



IE-MultiWay

Operation Manual



FCC Radio Frequency Interference Statement

Class A (using 48V Telco type power)

This equipment has been tested and found to comply with the limits for a Class A computing 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 to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which the user will be required to correct the interference at his own expense.

Any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

The use of non-shielded I/O cables may not guarantee compliance with FCC RFI limits. This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par le ministère des Communications du Canada.

Class B (using all other power options)

This equipment has been tested and found to comply with the limits for a Class B computing 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 to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which the user will be required to correct the interference at his own expense.

Any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

The use of non-shielded I/O cables may not guarantee compliance with FCC RFI limits. This digital apparatus does not exceed the Class B limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de classe B prescrites dans le Règlement sur le brouillage radioélectrique publié par le ministère des Communications du Canada.

Warranty

IMC Networks warrants to the original end-user purchaser that this product, EXCLUSIVE OF SOFTWARE, shall be free from defects in materials and workmanship under normal and proper use in accordance with IMC Networks' instructions and directions for a period of six (6) years after the original date of purchase. This warranty is subject to the limitations set forth below.

At its option, IMC Networks will repair or replace at no charge the product which proves to be defective within such warranty period. This limited warranty shall not apply if the IMC Networks product has been damaged by unreasonable use, accident, negligence, service or modification by anyone other than an authorized IMC Networks Service Technician or by any other causes unrelated to defective materials or workmanship. Any replaced or repaired products or parts carry a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

To receive in-warranty service, the defective product must be received at IMC Networks no later than the end of the warranty period. The product must be accompanied by proof of purchase, satisfactory to IMC Networks, denoting product serial number and purchase date, a written description of the defect and a Return Merchandise Authorization (RMA) number issued by IMC Networks. No products will be accepted by IMC Networks which do not have an RMA number. For an RMA number, contact IMC Networks at PHONE: (800) 624-1070 (in the U.S and Canada) or (949) 465-3000 or FAX: (949) 465-3020. The end-user shall return the defective product to IMC Networks, freight, customs and handling charges prepaid. End-user agrees to accept all liability for loss of or damages to the returned product during shipment. IMC Networks shall repair or replace the returned product, at its option, and return the repaired or new product to the end-user, freight prepaid, via method to be determined by IMC Networks. IMC Networks shall not be liable for any costs of procurement of substitute goods, loss of profits, or any incidental, consequential, and/or special damages of any kind resulting from a breach of any applicable express or implied warranty, breach of any obligation arising from breach of warranty, or otherwise with respect to the manufacture and sale of any IMC Networks product, whether or not IMC Networks has been advised of the possibility of such loss or damage.

EXCEPT FOR THE EXPRESS WARRANTY SET FORTH ABOVE, IMC NETWORKS MAKES NO OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, WITH RESPECT TO THIS IMC NETWORKS PRODUCT, INCLUDING WITHOUT LIMITATION ANY SOFTWARE ASSOCIATED OR INCLUDED. IMC NETWORKS SHALL DISREGARD AND NOT BE BOUND BY ANY REPRESENTATIONS OR WARRANTIES MADE BY ANY OTHER PERSON, INCLUDING EMPLOYEES, DISTRIBUTORS, RESELLERS OR DEALERS OF IMC NETWORKS, WHICH ARE INCONSISTENT WITH THE WARRANTY SET FORTH ABOVE. ALL IMPLIED WARRANTIES INCLUDING THOSE OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY LIMITED TO THE DURATION OF THE EXPRESS WARRANTY STATED ABOVE.

Every reasonable effort has been made to ensure that IMC Networks product manuals and promotional materials accurately describe IMC Networks product specifications and capabilities at the time of publication. However, because of ongoing improvements and updating of IMC Networks products, IMC Networks cannot guarantee the accuracy of printed materials after the date of publication and disclaims liability for changes, errors or omissions.

Table of Contents

FCC Radio Frequency Interference Statement	ii
Warranty.....	ii
About the IE-MultiWay.....	1
Operations, Administration and Maintenance (OAM)	3
iView ² Management Software	4
iView ² (iConfig view)	4
Hardware Mounting Options	5
DIP Switch Selectable Mode Configuration	6
DIP Switch Configuration	7
Powering the IE-MultiWay.....	7
Mini-Serial Port.....	7
LED Operation.....	8
Autocross Feature for Twisted Pair Connections	8
Configuration	8
Configuration Options.....	9
Basic Device Configuration Using the CLI.....	10
Saved and Current Values	11
Command List	11
Assigning IP Information.....	11
Password Protection for Serial Port Connections.....	11
Assigning SNMP Trap Destinations	12
Removing Trap Destinations.....	12
Creating Community Strings.....	12
Deleting Community Strings.....	13
Ending the Session	13
Rebooting the Unit	13
Enabling/Disabling DHCP.....	13
Commands List (Space Bar).....	14
Cleandb	15
Downloading Files	15
Accounts.....	16
VLAN Configuration.....	16
Bandwidth (bw)	19
Version	22
Viewing Port Statistics (ifstats)	22
Viewing Port RMON Statistics (rmstats).....	22
System Description (sysDescr)	23
Reboot.....	23
(Operation and Administration Management) OAM	23
Viewing SFP Statistics (sfpstats)	24
Unit.....	24

Port Configuration (port)	25
Using iView ²	26
Unit Configuration	28
Port Configuration.....	29
Bandwidth	29
Tables	30
VLAN.....	31
Advanced	32
OAM AH	32
Loopback Testing.....	33
OAM CFM.....	35
Agent Info	40
Connecting the IE-MultiWay to an iMcV-Giga-FiberLinX-II	41
Configuration File Save/Restore Function.....	42
Saving a Configuration File to Disk:	43
Uploading a Saved Configuration File through iView ² (iConfig view)	45
SFP Ports.....	46
Hardware/Wiring Specifications	46
DC Terminal Block Wiring Instructions.....	46
RJ-45 Data Port Pinout.....	47
RS-232 Serial Console Port.....	47
Product Applications	48
Glossary	49
Troubleshooting.....	51
Specifications	52
Standards/Compliance	53
IMC Networks Technical Support.....	53
Fiber Optic Cleaning Guidelines.....	54
Electrostatic Discharge Precautions.....	54
Safety Certifications.....	55

About the IE-MultiWay

The IE-MultiWay is an SNMP manageable standalone device providing two fixed 10/100/1000Base-T copper ports and 2 SFP ports. The SFP ports support fiber or copper SFPs. As a plug and play device, the IE-MultiWay provides several distinct modes of operation to support a wide range of applications. The IE-MultiWay provides OAM functionality with 802.3ah (LINK-OAM ah) and 802.1ag (SERVICE-OAM ag) supported on each port. It supports jumbo frame sizes of up to 10,240 bytes as well as AutoCross on the copper ports. Power options for the IE-MultiWay include both a standard low voltage wall transformer and a Power Block for Office Battery or a DC Power Supply connection. As an Industrial Ethernet device, it supports an extended temperature range of -40°C to +85°C. A console port and a DIP Switch bay provide configuration options.

The IE-MultiWay can be directly managed, because it contains on-board logic. Management capability is available if the device has firmware version 123-00A1 or higher, which can be downloaded from the IMC Networks site. iView² is a free software, posted on the website under Support/Downloads. Please refer to page 4 for details.

The IE-MultiWay requires two small form-factor (SFP) modules which provide greater flexibility in the network environment. The hot-swappable nature of the SFPs, available in dual strand for Multi Mode and Single Mode, and single strand fiber types for Single Mode, allow for easy configuration and future upgrading as network demands evolve. The SFP modules must be MSA-compliant and both DDMI and non-DDMI are supported. The fiber SFP can support 100Mbps or 1000Mbps; while the copper SFPs support 10/100/1000Mbps and 1000Mbps.

SFPs are sold separately by IMC Networks and meet Class 1 Laser Safety Standard.

IE-MultiWay Features and Configuration

The IE-MultiWay offers a full feature set including Auto Negotiation, Selective Advertising, AutoCross, VLANs, SNMP management, loopback testing and OAM. Unit software updates can be downloaded through TFTP or iView² (iConfig view).

IE-MultiWay features include:

- SNMP manageable
- OAM AH
 - IEEE 802.3ah Link OAM for per port monitoring (OAM AH)

- OAM AH Functions
 - Discovery
 - Link Performance Monitoring
 - Remote Loopback
 - Fault Detection
 - Link Fault
 - Dying Gasp
 - Critical Event
- OAM CFM (SERVICE-OAM)
 - IEEE 802.1ag Connectivity Fault Management (OAM CFM)
 - OAM CFM Functions
 - Continuity Check
 - Loopback
- Speed/duplex modes
- 802.1q VLAN
- Extra tagging with user-defined VLAN tag Ethertype
- Ethertype 88A8 as defined in 802.1ad
- Command Line Interface capable (CLI)
- Telnet
- Password assignment via CLI, Telnet or iView²
- DIP Switch configuration for Modes
- Bandwidth Limiting

The IE-MultiWay can be installed as a standalone CPE device, back to back, or as a Remote when connected to an iMcV-Giga-FiberLinX-II configured as a Host.

As a CPE device, the IE-MultiWay can behave as a remote to an iMcV-Giga-FiberLinX-II host when:

- 1) The iMcV-Giga-FiberLinX-II:
 - Is connected via the SFP ports on the IE-MultiWay
 - Is configured as a Host
 - Uses firmware version A1 860-00D1 or higher
- 2) The SNMP card (if present):
 - Uses SNMP firmware version 953-00C8 or higher
- 3) The IE-MultiWay:
 - Uses firmware version 123-00A1 or higher

When using iView², the IE-MultiWay can be fully managed without an IP address using a secure management channel. However, an IP address can be assigned

through iView² (iConfig view), the CLI or Telnet using the default IP address of 10.10.10.10.

Operations, Administration and Maintenance (OAM)

OAM is a general term used in network management and is typically applied to a series of standard protocols for installing, monitoring, and troubleshooting Metropolitan Area Networks.

When applied to Ethernet – OAM is typically assumed to refer to the layer 2 (MAC layer), management protocols, specifically 802.3ah and 802.1ag. Layer 2 management protocols do not need higher level transport protocols to operate, OAM data is transferred in standard multicast Ethernet frames.

802.3ah OAM: Is a point-to-point protocol designed to verify a specific link between two directly connected devices (over copper or fiber), which support 802.3ah OAM. One device must be configured to be an active OAM device, the other a passive (typically the core switch would be the active device, the end device passive). 802.3ah OAM provides link status, remote fault detection and the ability to initiate a loopback circuit.
(LINK-OAM)

802.1ag: Often referred to as Connectivity Fault Management (CFM), is an end-to-end protocol designed to verify a specific network path between two devices that may well be in different geographical locations. CFM allows the network operator to administer, monitor and debug the network using continuity check (a heart beat message), link trace (similar to traceroot, but operating at the MAC layer) and finally loopback (can be likened to a layer 2 ping).
(SERVICE-OAM)

iView² Management Software

iView² is the IMC Networks management software that features a Graphical User Interface (GUI) and gives network managers the ability to monitor and control the manageable IMC Networks products.

iView² is available in several versions, including a WebServer version 3.0, and can also function as a snap-in module for HP OpenView Network Node Manager and other third party SNMP Management software. For assistance in selecting the right version of iView² for a specific operating system, please visit:

<http://www.imcnetworks.com/products/iview2.cfm>

iView² supports the following platforms:

- Windows 2000
- Windows XP
- Windows Vista
- Windows 7

Please see the SNMP Management Module manual for software configuration options.

iView² (iConfig view)

iView² (iConfig view) is an in-band utility created by IMC Networks, used for SNMP configuration for IMC Networks' SNMP-manageable devices.

