BLONDER TONGUE LABORATORIES, INC.

One Jake Brown Road
Old Bridge, NJ 08857-1000 USA
(800) 523-6049 • (732) 679-4000 • FAX: (732) 679-4353
www.blondertongue.com

INSTRUCTION MANUAL

IPME Series

Internet Protocol MPEG Encoder

Model	Stock No.	Description
IPME-2	2420	Internet Protocol MPEG-2 Encoder Module
IPME-CH	2419	Internet Protocol MPEG Encoder Chassis
MPEGLA	2412	MPEG License Authority Royalty Fee
Accessories:		
IPME-SM	2415	Internet Protocol MPEG Encoder Stream Manager
IPCV	2411	Internet Protocol Client Viewer Software

MADE IN USA

651216900A

The lightning flash with arrowhead symbol within an equilateral triangle is intended to alert you to the presence of uninsulated "dangerous voltage" within the product's enclosure that may be of sufficient magnitude to constitute a risk of electrical shock to persons.

CAUTION
RISK OF ELECTRIC SHOCK
DO NOT OPEN

The exclamation point within an equilateral triangle is intended to alert you to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the product.

TO REDUCE THE RISK OF ELECTRICAL SHOCK, DO NOT REMOVE COVER FROM THIS UNIT. NO USER-SERVICEABLE PARTS INSIDE. REFER SERVICING TO QUALIFIED SERVICE PERSONNEL.

WARNING: TO PREVENT FIRE OR SHOCK HAZARD, DO NOT EXPOSE THIS UNIT TO RAIN OR MOISTURE

NOTE TO CATV SYSTEM INSTALLER

This reminder is provided to call the CATV System Installer's attention to Article 820-40 of the NEC that provides guidelines for proper grounding and, in particular, specifies that the cable ground shall be connected to the grounding system of the building, as close to the point of cable entry as practical.

For all pluggable equipment the socket-outlet shall be installed near the equipment and shall be easily accessible.

Never power up one RPR from the outlet of another RPR, Daisy chaining or using a multiple outlet power strip powered from the RPR could result in fire due to overloading of the AC supply circuit.

Unpacking and Installation

NOTE TO CATV SYSTEM INSTALLER

This reminder is provided to call the CATV System Installer's attention to Article 820-40 of the NEC that provides guidelines for proper grounding and, in particular, specifies that the cable ground shall be connected to the grounding system of the building, as close to the point of cable entry as practical.

Unpacking and Handling

Each unit is shipped with all equipment assembled, wired, factory tested, and then packaged in an appropriate shipping container.

Ensure that all accessories are removed from the container and packing material before they are discarded.

Mechanical Inspection

Inspect the front and rear of the equipment for shipping damage. Make sure the equipment is clean, and no wires, cables, or connectors are broken, damaged or loose.

Precautions

Adherence to the initial installation precautions outlined in the Table below will help prevent problems arising during the installation and future maintenance of the unit.

Damage in Shipment

Should any damage be discovered after unpacking the unit, immediately file a claim with the carrier. A full report of the damage shall be made and a copy forwarded to Blonder Tongue Laboratories Inc. The company will then advise what disposition is to be made of the equipment.

Unit Adjustments

After installing the unit, make the following adjustments:

Audio Modulation

With audio source connected, adjust Audio Modulation control for 25 kHz deviation. In lieu of an audio modulation meter, use a TV set and adjust for equal volume as compared to a known off-air broadcast. Monitor for a few minutes to assure that maximum volume does not over modulate, which can cause picture distortion.

Video Modulation
With a nominal 1 volt P-P video source connected, adjust the Video Modulation control for the correct percentage of modulation (87.5%). If test equipment is not available for such measurements, then adjust for proper picture contrast when viewed on a TV set (compare with known off-air broadcast picture quality).

Returning Product for Repair or Credit

A Return Material Authorization (RMA) Number is required on all products returned to Blonder Tongue, regardless if the product is being returned for repair or credit. Before returning product, please contact the Blonder Tongue Service Department at 1-800-523-6049, Ext. 4256 or visit our website: www.blondertongue.com for further information.

