are discovered, if functions are added, or if factory default settings are changed, the firmware in the converter will require upgrading. The only method to do upgrade for this converter is through the local Web (HTTP) user interface. The firmware image is uploaded from the browser (Post), it is checked for integrity, the flash is erased and then the flash is written with the new image.

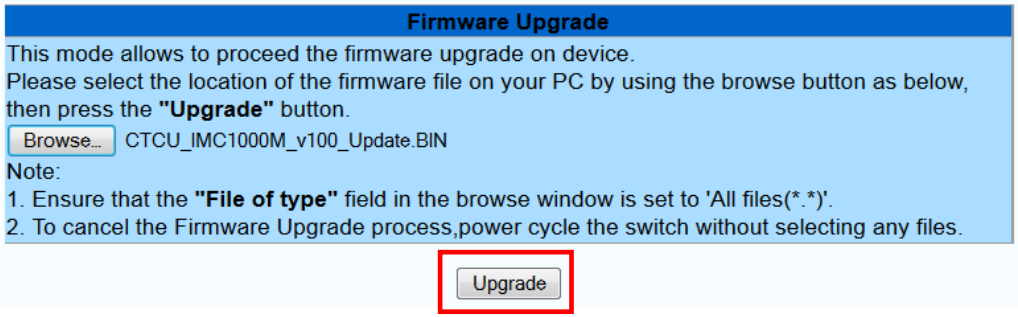
DO NOT LET ANY POWER INTERRUPTION OCCUR DURING THE UPGRADE PROCEDURE.



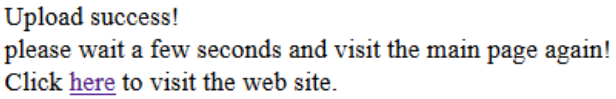
Click the “Browse” button and locate the image upgrade file through the “File Upload” dialogue box, then click “Open”.



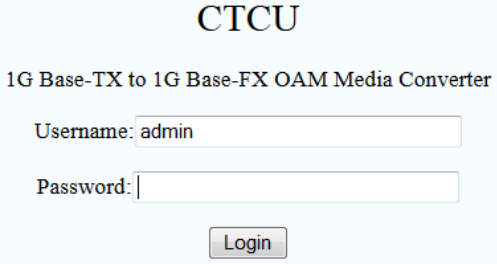
Next, click the “Upgrade” button.



The “Upload success!” indicates the image was transferred OK. **Do not do anything for the next 60 seconds!!!!**.

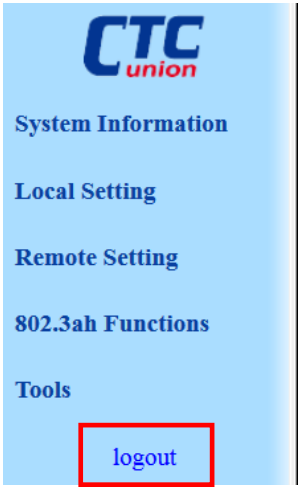


After 60 seconds, you may click the link to re-login to the web interface. Login as usual.

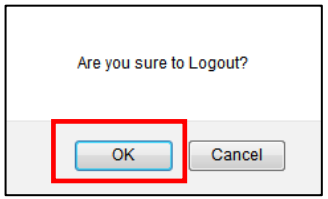


3.10 Logout

Logging out will ensure that the management session with **IMC-1000MS** is terminated. This is especially important if you are using a public computer to manage the device. Once logged out, a password must be entered to access **IMC-1000MS** again.



Click the “OK” button to completely log out. Click the “Cancel” button to return to configuration of **IMC-1000MS**.



3.11 Troubleshooting

3.11.1 Factory Default.

Apply power to **IMC-1000MS** and allow 25-30 seconds to fully boot. Using a pencil or ball-point pen, press the 'DEFAULT' recessed push-button switch (located on the face plate) and hold for 10 seconds or more then release. **DO NOT POWER OFF**; Allow the unit to again fully reboot (about 25 seconds). The factory default TCP/IP settings are:

IP=10.1.1.1
netmask=255.255.255.0
GW=10.1.1.254

The username and password are both reset to 'admin'.

Additionally, any VLAN, 1Q or bandwidth control will be disabled. All ports will be enabled, UTP ports set for auto-negotiation.

3.11.2 Reset

The reset function is a hardware reboot. Using a pencil or ball-point pen, press the 'DEFAULT' recessed push-button switch (located on the face plate) and hold for 3 seconds (no more than 4 seconds) and release. The unit will reboot using the previous saved configuration.