The iView² (iConfig view) feature allows the following to be performed:

- Set an IP address, subnet mask and default gateway
- Define community strings and SNMP Traps

iView² (iConfig view) also includes an authorized IP address system and restricted access to MIB groups which are supported by IMC Networks' manageable devices. These extra layers of security do not affect SNMP compatibility. iView² (iConfig view) can upload new versions of the system software and new MIB information. It also includes diagnostic capabilities for faster resolution of technical support issues.

Hardware Mounting Options

The IE-MultiWay can be mounted on a DIN Rail or using a wall mount bracket (shown below). DIN Rail clips (part number 806-39105) and wall mount brackets (part number 895-39229) are available for purchase through an IMC Networks Distributor.



The IE-MultiWay can be mounted with two DIN Rail clips, a hardware option available through IMC Networks. The DIN Rail clips include screws, to allow the installation onto a DIN Rail. Install the screws into DIN Rail clips, which can be mounted parallel or perpendicular to the DIN Rail. Snap the converter onto the clips. To remove the converter from the DIN Rail, use a flat-head screwdriver into the slot to gently pry the converter from the rail. Refer to picture on page 7.

NOTE
<i>The DIN Rail clips are designed for use on a DIN-35 rail.</i>

DIP Switch Selectable Mode Configuration

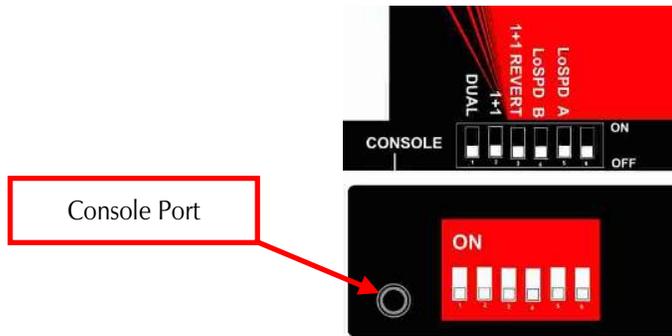
The IE-MultiWay can be configured in one of the following ways via DIP Switch settings (see page 7):

Configuration Method	Description
4-Port Switch (default)	In this mode, the unit acts as a standard 4-port MAC-layer switch.
Dual Converter mode	In this mode, the unit functions as two independent (SFP to TX) media converters and traffic never passes between the two converters.
1+1 SFP Protection Non-Revertive mode	<p>In this mode, the "SFP A" port (fiber or copper) is connected through the switch to the drop ports as the main link. The "SFP B" port (fiber or copper) is active into the MAC switch, but no connection inside the switch is made; in this way, the "SFP B" line is held as the standby line. The "SFP B" line is held in the LINK state for testing and line verification, but does not actively carry user data.</p> <p>When a fault is detected on the active line, all customer traffic is switched to the "SFP B" port. With non-Revertive mode data is not resumed by "SFP A" port until SFP B fails or is disconnected.</p>
1+1 SFP Protection Revertive mode	<p>In this mode, the "SFP A" port (fiber or copper) is connected through the switch to the drop ports as the main link. The "SFP B" port (fiber or copper) is active into the MAC switch, but no connection inside the switch is made; in this way, the "SFP B" line is held as the standby line. The "SFP B" line is held in the LINK state for testing and line verification, but does not actively carry user data.</p> <p>When a fault is detected on the active line, all customer traffic is switched to the "SFP B" port. Once the "A" port is no longer in a fault condition, data is resumed on that port.</p>

NOTE

Revertive and Non-Revertive modes can only operate on the ports with SFPs, not the fixed copper ports.

DIP Switch Configuration

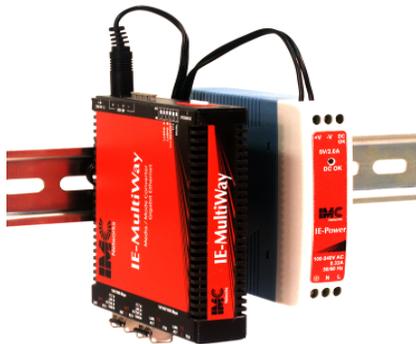


DIP Switch	Name	Description	Default Setting
1	Dual	Enable dual channel	OFF
2	1+1	Provides 1+1 protection with non-revertive switching	OFF
3	1+1 Revert	Provides 1+1 protection with revertive switching	OFF
4	LoSpd B	Optional-for future use	OFF
5	LoSpd A	Optional-for future use	OFF
6	Reserved		

Powering the IE-MultiWay

The IE-MultiWay includes multiple powering options:

- AC adapter
- The 4-terminal DC power block
- An optional IE-Power/5V DIN Rail mount power supply, extended temperature
- An optional IMC Networks Double-USB Power Cable



IE-MultiWay with optional DIN Rail mount power supply

Mini-Serial Port

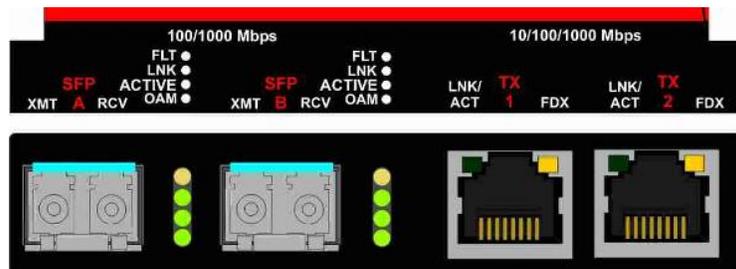
A console port, located next to the DIP Switch bay, allows the customer to use a local RS-232 serial interface for management. A special mini-jack to DB9-F cable is provided with the product for direct connection to a PC serial port.

NOTE

To log on through the serial port, set the computer/terminal for VT-100 emulation, with: 38.4K baud, 8 data bits, 1 stop bit, no parity, no FlowControl.

LED Operation

Each IE-MultiWay includes SFP and RJ-45 LEDs.



SFP LED functions are as follows:

FLT	Glows amber when a fault is detected.
LNK	Glows green with a valid optical link.
ACTIVE	Glows green when the port is active OFF when SFP is in standby (does not indicate activity)
OAM	Glows green when an active OAM AH channel is established.

RJ-45 LED functions are as follows:

LNK/ACT	Glows green when a link is established on the TX port; blinks green when activity is detected on the TX port.
FDX	Glows amber when an FDX link is established on the TX port. Not lit for HDX.

Autocross Feature for Twisted Pair Connections

All fixed twisted pair ports on the IE-MultiWay include AutoCross, a feature that automatically selects between a crossover workstation and a straight-through connection depending on the connected device.

Configuration

The IE-MultiWay includes many features that are configurable via a serial/Telnet session (CLI) or through iView² (SNMP Management view or iConfig view).

Configuration Options

The following options are configurable through both the iView² (iConfig view) and Serial/Telnet.

Feature	iView ²	Serial/Telnet
Loopback	✓	✓
Auto Negotiation	✓	✓
Force Mode	✓	✓
FlowControl	✓	✓
VLANs	✓	✓
IP Address	✓	✓
Subnet Mask	✓	✓
Default Gateway	✓	✓
MIB Community	✓	✓
Traps Assignment	✓	✓
Users	✓	✓
Passwords	✓	✓
Access Level	✓	✓
Reboot	✓	✓
Frame size selection	✓	✓
Bandwidth Limiting	✓	✓

The following table presents management options configurable via iView² (iConfig view) or a serial/Telnet session.

Feature	iView ² (iConfig)	Serial/Telnet
PROM Software Download/Upload	✓	
Telnet Session	✓	✓
Software Download Setup (TFTP)		✓
DHCP		✓
Restore Configuration	✓	✓
Save Configuration	✓	

Basic Device Configuration Using the CLI

After running through an initial self test, the screen will display the following message:
Press **Enter** for Device Configuration.

```
Press <Enter> for Device Configuration
```

Press **Enter** to open the main configuration screen. This screen allows the user to set the IP address and the destination IP address for traps with the community string, read/write access and password as usual.

```
Saved Values. (These values will be active after reboot)
IP Address      - 10.10.10.10
Subnet Mask     - 255.255.255.0           DHCP is Not Active
Default Gateway - 0.0.0.0

Current Values. (These values are in use now)
IP Address      - 10.10.10.10
Subnet Mask     - 255.255.255.0
Default Gateway - 0.0.0.0

Community String: public   Access: r/w

Press I to enter new saved parameter values. Press P to change Password.
Press T to enter new Trap Destination. Press K to remove All Trap Destinations.
Press C to enter new Community String. Press U to remove All Community Strings.
Press E to End session. Type REBOOT to reboot unit. Press D for DHCP On/Off.
Press SpaceBar for additional commands.
```

This screen contains the following information and options:

Saved and Current Values

Saved values display the changes made during the current session and current values display the values currently in use:

- IP Address (IP address of SNMP agent)
- Subnet Mask (mask to define IP subnet to which agent is connected)
- Default Gateway (default router for IP traffic outside of the subnet)

Command List

I = Enter new **Saved Parameter Values**

P = Change the **Password***

T = Enter new **Trap Destinations**

K = Remove **All Trap Destinations**

C = Create **SNMP Community Strings**

U = Delete All **SNMP Community Strings**

E = **End** the session*

Reboot = Reboot the unit (may result in short data loss)

D = Enable or disable **DHCP**

Space Bar = Opens the device specific configuration options screen.

*The screens illustrated in this manual show capabilities for users with Admin rights. Individuals with User-level rights can only view port status and port settings, change their password, end a session, and reboot the unit.

NOTE

*It is necessary to reboot the IE-MultiWay after making any modifications to the Saved Values for the changes to take effect. To reboot, type **Reboot** at the prompt on the Main Configuration screen.*

Assigning IP Information

To modify the Saved Parameter Values (i.e., assign IP address and subnet mask), press **I**. The system prompts for the IP address and subnet mask for the connected device. Press **Enter** after each entry. A default gateway can also be assigned, or press **Enter** to skip. When finished, press **Enter**, then type **reboot** for changes to take effect. The Current Values can only be saved and acted on after the IE-MultiWay has been successfully rebooted.

Password Protection for Serial Port Connections

Password/username is not offered for the serial port by default. This allows the end user to quickly access the device for some basic configuration capability. Password protection is provided for the serial configuration process by pressing **P** on the main configuration screen. Enter a password, keeping in mind that passwords are case-

sensitive and must not exceed eight characters or include spaces, and press **Enter**. This password will be requested whenever logging on. To remove password protection, select **P** and, instead of entering a password, press **Enter**.

Passwords have the following requirements:

- The password must be between 1 and 8 characters long
- The password consists of a combination of any ASCII characters except spaces
- Passwords are case sensitive

Passwords are a way to make the management of the IMC Networks devices secure, but these password lists must be stored and maintained.

Assigning SNMP Trap Destinations

Traps are sent by the manageable device to a management PC when a certain event takes place. To enter a trap destination, press **T**. When prompted, enter a New IP Address prompt, enter the appropriate IP address of the destination device and press **Enter**. Then, type the name of the community string (that the destination device has been configured to accept) and press **Enter**. Select whether the trap is for SNMP version 1 or 2c and press **Enter**. This function enables ALL of the device traps. Supported traps include: Link Down, Link Up, and Last Gasp.

Removing Trap Destinations

To remove all trap destinations, press **K**. Press **Y** to continue to confirm or **N** to abort and remove all trap destinations. Press **Enter** to finish.

This function will delete all trap destinations. To selectively delete trap destinations or to disable/enable Traps, use iView² (iConfig view) to configure the device.

Creating Community Strings

Community strings add a level of security to a network. The default community string is named "public" and has read/write access. For security, "public" should be replaced with custom community strings such as ones created with read-only access (for general use), and another with read/write access (for the administrator).