Table 1 - Installation Precautions Table

PRECAUTIONS	REQUIREMENTS
Avoid Heat Buildup	Allow (1) EIA rack space ($1^{3/4}$") between powered headend products in the equipment racks.
Ensure easy access to rack wiring.	Allow a minimum of 18 inches behind the equipment rack(s)
Facilitate servicing and maintenance.	Allow a minimum of 36" of clearance in front of the equipment rack(s).
Avoid direct heating or air conditioning.	If unavoidable, use deflector plates.
AC power source outlets.	Locate equipment near sufficient outlets to provide power for test equipment and power tools.
Rack Support.	Make certain rack supports are sufficiently rigid to support racks.
Building leakage.	Beware of dripping water onto equipment from leaky roofs, waveguide roof entries, and cold water pipe condensations.

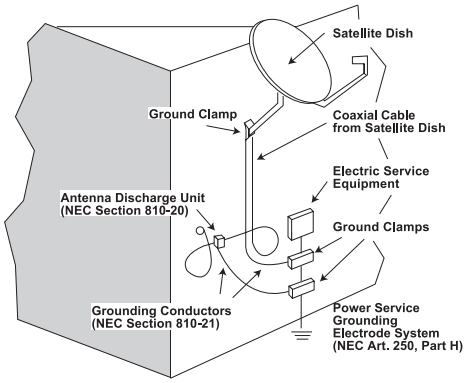
Safety Instructions

You should always follow these instructions to help ensure against injury to yourself and damage to your equipment.

- Read all safety and operating instructions before you operate the unit.
- Retain all safety and operating instructions for future reference.
- Heed all warnings on the unit and in the safety and operating instructions.
- Follow all installation, operating, and use instructions.
- Unplug the unit from the AC power outlet before cleaning. Use only a damp cloth for cleaning the exterior of the unit.
- Do not use accessories or attachments not recommended by Blonder Tongue, as they may cause hazards, and will void the warranty.
- Do not operate the unit in high-humidity areas, or expose it to water or moisture.
- Do not place the unit on an unstable cart, stand, tripod, bracket, or table. The unit may fall, causing serious personal injury and damage to the unit. Install the unit only in a mounting rack designed for 19" rack-mounted equipment.
- Do not block or cover slots and openings in the unit. These are provided for ventilation and protection from overheating. Never place the unit near or over a radiator or heat register. Do not place the unit in an enclosure such as a cabinet without proper ventilation. Do not mount equipment in the rack space directly above or below the unit.

Safety Instructions - continued

- Operate the unit using only the type of power source indicated on the marking label. Unplug the unit power cord by gripping the plug, not the cord.
- The unit is equipped with a three-wire ground-type plug. This plug will fit only into a ground-type power outlet. If you are unable to insert the plug into the outlet, contact an electrician to replace the outlet. Do not defeat the safety purpose of the ground-type plug.
- Route power supply cords so that they are not likely to be walked on or pinched by items placed upon or against them. Pay particular attention to cords at plugs, convenience receptacles, and the point where they exit from the unit.
- Be sure that the outdoor components of the antenna system are grounded in accordance with local, federal, and National Electrical Code (NEC) requirements. Pay special attention to NEC Sections 810 and 820. See the example shown in the following diagram:



- We strongly recommend using an outlet that contains surge suppression or ground fault protection. For added protection during a lightning storm, or when the unit is left unattended and unused for long periods of time, unplug it from the wall outlet and disconnect the lines between the unit and other equipment. This will prevent damage caused by lightning or power line surges.
- Do not locate the antenna near overhead power lines or other electric light or power circuits, or where it can fall into such power lines or circuits. When installing an antenna, take extreme care to avoid touching such power lines or circuits, as contact with them can be fatal.
- Do not overload wall outlets or extension cords, as this can result in a risk of fire or electrical shock.
- Never insert objects of any kind into the unit through openings, as the objects may touch dangerous voltage points or short out parts. This could cause fire or electrical shock.
- Do not attempt to service the unit yourself, as opening or removing covers may expose you to dangerous voltage and will void the warranty. Refer all servicing to authorized service personnel.
- Unplug the unit from the wall outlet and refer servicing to authorized service personnel whenever the following occurs:
  - ❒ The power supply cord or plug is damaged;
  - ❒ Liquid has been spilled, or objects have fallen into the unit;
  - ❒ The unit has been exposed to rain or water;
  - ❒ The unit has been dropped or the chassis has been damaged;
  - ❒ The unit exhibits a distinct change in performance.
- When replacement parts are required, ensure that the service technician uses replacement parts specified by Blonder Tongue. Unauthorized substitutions may damage the unit or cause electrical shock or fire, and will void the warranty.
- Upon completion of any service or repair to the unit, ask the service technician to perform safety checks to ensure that the unit is in proper operating condition.