3.11.3 LED Observations

3.11.3.1 Power On

At initial power on, PWR LED will not be lit. If active LAN is connected to the TP port, that Link and Speed LED will be lit. After 25 seconds the CPU has fully booted, PWR LED will be lit and any fiber link or alarm will be actively shown by the LEDs

Error conditions :

If all LEDs immediately light and never turn off, or if no LED ever lights, then the unit is possibly defective. Be sure to double check power source.

3.11.3.2 UTP Link Test.

Following a complete power and boot up (about 25 seconds) the converter will be active and LAN port will display LAN LNK state when connected to a live Ethernet circuit. The LAN SPD LED will be green when connected to Fast Ethernet (100M) and yellow when connected to Gigabit Ethernet (1000M). When connected to 10Base-T the LAN SPD LED will be off.

3.11.3.3 Fiber Link Test

Following a complete power and boot up (about 25 seconds) the converter will be active. For **IMC-1000MS**, place a known good SFP module into Fiber Port cage. Use a simplex patch cable (single fiber strand, LC to LC), route the SFP Tx back to the Rx optical connection. The FX LNK LED should light. For **IMC-1000M**, use a simplex patch cable (single fiber strand, SC to SC, ST to ST or FC to FC), route the Tx back to the Rx optical connection. The FX LNK LED should light.

Caution: When performing a physical loop back on any fiber port, DO NOT connect the LAN port to a live Ethernet network. Doing so could create a broadcast storm.

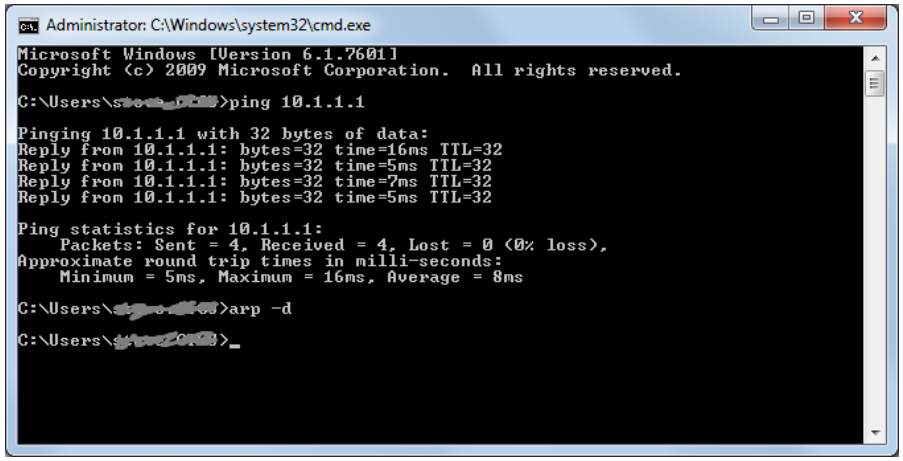
3.11.4 Operation Checks

3.11.4.1 Converter Check

A very easy way to ensure a pair of **IMC-1000MS** is passing traffic, is to place them between two PCs. Connect PC1 to LAN of one converter and PC2 to LAN of the other converter. When the two PCs can ping each other, it indicates **IMC-1000MS** pair is operational.

3.11.4.2 Ping Test

With **IMC-1000MS** reset to factory default, connect a PC and configure the PC to the 10.1.1.0 network (10.1.1.100 recommended). Use a PC to ping **IMC-1000MS** at its factory default IP address of 10.1.1.1. With a direct connection to PC, there should be no time outs and ping latency should be less than 1 millisecond. If you switch to another **IMC-1000MS**, be sure to clear the PC ARP table. Every **IMC-1000MS** has the same default IP address, but every unit has a different MAC address. To clear the PC's MAC table, open a command window and execute the command 'arp –d'. In addition, if you disconnect the PC from any LAN connection and then re-connect, the ARP table should also be cleared.



3.11.4.3 Web Access Test

With **IMC-1000MS** reset to factory default, connect a PC and configure the PC to the 10.1.1.0 network (10.1.1.100 recommended). Use a PC to connect to **IMC-1000MS** at its factory default IP address of 10.1.1.1 using a web browser (Internet Explorer, Firefox, Chrome, etc.). The local web page login page should display. Use 'admin/admin' to login; the local main page should be displayed in the browser.

If the ping test can pass and the login page can be displayed but login fails, we recommend that cookies be deleted. You may either delete all cookies for your browser or only the individual cookie created for the IP address of **IMC-1000MS**.

w w w . c t c u . c o m

T +886-2 2659-1021 **F** +886-2 2659-0237 **E** info@ctcu.com