To create a new community string, go to the main configuration screen and press **C**. Enter the name of the new community (up to 16 characters, no spaces) and press **Enter**. Then type one of the following to assign the community string's access rights:

- **R** = read-only access
- **W** = read/write access
- **Enter** = abort

After entering **R** or **W**, press **Enter**. To finish, press **Enter** and reboot.

Deleting Community Strings

To delete all community strings, perform the following:

Press **U**. The "Are you sure you want to delete all future strings?" prompt is displayed.
Press **Y** when prompted to proceed and delete all community strings, **N** to abort.
Press **Enter** to finish.

This function will delete ALL community strings. To selectively delete community strings, use iView² (iConfig view) to configure the device.

Ending the Session

Press **E** to end a serial port or Telnet/HyperTerminal session before disconnecting the serial cable. This will stop the continuous stream of data to the serial port.

Rebooting the Unit

To reboot the IE-MultiWay, type **reboot** from the main screen or the command menu.

Enabling/Disabling DHCP

To toggle DHCP on the IE-MultiWay between enable and disable, press **D** and then **Y**. Press the **Space Bar** once to return to the main screen without making any changes.

DHCP Disable (Static IP Addressing)

DHCP is disabled in the default configuration. Initially, modules are assigned a Static default IP Address of 10.10.10.10. Changes to the Static IP Address can be added manually through iView² (iConfig view) or a Console session. The changes will be initiated following reboot of the module.

DHCP Enable (Dynamic IP Addressing)

If a DHCP server is present on the network and DHCP is enabled, the DHCP client will initiate a dialogue with the server during the boot up sequence. The server will then issue an IP address to the management card. Once the new IP address is received, the SNMP Management Module will reboot so that the new IP address will take effect. Refer to About Serial Port Configuration for more information about Enabling/Disabling DHCP.

When there is no DHCP server on the network, use the serial configuration to manually set the IP addresses.

When DHCP is enabled, the IP address (default 10.10.10.10 or a previously used IP address, or user-configured) is saved. When DHCP is disabled, the saved IP address will be reinstated and the device will reboot.

DHCP servers give out lease times: devices renew their leases based on the administrator-specified time. If a device cannot renew its lease, and the lease expires, the device will be given the IP address 10.10.10.10 and will reboot.

Commands List (Space Bar)

Command	Description
cleandb	Reboot With Clean Database
download	File Download from TFTP Server
accounts	Add or Delete Username/Password Accounts
vlan	Display And Change VLAN Settings
bw	Display And Change Bandwidth Settings
version	Show Firmware Version
ifstats	Display Port Statistics
rmstats	Display Port RMON Statistics
sysdescr	Change System Descriptions
reboot	Reboot Unit
oam	Display And Change OAM Settings
sfpstats	Display SFP DDMI Info
unit	Display And Change Unit Settings
port	Display And Change Port Settings

->
Press RETURN To Go Back To Main Screen.

The IE-MultiWay also includes several device-specific options. To access these options, press the **Space Bar** from the Main Configuration screen, type the name of the action to be performed (as shown below) and press **Enter**.

Command	Description
cleandb	Reboots the unit with a clean database. This removes all information from the database and sets the unit to factory defaults.
download	Downloads firmware via the TFTP protocol
accounts	Allows the addition for User, Superuser, Admin
vlan	Provides selection of two modes of operation to support all VLAN configurations.
bw	Displays settings for Bandwidth configuration
version	Displays the unit's firmware and hardware version
ifstats	Displays interface statistics
rmstats	Displays remote monitoring (RMON) statistics on packets received as defined in RFC 2819 for RMON.
sysDescr	Allows the editing of sysName, sysDescr, and Port information
reboot	Allows a soft reboot of the unit after changes are made by the end user
oam	Enable/disable OAM
sfpstats	Provides information about the wavelength, serial number, output power,

Command	Description
	BER and other information. Requires an SFP with DDMI.
unit	Unit global settings, frame size selection. Unit OAM enable must be enabled for AH and AG to function.
port	Displays the port status and allows changes to port settings, such as duplex status and speed.

Cleandb

Entering cleandb reboots the unit with its database cleaned depending on the option selected. Users are presented with two, sequential options, first to reset all SNMP settings and, second, to reset all of the unit's configuration to default. Enabling the first option presents the second. Resetting the unit to factory default values (option two) will delete all custom IP and other configurations performed through iView².

Downloading Files

Firmware and/or saved configuration data for the IE-MultiWay can be downloaded via a TFTP connection from a central server via TFTP protocol. Initiate this download via serial configuration or Telnet session. To download a configuration file, type **download** and press **Enter** to be taken to the Download a file screen. This screen displays the IP Address of the TFTP server and the name of the file to be downloaded:

```

----- Download a file from TFTP server -----
IP address of Server: 0.0.0.0
Name of File to download:
Enter New IP Address of TFTP Server: >192.168.10.65      <
Enter New Name of File to Download: >config.scl_ <

```

The TFTP server should be open. Press **Enter** to start downloading the file.

After the transfer process is complete, press **Enter** to load the configuration file:

```

----- Download a file from TFTP server -----
IP address of Server: 0.0.0.0
Name of File to download:
Enter New IP Address of TFTP Server: >192.168.10.65      <
Enter New Name of File to Download: >config.scl  <

Ready to attempt transfer of file from TFTP server to local file storage.
Press RETURN to Continue, or Q to Quit
Transfer Block Counter: 143
An SNMP Configuration file has been downloaded from the TFTP
Server and has been put in local storage.

Press RETURN to load the configuration data from this
file into the device's SNMP configuration area.
Press Q to Not LOAD the configuration data,
but leave the file in local storage.
-

```

Once loaded into the device's SNMP memory area, the system prompts the user to **reboot** the device to make the new configuration active.

Accounts

The following are the three levels for CLI or Telnet account access:

- User:** View status, change own password, and reboot.
- Operator:** All User privileges mentioned above, plus ability to change settings.
- Administrator:** Operator privileges mentioned above, plus ability to add/delete accounts and reinitialize the unit to default settings (cleandb).

VLAN Configuration

The ports can be assigned as a trunk or access port.

```

sysName = MultiWay                               IE-MultiWay
This Device is currently in OPERATION MODE 2
DIP Switch Configuration: 4 Port Switch
-----

SFP A                Port Is Trunk
SFP B                Port Is Access
TX 1                 Port Is Access
TX 2                 Port Is Access

-----

Press Space Bar To Change Value.
Up-Arrow or Dn-Arrow
Save Changes and Exit: F3 or S. Exit without Saving: F4 or Q.

```

When configuring a trunk port, an Ethertype can be user-defined (a trunk port is also defined as a provider port based on 802.1ad). If an Ethertype value comes in a trunk port and is different than the user-defined Ethertype, it will be treated as an unrecognized VLAN tagged frame. If configuring the port as an access port, enter a VLAN ID between 1 and 4,094. Possible priority settings are 0 (lowest priority) through 7 (highest priority).

```

sysName = MultiWay                                     IE-MultiWay
This Device is currently in OPERATION MODE 2
DIP Switch Configuration: 4 Port Switch
-----
          | For Trunk Ports | For Access Ports |
          | Vlan Tag EtherType | VID  Priority    |
SFP A    | 8100              |                |
SFP B    | 88a8              |                |
TX 1     |                    | 21    4        |
TX 2     |                    | 893   2        |
-----
Enter VLAN TAG EtherType, 0000 - FFFF, F2 = Del.
Arrow Keyes for navigation.
Save Changes and Exit: F3 or S. Exit without Saving: F4 or Q.

```

NOTE

When an Ethertype or VLAN ID is assigned, the same values need to be configured at the end device (router, etc) to avoid network configuration problems.

Operational Mode Configuration

There are two modes of operation that can be configured through the Serial/Telnet session: Mode 1, which supports a mixture of tagged and untagged traffic, and Mode 2 Extra tagging.

The configuration screen is accessed by typing **vlan** and pressing **Enter** from the Additional Commands screen. The system displays the current operation mode screen. Press the **Space Bar** to select the other mode.

Operation Mode 1 – Mixed Tagged and Untagged Frames

In this mode, all tagged and untagged frames pass on any given port. Management to the device can be tagged or untagged.

```
sysName = MultiWay                               IE-MultiWay
This Device is currently in OPERATION MODE 1
DIP Switch Configuration:  4 Port Switch
-----
                OPERATION MODE 1 – Mixed tagged and untagged frames
MODE 1 forwards both tagged and untagged frames.
* Device does not act on Ulan tags, they pass through unchanged.
* Management traffic to device accepted from any Port.
* Management traffic to device can be either tagged or untagged.
* Any traffic, including management traffic, allowed to flow
  to/from Ports transparently.
-----
Press Space Bar To Browse Mode Setting, Press RETURN To SET New Mode.
Dn-Arrow to change settings for current mode
Save Changes and Exit: F3 or S. Exit without Saving: F4 or Q.
```

Press the down arrow on the computer keyboard to access additional configuration selections.

```
sysName = MultiWay                               IE-MultiWay
This Device is currently in OPERATION MODE 1
DIP Switch Configuration:  Dual 2 Port Switches
-----
Management Domain Tags:           Tags on Management Traffic
Management Ulan ID:               3159
Management Ulan Priority           0
Xstratags On IEEE Reserved Frames No Tags on IEEE Res. Frames <Trunks>
-----
Press Space Bar To Change Value. Up-Arrow to go back to previous screen.
Dn-Arrow for next setting.
Save Changes and Exit: F3 or S. Exit without Saving: F4 or Q.
```

WARNING

If a VLAN # is added to a port and is the same VLAN # assigned for a tag on management traffic, saving these changes will disrupt management indefinitely.

Operation Mode 2 Port Based Xtra Tagging

Any port can be configured for extra tags on the frames.

```
sysName = MultiWay                               IE-MultiWay
This Device is currently in OPERATION MODE 1
DIP Switch Configuration:  4 Port Switch
-----
                OPERATION MODE 2 - Port based Xtra tagging.
In MODE 2 any port can be defined for Xtra tagging
* A port defined for Xtra tagging is called a Trunk, others are Access ports.
* Tagged traffic flows freely between Trunks. No adding or deleting of tags.
* Untagged or improperly tagged frames do not flow between Trunks.
* One tag will be removed in traffic from Trunk ports to Access Ports.
* Frames arriving on an Access port will be given an extra tag with
  UID and Priority, as defined for that specific Access Port.
* The extra tag is inserted in front of any other tags already in the frame.
* Management traffic to device accepted from any Trunk port.
* Management accepted from Access ports if Port UID matches Mgmt. domain.
-----
Press Space Bar To Browse Mode Setting. Press RETURN To SET New Mode.
Dn-Arrow to change settings for current mode
Save Changes and Exit: F3 or S. Exit without Saving: F4 or Q.
```

Press the down arrow on the computer keyboard to access the additional configuration commands.

Bandwidth (bw)

Displays settings for Bandwidth configuration.

```
----- Bandwidth Control Settings -----
                                     SFP A           SFP B
Ingress Bandwidth Limit 0 = None (bits/s)  0           0
Max Burst Allocation Size (bits)           0           0
Ingress Burst Allocation 0 = Max (bits)    300000      0
Egress Traffic Shaping 0 = None (bits/s)  0           0
                                     TX 1           TX 2
Ingress Bandwidth Limit 0 = None (bits/s)  0           0
Max Burst Allocation Size (bits)           0           0
Ingress Burst Allocation 0 = Max (bits)    0           0
Egress Traffic Shaping 0 = None (bits/s)  0           0
OSI Level Used In Calculations             Layer 1
Unit Rate Control Enable/Disable           Enabled
Use Arrow Keys To Move Cursor To Other Fields. Enter New Value.
Press RETURN To Set New Value. Press Q Or F4 To Exit.
```

SFP A/B Ports

Ingress Bandwidth Limit (CIR)

Monitors the traffic entering the unit (ingress), discarding traffic that exceeds a fixed Committed Information Rate (CIR) plus Burst Allocation (BA). Frames are not held in queue, they either meet the bandwidth limits and are accepted into the unit or they are dropped.

Max Burst Allocation size (BA)	The BA size is specified in bits; the # of bits above the bandwidth limit before packets are thrown away.
Ingress Burst Allocation	Bandwidth Limiting can be set at Ingress of each port individually by setting the MAX Bandwidth Limit in bits/Sec. and the BA in bits. Traffic in excess of the Bandwidth limit plus BA for any time interval will be dropped. This function utilizes an advanced “Leaky Token-Bucket” algorithm to provide typical resolution under 5% of the set values at all data rate and frames sizes.
Egress Traffic Shaping	Egress Traffic shaping actively controls the transmitter and hard limits the maximum frame rate that can be sent. Frames can be delayed in the internal buffers of the unit, waiting their turn to be sent. If the internal buffers are full, excess traffic will be dropped. The Unit Rate Control can be used to alleviate this.
TX1/2 Ingress Bandwidth Limit (CIR)	Monitors the traffic entering the unit (ingress), discarding traffic that exceeds a fixed Committed Information Rate (CIR) plus Burst Allocation (BA). <u>Frames are not held in queue</u> , they either meet the bandwidth limits and are accepted into the unit or they are dropped.
Max Burst Allocation size (BA)	The BA size is specified in bits; the # of bits above the bandwidth limit before packets are thrown away.
Ingress Burst Allocation	Bandwidth Limiting can be set at Ingress of each port individually by setting the MAX BW Limit in bits/Sec. and the BA in bits. Traffic in excess of the Bandwidth limit plus BA for any time interval will be dropped. This function utilizes an advanced “Leaky Token-Bucket” algorithm to provide typical resolution under 5% of the set values at all data rate and frames sizes.
Egress Traffic Shaping	Actively controls the transmitter and hard limits the maximum frame rate that can be sent. Frames can be delayed in the internal buffers of the unit, waiting their turn to be sent. If the internal buffers are full, excess traffic will be dropped. The Unit Rate Control can be

used to alleviate this.

OSI Level Used in Calculations

Choose Layer 1, 2 or 3 for the counter, this will determine how many bytes from the Ethernet frame are to be included in the calculations.

(Open Systems Interconnect, referring to the seven layers for TCP/IP)

Layer 1: Preamble + DA to CRC + IFG
Layer 2: Frames DA to CRC
Layer 3: Frames DA to CRC – 18
(- 4 if frame is tagged)

Explanations:

Preamble = 8 bytes
DA = EtherNet Destination Address
CRC = EtherNet Checksum
IFG = 12 bytes

Unit Rate Control Enable/Disable

Allows the end user to globally configure all Bandwidth settings when enabling Unit Rate Control (Flow Control). If the END device connected to the port also has Flow Control enabled, this will ensure packets will not be dropped.

*OSI NOTES

The Bandwidth Limit functions can be adjusted to only count the Layer 1, 2, or 3 portions of the physical line rate. Layer 1 is used to relate Bandwidth to the physical line rate where a 100BaseT Ethernet line can carry a MAX bandwidth of 100Mbps. Layer 2 may be more useful when the Ethernet Frame may be carried over several different physical protocols such as SONET or SDH. Only the bandwidth required by the Ethernet frame is counted, making this a more consistent number over different protocols. Layer 3 counting could be used when a relationship to the actual customer data or line payload is required. If a 10 Mbps customer file needs to be sent in one second, then a minimum bandwidth limit of 10Mbps would need to use Layer 3 counting to allow this.

It must be noted that only Layer 1 counting is not affected by the size of the Ethernet frame. At 64 byte Ethernet frames, the MAX bandwidth the line can support at Layer 2 is only 76.2% of the line rate. This maximum falls to 54.8% of the line rate when counting is further limited by only counting Layer 3 payload data.

Version

Entering **version** will display the version of the firmware operating the IE-MultiWay. Settings should be saved prior to reboot.

Viewing Port Statistics (ifstats)

To view port statistics on the IE-MultiWay, enter ifstats. This will open a screen displaying information on packets received and transmitted as defined by MIB-II standard RFC 1213.

Pressing the **Space Bar** will refresh the data on the screen.

```
->ifstats
MIB-II Var
```

	SFP A	SFP B	TX 1	TX 2
PhysAddress	0000290262E2	0000290262E2	0000290262E2	0000290262E2
AdminStatus	1	1	1	1
OperStatus	1	1	2	1
LastChange	5894956	5665750	142	5663442
InOctets	5382096	7556480	0	7174046
InUcastPkts	0	10828	0	16405
InNUcastPkts	57872	68001	0	58095
InErrors	0	0	0	0
InUnknownProt	0	0	0	0
OutOctets	12468585	11953238	0	13565810
OutUcastPkts	677	9373	0	20039
OutNUcastPkts	125398	115581	0	124763
OutDiscards	0	0	0	0
OutErrors	0	0	0	0

```
Press SpaceBar to refresh, Any other key to exit_
```

Viewing Port RMON Statistics (rmstats)

To view port RMON (Remote MONitoring) statistics on the IE-MultiWay, enter rmstats. This will display RMON information on packets received as defined in RFC 2819 for RMON.

Pressing the **Space Bar** will refresh the data on the screen.

```

->rmstats
RMON Counter          SFP A          SFP B          TX 1          TX 2
-----
DropEvents            0              0              0              0
Octets                5385537       7570978       0              7183822
Pkts                  57909         78978         0              74599
BroadcastPkts        0              124           0              19034
MulticastPkts        57909         68021         0              39132
CRCAlignErrors       0              0              0              0
UndersizePkts        0              0              0              0
OversizePkts         0              0              0              0
Fragments            0              0              0              0
Jabbers              0              0              0              0
Collisions            0              0              0              0
Pkts64Octets         12644         12888         0              13404
Pkts65to127          162559        182051         0              196999
Pkts128to255         4662          4687          0              4730
Pkts256to511         4333          4402          0              4456
Pkts512to1023        0              14            0              34
Pkts1024toMAX        0              0              0              0
Press SpaceBar to refresh, Any other key to exit

```

System Description (sysDescr)

The sysDescr allows the end user to enter a description for the IMC Networks device. Within the iView² GUI, a name or some kind of identifier can be entered into the text box labeled **Description**. Once that description is saved, the identifier will be maintained, even if power is interrupted to the unit.

Reboot

Entering reboot will save settings and reboot the IE-MultiWay.

(Operation and Administration Management) OAM

```

-----
OAM Settings
-----
LB Ignore RX          SFP A          SFP B
LB Status             Process Loopback
OAM Enable           NoLoopback
Oper Status           Enabled
OAM Mode              Passive Wait
Sym Per Events        Enabled
Frame Events          Enabled
Frm Secs Evnts       Enabled
Frm Peri Evnts       Enabled

LB Ignore RX          TX 1           TX 2
LB Status             Process Loopback
OAM Enable           NoLoopback
Oper Status           Disabled
OAM Mode              Disabled
Sym Per Events        Passive
Frame Events          Enabled
Frm Secs Evnts       Enabled
Frm Peri Evnts       Enabled
Use Arrow Keys To Move Cursor. Press Space Bar To Change Value.
Press RETURN To Set New Value. Press Q Or F4 To Exit.

```

Two modes of operations control the OAM function, Passive and Active. Passive mode is the default mode.

OAM AH passive/active is available on the fiber SFP ports and TX ports

- Supports Discovery functions on the SFP ports.
- Supports reporting OAM Flag Events (Link Fault, Critical Event, and Dying Gasp)
- Supports Loopback

Viewing SFP Statistics (sfpstats)

To view SFP statistics on the IE-MultiWay, enter sfpstats. This will open a screen displaying SFP information, including vendor, serial number, bit rate and other options.

Pressing the **Space Bar** will refresh the data on the screen.

SFP Information	SFP A	SFP B
Vendor Name	IMC Networks	IMC Networks
Vendor OUI	000000	000000
Serial Number	MTC0701021234	MTC0701021242
Part Number	HTSFP-24-1111F	HTSFP-24-1112F
Bit Rate	1300000000	1300000000
WaveLength nM	1111	1112
Temperature C		
Voltage V		
Bias cur. mA		
TX Power mW		
TX Power dBm		
RX Power mW		
RX Power dBm		

Press SpaceBar to refresh, Any other key to exit_

Unit

Advertise FlowC and **Force FlowCtrl** - This is the FlowControl feature.

- When using FlowControl functionality on any port, enable Global FlowControl. Then, configure each port individually.
- When using Auto Negotiation and FlowControl, set Advertise FlowC to Advertise Flow and set Force FlowCtrl to Flow Auto.
- Set Advertise FlowC to No Flow to disable FlowControl on a given port.
- When using FlowControl and Force Mode on a given port, set Advertise FlowC to Advertise Flow and set Force FlowCtrl to Frc FlowCt.

Unit FlowControl This enables/disables FlowControl functionality on the unit and must be enabled for FlowControl to function on any port.

Unit FlowControl displays the following screen:

```

----- Unit Control Settings -----
Unit FlowControl          Disable FlowControl Globally
Unit Max FrameSize       Max Framesize:          10240
Boot Trap Delay, Seconds  0
Unit OAM Enable          OAM is enabled <Peering OAM PDUs>

Use Arrow Keys To Move Cursor. Press Space Bar To Change Value.
Press RETURN To Set New Value. Press Q Or F4 To Exit.

```

Unit FlowControl globally enables “Pause” frames to be sent.

Port Configuration (port)

Serial/Telnet sessions display port status as well as allowing configuration of some port features. Type **port** and press **Enter** to be taken to the Port screen. From this screen, view the port speed, duplex and link status.

```

----- Port Status Values -----
                SFP A          SFP B          TX 1          TX 2
SFP Status      No SFP Inst    Fiber 1G FDX  N/A          N/A
Link Status     Up                Up            Down
Link Lost Cntr  0                    0
Duplex Status   Full              Full          Half
Port Speed      1000 Mbits        100 Mbits    1000 Mbits

----- Port Control Settings -----
                SFP A          SFP B          TX 1          TX 2
Port Enable     Enabled           Enabled       Enabled       Enabled
Admin Status   Up                Up            Up            Up
Port Speed Ctrl Autoneg.         Autoneg.     Autoneg.     Autoneg.
Advertise Ctrl Advert All      Adv 1G FDX   Advert All    Advert All
Advertise FlowC Adv Flow        Adv Flow     Adv Flow     Adv Flow
Force FlowCtrl Frc FlowCt     Frc FlowCt   Frc FlowCt   Frc FlowCt

Unit FlowCtrl   Dis. FlowC

Use Arrow Keys To Move Cursor. Press Space Bar To Change Value.
Press RETURN To Set New Value, Press Q Or F4 To Exit.

```

The Port screen contains the following commands:

- | | |
|------------------------|---|
| Port Enable | Enable/Disable the port. (Select Enable to enable the port.) |
| Admin Status | Set Administration level. (Select UP to enable management through the port.)
Both settings must be enabled to enable the port. |
| Port Speed Ctrl | Set the port manually or for Auto Negotiation. |
| Advertise Ctrl | This is the Selective Advertising feature. Selective Advertising, when used in combination with Auto Negotiation, advertises the configured speed and duplex mode for the twisted pair ports. Auto Negotiation must be enabled for Selective Advertising. |

NOTE

<i>Selective Advertising must be used when connecting to a device that auto negotiates and a specific speed and duplex mode is desired.</i>

Using iView²

iView² is IMC Networks' management software, providing network management in an easy to use GUI. Once iView² is installed on a network management PC using a Windows operating system, use the Start menu to access iView².

NOTE

<i>Windows SNMP services must be installed to receive traps.</i>
--

The autoscan feature of iView² will detect IMC Network devices on an active subnet and list them in the network outline. Click the connection for the IE-MultiWay to open its iView² screen. To perform additional configuration, select the iView² iConfig view icon on the toolbar in iView². This allows a session to be launched, and the default password/username is admin/admin. Additional private usernames and passwords can be entered in the USERS tab. If the list of passwords is not maintained, the usernames and passwords can be reset by opening a CLI session and typing in the cleandb command. This will reset all but the IP address of the device.



The following functions can be performed via iView²:

Function	Description
Unit Configuration	Display/modify unit information
Port Configuration	Display/modify port data
Bandwidth	Displays settings for Bandwidth configuration
Tables	Display statistics tables, including Unit and Port tables, RMON statistics, MIB-II ifTable and SFP Info.
VLAN	Provides configuration for VLAN IDs per port
Advanced	Reboot the module; also allows boot trap delay
OAM AH	Configure passive and active 802.3ah
OAM CFM	Perform administrative configuration functions
Agent Info	Displays SNMP agent data

Unit Configuration

Select Unit Configuration to display/modify unit information including IP address (display only, modification not allowed), global flow control, maximum frame size and OAMPDU:

The screenshot displays the 'Unit Configuration' page of the IE-MultiWay web interface. At the top, there is a navigation bar with tabs for 'Unit Configuration', 'Port Configuration', 'Bandwidth', 'Tables', 'VLAN', 'Advanced', 'OAM AH', 'OAM CFM', and 'Agent Info'. The main content area features a large graphic of the device's front panel, labeled 'IE-MultiWay 10/100/1000 Mbps Ethernet Media/Mode Converter'. Below this graphic, the 'Unit Configuration' section is visible, containing a 'Refresh' button, a 'Description' field with a 'Save Changes' button, an 'IP Address' field showing '192.168.10.196', and a 'Global Flow Control' dropdown menu set to 'Disabled' with a 'Save Changes' button.

NOTE

Entering a descriptor in the Description field can make it easier to track down the source of a Trap.

Port Configuration

Select Port Configuration to display/modify port information including description and flow control:

Bandwidth

Select Bandwidth to display configure bandwidth settings for each port.

Bandwidth Configuration Refresh

	SFP A	SFP B
Ingress Bandwidth Limit 0 = None (bits/s)	0 <input type="text"/>	0 <input type="text"/>
Max Burst Allocation Size (bits)	0 <input type="text"/>	0 <input type="text"/>
Ingress Burst Allocation 0 = Max (bits)	0 <input type="text"/>	0 <input type="text"/>
Egress Traffic Shaping 0 = None (bits/s)	0 <input type="text"/>	0 <input type="text"/>

	TX 1	TX 2
Ingress Bandwidth Limit 0 = None (bits/s)	0 <input type="text"/>	0 <input type="text"/>
Max Burst Allocation Size (bits)	0 <input type="text"/>	0 <input type="text"/>
Ingress Burst Allocation 0 = Max (bits)	0 <input type="text"/>	0 <input type="text"/>
Egress Traffic Shaping 0 = None (bits/s)	0 <input type="text"/>	0 <input type="text"/>

OSI Level Used in Calculations	Layer 1 <input type="text"/>
Unit Rate Control Enable/Disable	Disabled <input type="text"/>

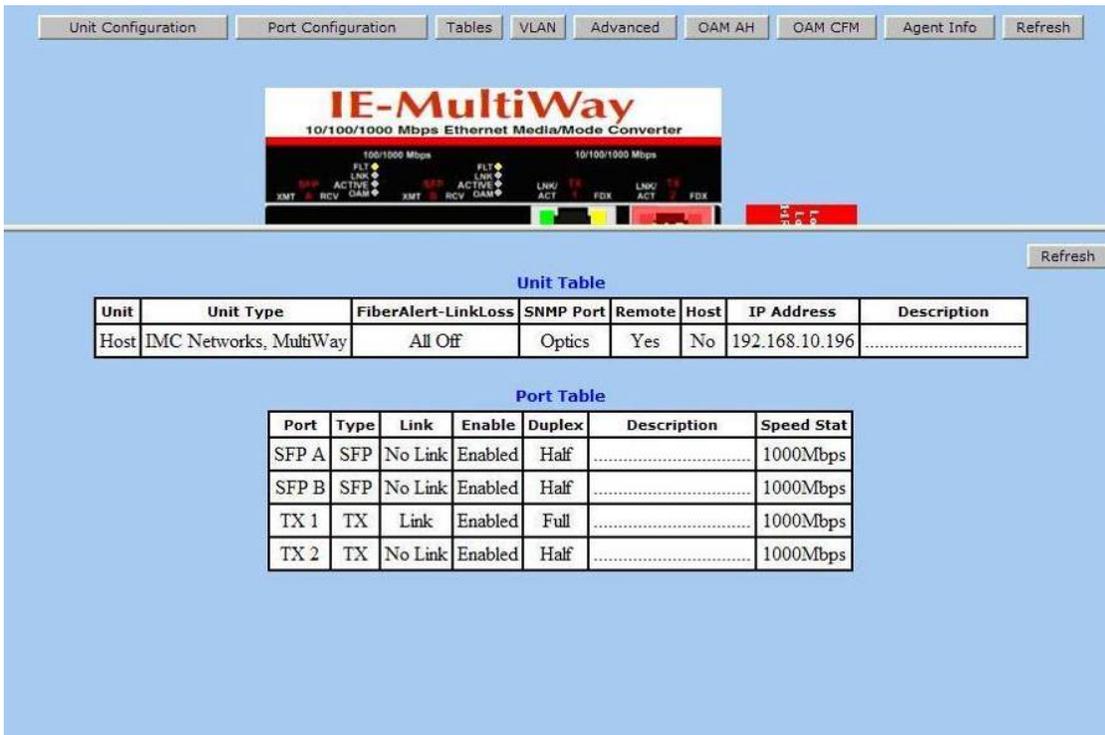
Save Changes

Tables

Select tables to display a screen from which to select the specific statistics to be viewed:



Select Unit and Port Tables to display the following information:



VLAN

Enter a VLAN ID between 1 and 4,094; possible priority settings are 0 (lowest priority) through 7 (highest priority).

The screenshot shows the 'VLAN Configuration (Dual 2 Port Switch)' page. The configuration is as follows:

- Operation Mode: 2 - Port Based Extra Tagging, Infrastructure Mode
- Management Domain Tags: Tags on Management Traffic
- Management VLAN ID: 3159
- Management VLAN Priority: 0
- Extra Tags on IEEE Reserved Frames: No Tags on IEEE Reserved Frames (Trunks)

Port	Type	VLAN EtherType	VLAN ID	Priority
SFP A	Access		1	0
SFP B	Access		1	0
TX 1	Access		1	0
TX 2	Access		1	0

WARNING

If a VLAN # is added to a port and is the same VLAN # assigned for a tag on management traffic, saving these changes will disrupt management indefinitely.

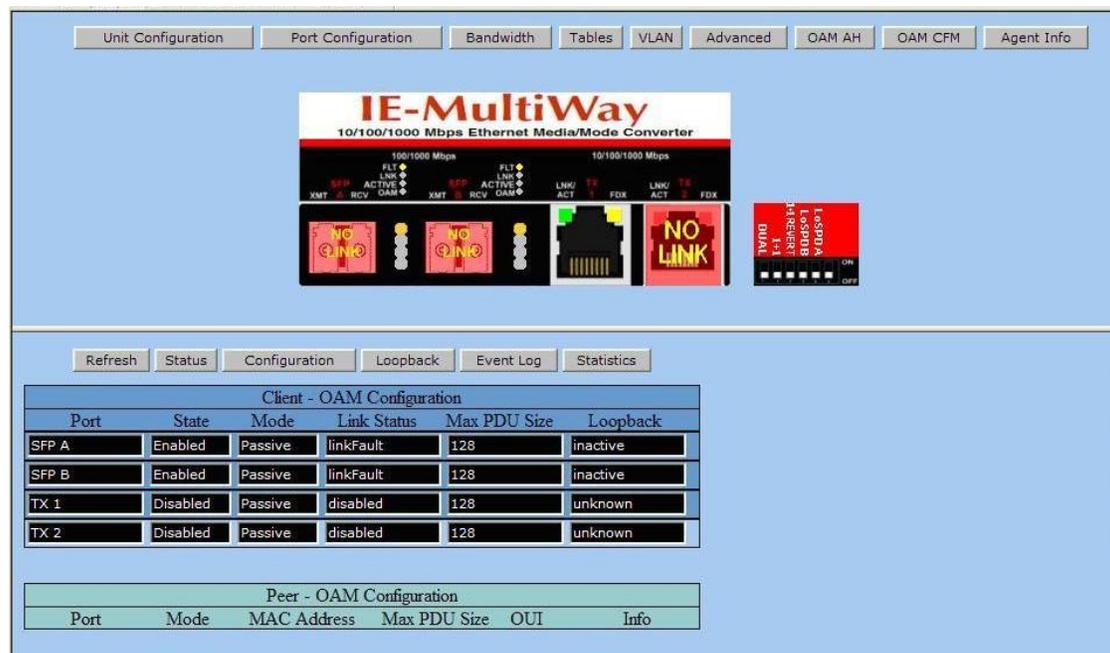
Advanced

Select Advanced to reboot the module:



OAM AH

Select OAM AH to display the following screen and monitor the status, configuration, loopback, event log and statistics:



From the above screen, select Configuration to display state and event configuration information as well as OAM supported functions:

The screenshot displays a network configuration interface with several tabs at the top: Unit Configuration, Port Configuration, Bandwidth, Tables, VLAN, Advanced, OAM AH, OAM CFM, and Agent Info. Below these, there are buttons for Refresh, Status, Configuration, Loopback, Event Log, and Statistics. The main content area is divided into three sections:

Client - OAM State Configuration

Port	State	Mode	Status	Max PDU Size(octets)	
SFP A	Enabled	Passive	linkFault	128	Set
SFP B	Enabled	Passive	linkFault	128	Set
TX 1	Disabled	Passive	disabled	128	Set
TX 2	Disabled	Passive	disabled	128	Set

Client - OAM Event Configuration

Port	Symbol	Frame	Frame Period	Frame Seconds	
SFP A	Enabled	Enabled	Enabled	Enabled	Set
SFP B	Enabled	Enabled	Enabled	Enabled	Set
TX 1	Enabled	Enabled	Enabled	Enabled	Set
TX 2	Enabled	Enabled	Enabled	Enabled	Set

Client - OAM Supported Functions

Port	Unidirectional	Loopback	Event	Variable Length
SFP A	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SFP B	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
TX 1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
TX 2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

At the bottom of the interface, there is a table with columns: eived, Source Address, Enterprise, Type, and Community.

Loopback Testing

The IE-MultiWay includes Loopback testing functionality. This feature is selectable via iView2 within the OAM AH configuration. The menu of choices for all ports includes:

- Terminate/initiate
- Process/ignore

OAM Loopback is controlled by using the “Loopback” and “Ignore Rx” control parameters. Selecting “Initiate” from the “Loopback” control tells the client to start a loopback process with the peer. Selecting “Process” from the “Ignore Rx” control tells the client to process received loopback commands.

Only AH “Active” units can send a Loopback command to a remote unit. Either Active or Passive AH units can respond to a Loopback command, but must be configured to process these commands or they will be ignored.

Select Loopback to display loopback data and define how loopback is configured:

Client - OAM Configuration

Port	Status	Loopback	Ignore Rx
SFP A	No Loopback	Terminate	Process
SFP B	No Loopback	Terminate	Process
TX 1	Unknown	Terminate	Process
TX 2	Unknown	Terminate	Process

OAM Loopback is controlled using the "Loopback" and "Ignore Rx" control parameters.

Selecting "Initiate" from the "Loopback" control tells the client to start a loopback process with the peer.

Selecting "Process" from the "Ignore Rx" control tells the client to process received loopback commands.

Select Event Log to display the OAM event log showing fault changes that have occurred via OAM configuration:

Client - OAM Event Log

Timestamp	Format	Type	Location	Event Window	Event Threshold	Log Value	Running Total	Event Total
0:8:39:11.54	IEEE 802.3	Errored Symbol	Local	125000000	1	1	1	1
0:8:39:12.42	IEEE 802.3	Link Fault	Local	N/A	N/A	N/A	1	1

The OAM Event Log table displays a history of the threshold crossing events and non-threshold crossing events that have occurred at the Ethernet OAM AH Level. There is a maximum of 8 events that can be displayed. When the maximum number of events is reached older entries are deleted to make room for newer entries.

Select Statistics to display OAM statistics:

Client - OAM Statistics				
	SFP A	SFP B	TX 1	TX 2
Information Tx	0	27488	0	0
Information Rx	0	27487	0	0
Unique Event Notification Tx	0	1	0	0
Unique Event Notification Rx	0	0	0	0
Duplicate Event Notification Tx	0	2	0	0
Duplicate Event Notification Rx	0	0	0	0
Loopback Control Tx	0	0	0	0
Loopback Control Rx	0	0	0	0
Variable Request Tx	0	0	0	0
Variable Request Rx	0	0	0	0
Variable Response Tx	0	0	0	0
Variable Response Rx	0	0	0	0

OAM CFM

Select OAM CFM to display the following screen and perform administrative control for Maintenance Domains (MDs), Maintenance Associations (MAs) and Maintenance Association End Points (MEPs). The page contains a list of the local MEPs and provides menu controls to access the administrative functions associated with Create, Delete, and List MD, MA, and MEP information. An example of a default OAM CFM Configuration page is shown below:

Unit Configuration | Port Configuration | Bandwidth | Tables | VLAN | Advanced | OAM AH | OAM CFM | Agent Info

IE-MultiWay
10/100/1000 Mbps Ethernet Media/Mode Converter

100/1000 Mbps | 10/100/1000 Mbps

FLY | LNK | LNK | LNK | TX | TX
ACTIVE | ACTIVE | ACT | FDX | FDX
XMT | RCV | OAM | XMT | RCV | OAM

NO LINK | NO LINK | NO LINK

OAM CFM - Maintenance Association End Point (MEP) Configuration

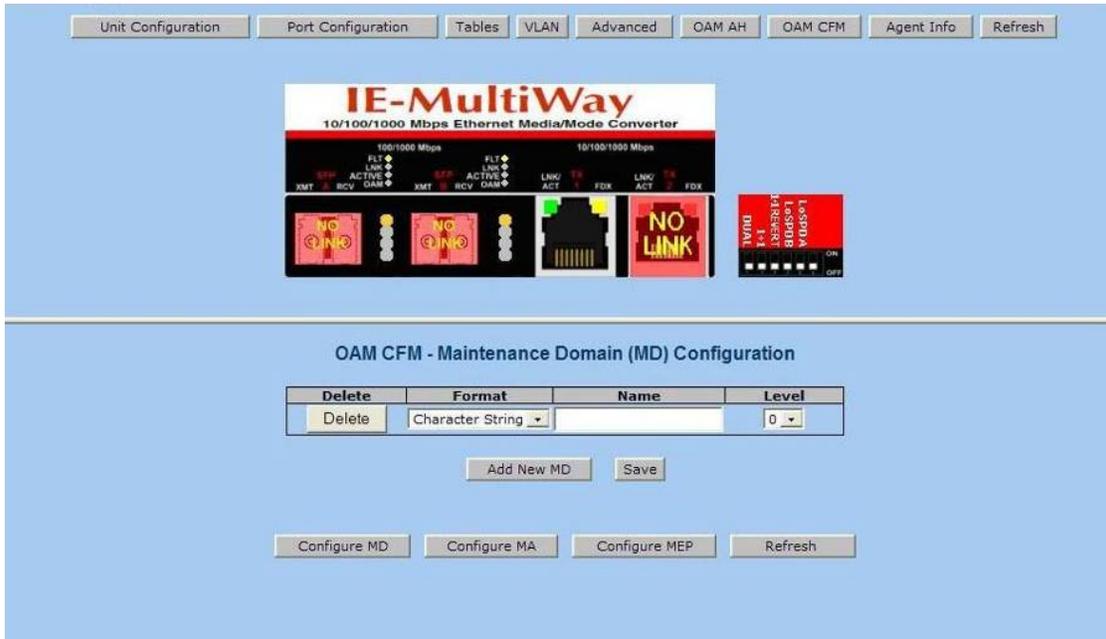
Delete	MD	MA	MEP ID	Type	Port	Direction	Primary VID	State
<input type="checkbox"/>	TestMD1	TestMA1	1	MEP	SFP A	Ingress (Down)	0	●

Add New MEP | Save

Configure MD | Configure MA | Configure MEP | Refresh

The OAM CFM Configuration page defaults to the “Configure MEP” selections.

For the first-time configuration, the user must first create an MD, then an MA, then local and peer MEPs can be added. To create an MD, select the "Configure MD" button to display the OAM CFM Maintenance Domain Configuration page as shown below:



NOTE

iView² will automatically display this page if there is no MD yet defined when the user attempts to access any other menu control.

Enter the MD name and select the level for the domain. To cancel the MD, select **Delete**. To store the MD, press **Save** and the screen is refreshed.

For the first configuration, create an MA after the MD. Select "Configure MA" to display the OAM CFM Maintenance Association Configuration screen as shown below:

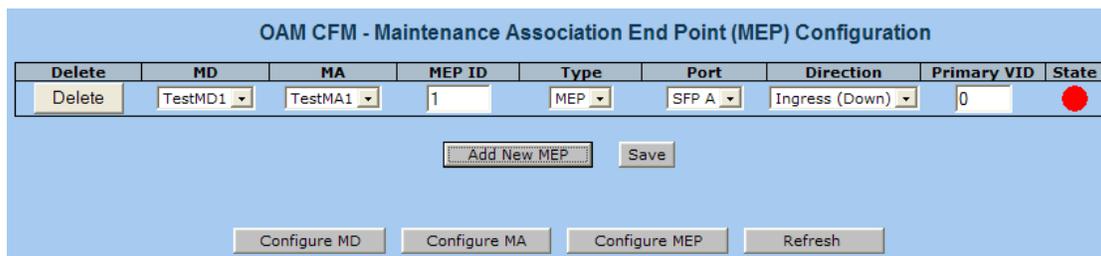


NOTE

iView² will automatically display this page if there is no MA yet defined when the user attempts to access any other menu control.

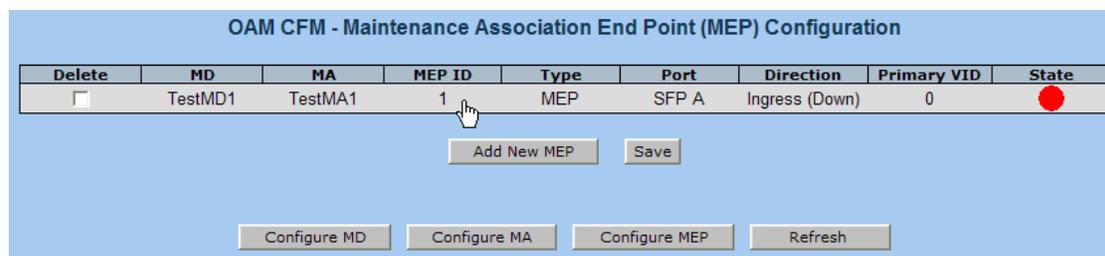
Select the **Domain** and **Format**, and enter the MA name in the **Name** field. Use **Interval** to select the interval for continuity check messaging, and choose **Primary VID**, if applicable. To cancel the MA without saving, select **Delete**. To store the MA, select **Save** and the screen is refreshed.

For a first time configuration, the next step is to create a MEP. Select **Add New MEP** to display the OAM CFM MEP configuration page as shown below:



Select the MD, MA, enter the MEP ID, select the appropriate type, port and direction, and select the **Primary VID**, if applicable. To cancel the MEP without saving, select **Delete**. To store the MEP, select **Save** and the screen is refreshed.

Once the user has configured the MD, MA and at least one MEP, a particular instance of an MEP can be accessed for more detailed configuration. To access a particular instance of an MEP, click on the row containing the desired MEP as shown below:



The current state of the MEP is shown by the color in the "State" column.

Color	Description
Green	Correctly functioning MEP—all MEP's are active and sending CCMs
Red	Idle state or problem associated with the MEP
Yellow	Not all peer MEP CCMs are being received.

Moving the mouse over the displayed color displays a comment giving additional information about the current state. Valid comments are:

- MEP is Idle
- MEP is Active
- Remote MEP Idle
- Remote MEP Failed

The MEP Instance Configuration page offers more details about an individual MEP as shown below:

OAM CFM - Maintenance Association End Point (MEP) Instance Configuration

MD	MA	MEP ID	Type	Port	Direction	Primary VID
TestMD1	TestMA1	1	MEP	SFP A	Ingress (Down)	0

Continuity Check

Enable	CCM Sent
Enable <input type="button" value="Set"/>	149,780

Instance State Details

Admin State	Last Defect	MAC Address
Active	defXConCCM	00:00:29:02:9D:01

Peer MEPs

Delete	Peer MEP ID	State
<input type="checkbox"/>	2	●

Loopback

Peer MEPID	Peer MAC Address	To Send
2	00:00:00:00:00:00	1

In-Order	Out-Of-Order	Bad MSDU
0	0	0

From this screen, the user can perform the following functions:

Function	Description
Continuity Check	Enable/disable CCMs and verify the number of CCMs that have been sent.
Instance State Details	Verify the current administrative state of the MEP, view the last defect identified by the MEP, and view the MAC address of the MEP.
Peer MEPs	Create/List/Delete Peer MEPS associated with the MEP
Loopback	Activate loopback and see the results of loopback operations.

Agent Info

Select Agent Info to display SNMP agent data:

The screenshot displays the web interface for an IE-MultiWay 10/100/1000 Mbps Ethernet Media/Mode Converter. The top navigation bar includes tabs for Unit Configuration, Port Configuration, Bandwidth, Tables, VLAN, Advanced, OAM AH, OAM CFM, and Agent Info. The main content area features a status panel with two 100/1000 Mbps ports, each showing 'NO LINK' and 'NO LINK' indicators. A central Ethernet port is also shown with a 'NO LINK' indicator. To the right, there is a red 'NO LINK' indicator and a 'DUAL' indicator. Below the status panel, there is a 'Refresh' button and a 'SNMP Agent Information' section. The SNMP Agent Information section lists the following details:

Field	Value
BIOS Date	05/17/10
Build Date	2011/03/15 14:17
Version	123-00A1.bin
IP Address	192.168.10.196
Up Time	0:22:6:59.2
Serial Number	99999998
Part Number	858-11121-A1
Mfg. Date	0315

Copyright 2002-2011 IMC Networks, Inc.

The interface also includes a 'Made in USA' logo and the IMC Networks logo with the tagline 'Making Your Network Better'.

Connecting the IE-MultiWay to an iMcV-Giga-FiberLinX-II

If the IE-MultiWay is being set up as a Remote (CPE) to a Host connection with an iMcV-Giga-FiberLinX-II, iView² provides support for SNMP management of the pair. Several pairs can be managed via UMA through the SNMP management module on the same IP address.

For information or instructions on the use of Unified Management Agent (UMA) refer to the SNMP Management module manual. Please refer to www.imcnetworks.com.



Configuration File Save/Restore Function

Requirements

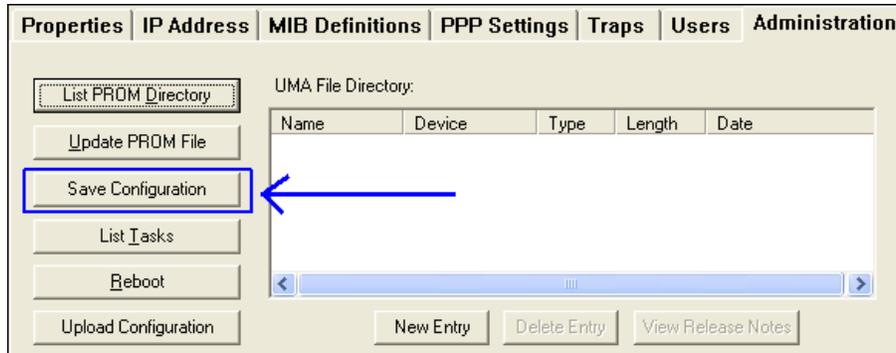
The Configuration File Save/Restore Function allows a user the ability to backup all the configuration settings of a unit. With this backup, a user can restore settings to a unit if necessary or use this backup to apply the same settings to a different unit.

All configurable managed objects are saved in a configuration file that is stored in the unit's Large File Area. This includes all configurable settings such as VLAN configurations, IP Address configuration and SNMP agent settings. The configuration file can be transferred from the unit to a PC and saved to disk through the iView² (iConfig view) protocol. The configuration file can be transferred from a PC to a unit of the same type through iView² (iConfig view) or TFTP into the unit's Large File Area. After the transfer is complete, the unit copies the configuration to flash and reboots.

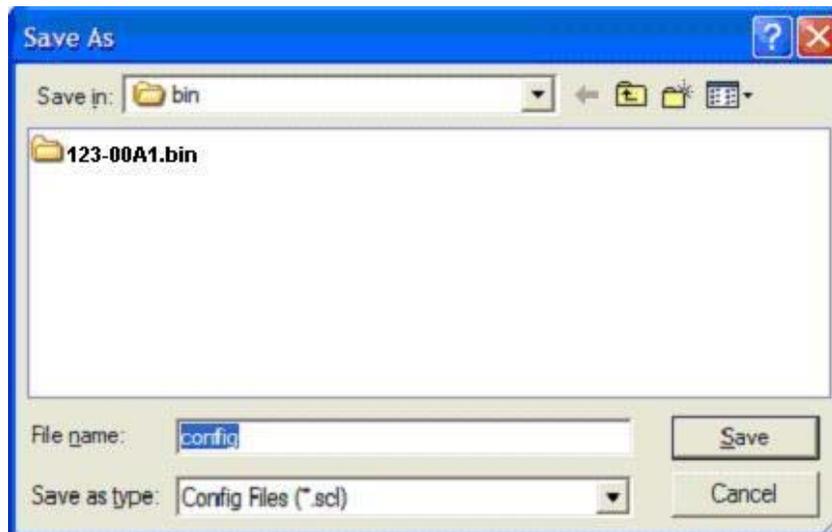
The configuration file's contents is device-type specific and can be identified by iView² (iConfig view) as a configuration file as well as to what type of device it is applicable to.

Saving a Configuration File to Disk:

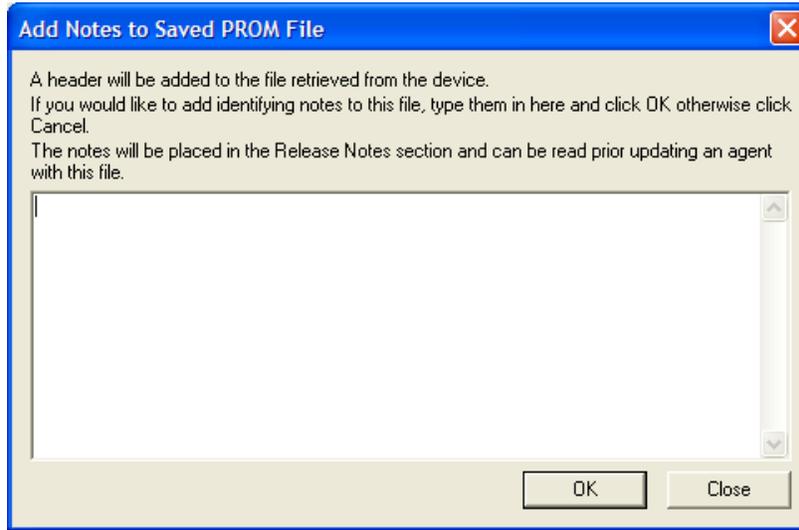
From the Administration Tab in iView² (iConfig view) click the **Save Configuration** button:



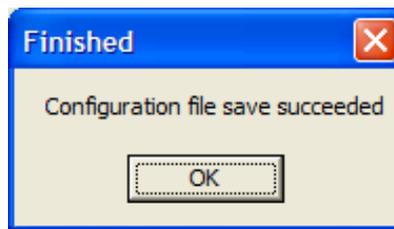
The user is prompted for a filename:



The user is prompted to enter any notes to the header of the saved file for future reference when uploading the file through iView² (iConfig view):

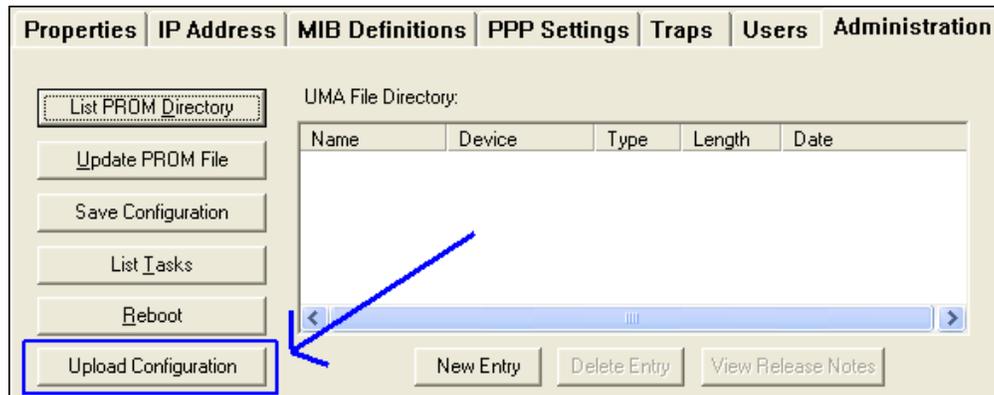


After the file transfer from the device to disk, the user is notified of the status:

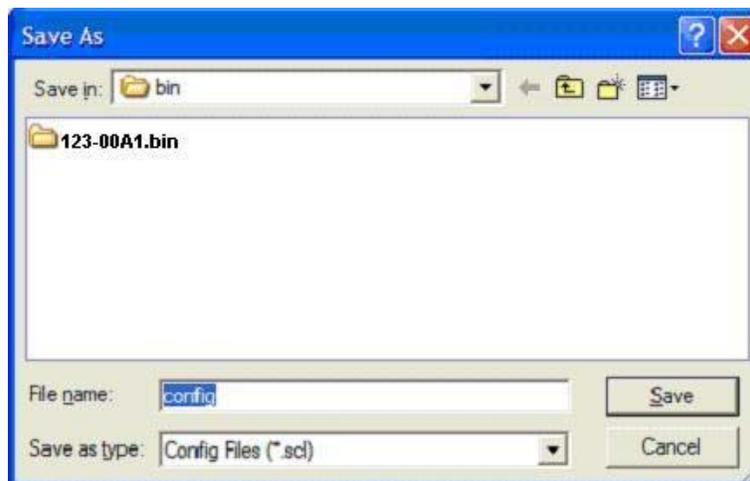


Uploading a Saved Configuration File through iView² (iConfig view)

From the Administration Tab in iView² (iConfig view) click the **Upload Configuration** button:



The user will be prompted to select a configuration file. Once selected, the user can also view any notes that were added when the file was saved:



After selecting the configuration file, the file upload process begins; when completed, the user is notified of the status and also notified that a reboot is necessary for the new configuration to become active:



By design, the IP Address configuration currently on the device is kept intact and not overwritten by the new configuration file.

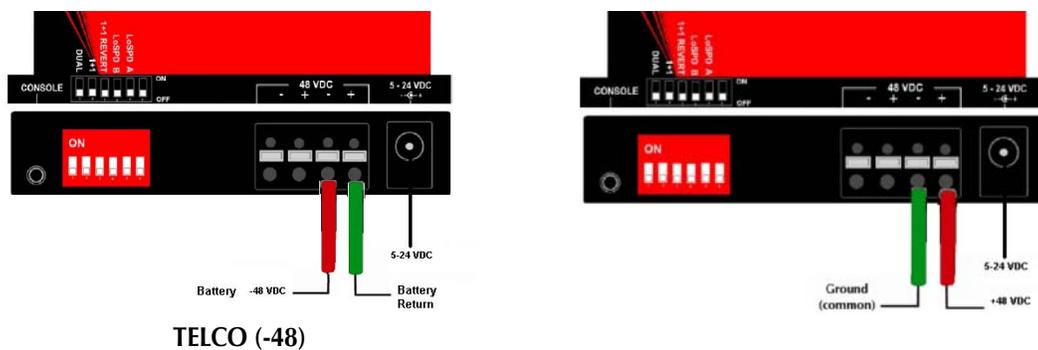
SFP Ports

The IE-MultiWay SFP ports support gigabit fiber SFPs and 100Mbps fiber SFPs, with or without Digital Diagnostics Monitoring Information (DDMI) as well as copper SFPs available in 10/100/1000Mbps and 1000Mbps. DDMI statistics provide real-time access to transceiver operating parameters such as voltage, temperature, laser bias current, and both transmitter and receive optical power. This information can be accessed through the management system. The SFPs must be MSA-compliant, and can be purchased from IMC Networks or other suppliers.

Hardware/Wiring Specifications

DC Terminal Block Wiring Instructions

The IE-MultiWay can also be powered with the DC terminal block. From a power source, connect to any one positive and any one negative terminal on the IE-MultiWay.



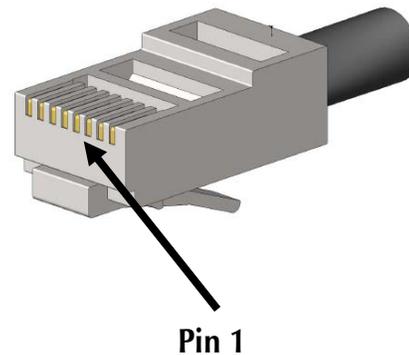
NOTE

When using stranded wire, the leads should be tinned. The DC terminal block is protected against polarity mis-wiring. AWG24 is recommended.

RJ-45 Data Port Pinout

The following table lists the pin configuration for the RJ-45 Data connector.

Pin	Signal Name 1000M	Signal Direction 10/100M
1	TXD1+	Out*
2	TXD1-	Out*
3	RXD2+	In*
4	D3+	
5	D3-	
6	RXD2-	In*
7	D4+	
8	D4-	



*NOTE

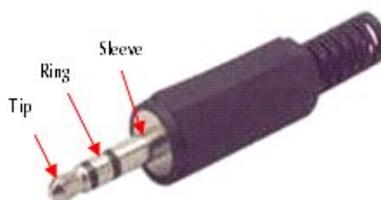
The MDI/MDIX function will automatically adjust the direction of these signals to match the connected unit when running 10/100Base-T. 1000Base-T will use all 4 pairs in full duplex mode.

RS-232 Serial Console Port

The IE-MultiWay includes an RS-232 Mini Jack for the Console port to allow the end user to launch a serial session and access a list of commands. The serial port on the computer/terminal should be set for: 38.4K baud, 8 data bits, 1 stop bit, no parity, no flow control. The **F2** key functions as a Delete key on VT-100 emulators.

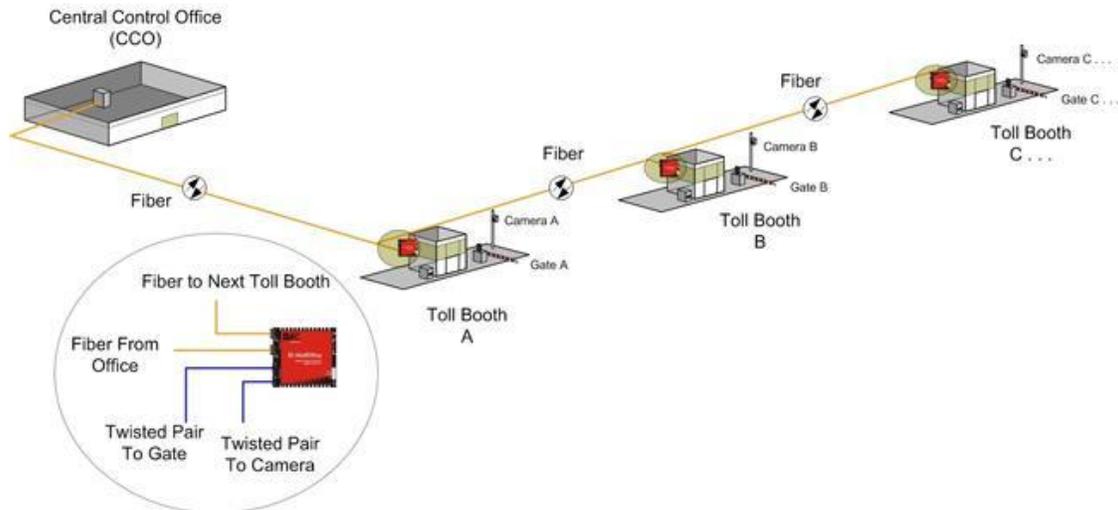
The following table lists the pin configuration for the RS-232 3-pin Mini Jack mating connector for the console serial port.

Pin	DB9-F Pin#	Signal Name	Direction
Tip	2	Transmit	Out of Unit
Ring	3	Receive	In to Unit
Sleeve	5	Return	Return



Product Applications

For a detailed description of the product applications, please refer to the IE-MultiWay data sheet at <http://www.imcnetworks.com/Assets/DocSupport/DS-IE-MultiWay-1102.pdf>.



Glossary

The following are terms and phrases used within this manual, or which are found in documents associated with this equipment.

Term/Acronym	Definition
1+1	The Term "1+1" refers to line protection where identical information is transmitted on two redundant lines. The Receiver chooses the "best" line to use based on the BER of the line.
802.1ag	IEEE standard for end-to-end OAM
802.3ah	IEEE standard addressing Ethernet in the first mile and also OAM for point-to-point Ethernet links.
CFM	Connectivity Fault Management
CLI	Command Line Interface: An interface screen, often DOS-based, used for system management and diagnostics requiring the user to type commands rather than use a <i>GUI</i> .
CPE	Customer Premises Equipment; normally the end point of a leased fiber.
DC	Direct Current
DDMI	Digital Diagnostic Monitor Interface: A defined serial interface and data format typically used to access SFP internal information
DHCP	Dynamic Host Configuration Protocol: Used to automate configuration of computers that use TCP/IP
GUI	Graphical User Interface: Software that provides a visual interface to enable an end-user to manage and monitor network devices.
IEEE	Institute of Electrical and Electronics Engineers; IEEE develops industry-wide standards for use in a variety of electronic devices
IP	Internet Protocol
LED	Light Emitting Diode: A small stack of lights to indicate link, duplex or other options.
MA	Maintenance Association
MD	Maintenance Domain

Term/Acronym	Definition
MDI/MDIX	Media-Dependent Interface/ Media-Dependent Interface Crossover. The ability of an Ethernet port to automatically detect and configure its cabling connections to accommodate crossover or non-crossover wiring, depending on its link partner and cabling.
MEP	Maintenance Association End Points
MIB	Management Information Base: A database of objects that can be monitored by a network management system. Both SNMP and RMON use standardized MIB formats that allow any SNMP and RMON tools to monitor any device defined by a MIB.
MSA	Multi-Source Agreement (SFP): The standard an SFP must meet to be compatible in network devices.
NOC	Network Operations and Control Center
OAM	Operations, Administration and Maintenance
OAM CFM	IEEE 802.1ag Connectivity Fault Management
PROM	Programmable Read-Only Memory
SFP	Small Form-Factor Pluggable: An industry standard optical pluggable module.
SNMP	Simple Network Management Protocol: A set of protocols for managing complex networks over a standards-based IP network.
TFTP	Trivial File Transfer Protocol
VLAN	Virtual Local Area Network

Troubleshooting

If a fiber connection cannot be established, perform the following to make sure that the fiber transceivers on the IE-MultiWay are not over/under driving the fiber receivers:

1. Make sure the fiber wavelength on both connected devices match (i.e. both are 1310 nm single-mode fiber).
2. Make sure the twisted-pair port speed on the IE-MultiWay matches that of the end devices connected to the IE-MultiWay. Configure the IE-MultiWay and its link partner to Auto Negotiation or, if using Force mode, be sure speed and duplex match.
3. IE-MultiWay allows the end user to assign a VLAN tag to all management traffic (SNMP and telnet). It is important to understand that IF using telnet or iView² to assign a VLAN tag to management traffic then as soon as this setting is saved the connectivity will be lost until the PC becomes a member of the VLAN which was assigned to management traffic.

If a VLAN tag has been assigned to management traffic and the end user cannot re-establish a connection to the device via iView² or telnet, directly connect a PC to the device via the serial cable and review/modify the changes made (reference section on serial port config).

Specifications

Ethernet Connections

- SFP 1000 Base-X
- SFP 100 Base –FX
- SFP 10/100/1000 Copper (SGMII)
- 10/100/1000 BaseT (Fixed Copper ports)
- Auto Negotiation
- Auto-Cross
- Flow Control
- Up to 10,240 MTU
- Full Line-Rate Forwarding

Power

DC terminal 48 VDC, Telco (42.5 to 56.5 VDC with 10mSec transients to 75 VDC)

DC jack 5 VDC - 24 VDC

Double-USB Power Spec 500mA

Cable Note that the laptop or PC USB ports must be 2.0 or greater to provide sufficient power to the unit.

AC wall adapter Input: 100 to 240 \pm 10% VAC
Output: 5 VDC, 2A max.

Operating Temperature

-40°F to +185°F (-40°C to +85°C) DC configuration
+14°F to +122°F (-10°C to +50°C) with AC wall adapter

Storage Temperature

-67°F to +257°F (-55°C to +125° C)

Humidity

5 to 95% (non-condensing); 0 to 10,000 ft. altitude

Dimensions

0.79"H x 3.82"W x 3.82"D (2cm H x 9.7cm W x 9.7cm D))

Current Draw

1.5A @ room temperature with data and copper SFPs
1.1A @ room temperature with fiber SFPs

Standards/Compliance

- IEEE 802.3x Flow Control
- IEEE 802.3i 10Base-T twisted pair
- IEEE 802.3u 100Base-TX twisted pair
- IEEE 802.3u 100Base-FX or SX fiber

NOTE
<i>SFPs are covered by a one-year warranty. The optional IE-5 VDC Power Block is covered by a three-year warranty.</i>

IMC Networks Technical Support

Tel: (949) 465-3000 or (800) 624-1070 (in the U.S. and Canada);
+32-16-550880 (Europe)

Fax: (949) 465-3020

E-Mail: techsupport@imcnetworks.com

Web: www.imcnetworks.com

Fiber Optic Cleaning Guidelines

Fiber Optic transmitters and receivers are extremely susceptible to contamination by particles of dirt or dust, which can obstruct the optic path and cause performance degradation. Good system performance requires clean optics and connector ferrules.

1. Use fiber patch cords (or connectors, if you terminate your own fiber) only from a reputable supplier; low-quality components can cause many hard-to-diagnose problems in an installation.
2. Dust caps are installed at IMC Networks to ensure factory-clean optical devices. These protective caps should not be removed until the moment of connecting the fiber cable to the device. Should it be necessary to disconnect the fiber device, reinstall the protective dust caps.
3. Store spare caps in a dust-free environment such as a sealed plastic bag or box so that when reinstalled they do not introduce any contamination to the optics.
4. If you suspect that the optics have been contaminated, alternate between blasting with clean, dry, compressed air and flushing with methanol to remove particles of dirt.

Electrostatic Discharge Precautions

Electrostatic discharge (ESD) can cause damage to any product, add-in modules or stand alone units, containing electronic components. Always observe the following precautions when installing or handling these kinds of products

1. Do not remove unit from its protective packaging until ready to install.
2. Wear an ESD wrist grounding strap before handling any module or component. If the wrist strap is not available, maintain grounded contact with the system unit throughout any procedure requiring ESD protection.
3. Hold the units by the edges; do not touch the electronic components or gold connectors.
4. After removal, always place the boards on a grounded, static-free surface, ESD pad or in a proper ESD bag. Do not slide the modules or stand alone units over any surface.



WARNING! Integrated circuits and fiber optic components are extremely susceptible to electrostatic discharge damage. Do not handle these components directly unless you are a qualified service technician and use tools and techniques that conform to accepted industry practices.

Safety Certifications

UL/CUL: Listed to Safety of Information Technology Equipment, including Electrical Business Equipment.

CE: The products described herein comply with the Council Directive on Electromagnetic Compatibility (2004/108/EC) and the Council Directive on Electrical Equipment Designed for use within Certain Voltage Limits (2006/95/EC). Certified to Safety of Information Technology Equipment, Including Electrical Business Equipment. For further details, contact IMC Networks.



**Class 1 Laser product, Luokan 1 Laserlaite,
Laser Klasse 1, Appareil A' Laser de Classe 1**

European Directive 2002/96/EC (WEEE) requires that any equipment that bears this symbol on product or packaging must not be disposed of with unsorted municipal waste. This symbol indicates that the equipment should be disposed of separately from regular household waste. It is the consumer's responsibility to dispose of this and all equipment so marked through designated collection facilities appointed by government or local authorities. Following these steps through proper disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about proper disposal, please contact local authorities, waste disposal services, or the point of purchase for this equipment.





19772 Pauling • Foothill Ranch, CA 92610-2611 USA
TEL: (949) 465-3000 • FAX: (949) 465-3020
www.imcnetworks.com

ISO 9001:2008
REGISTERED



© 2012 IMC Networks. All rights reserved.

The information in this document is subject to change without notice. IMC Networks assumes no responsibility for any errors that may appear in this document. IE-MultiWay is a trademark of IMC Networks. Other brands or product names may be trademarks and are the property of their respective companies.

Document Number 58-80121-00 A6 Preliminary

February 2012