BLONDER TONGUE SOFTWARE LICENSE AGREEMENT
IMPORTANT — READ BEFORE COPYING, INSTALLING OR USING

Do not use or load this software and any associated materials (collectively, the "Software") until you have carefully read the following terms and conditions. By loading or using the Software, you agree to the terms of this Agreement. If you do not wish to so agree, do not install or use the Software.

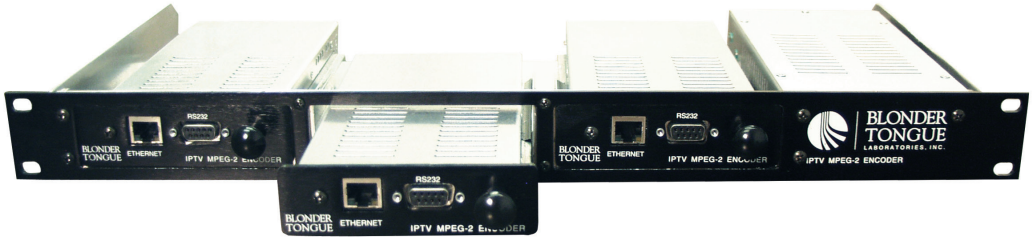
LICENSE: This Software is licensed for use only in conjunction with Blonder Tongue (BT) products. Use of the Software in conjunction with non-BT products is not licensed hereunder. Subject to the terms of this Agreement, BT grants to You a nonexclusive, nontransferable, license under BT's copyrights to use, modify and copy Software internally for Your own development and maintenance purposes.

OWNERSHIP OF SOFTWARE AND COPYRIGHTS: Title to all copies of the Software remains with BT or its suppliers. The Software is copyrighted and protected by the laws of the United States and other countries, and international treaty provisions. You may not remove any copyright notices from the Software. BT may make changes to the Software, or to items referenced therein, at any time and without notice, but is not obligated to support or update the Software. Except as otherwise expressly provided, BT grants no express or implied right under BT patents, copyrights, trademarks, or other intellectual property rights. You may transfer the Software only if the recipient agrees to be fully bound by these terms and if you retain no copies of the Software.

EXCLUSION OF OTHER WARRANTIES: EXCEPT AS PROVIDED ABOVE, THE SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTY OF ANY KIND, INCLUDING WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR FITNESS FOR A PARTICULAR PURPOSE. Blonder Tongue does not warrant or assume responsibility for the accuracy or completeness of any information, text, graphics, links or other items contained within the Software.

LIMITATION OF LIABILITY: IN NO EVENT SHALL BT OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, LOST PROFITS, BUSINESS INTERRUPTION OR LOST INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF BT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS PROHIBIT EXCLUSION OR LIMITATION OF LIABILITY FOR IMPLIED WARRANTIES OR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER LEGAL RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION.

TERMINATION OF THIS AGREEMENT: BT may terminate this Agreement at any time if you violate its terms. Upon termination, you will immediately destroy the Software or return all copies of the Software to BT.



Description

The Blonder Tongue MPEG-2 IPTV Encoder permits the ability to stream a single audio/video program signal in MPEG-2 format over a LAN (Local Area Network) infrastructure. The compact and modular package facilitates easy integration with existing or new systems. The unit transmits video in real time DVD quality at 30 fps (frames per second) and full screen resolution up to 720 x 480. Multicast or Unicast modes are supported. The module is designed to work in conjunction with standards compliant viewers for the PC such as the Blonder Tongue IPClientViewer software or a TV monitor with an IP set top box. Easy configuration and system administration can also be accomplished using the optional IPME-Stream Manager.

Features & Benefits

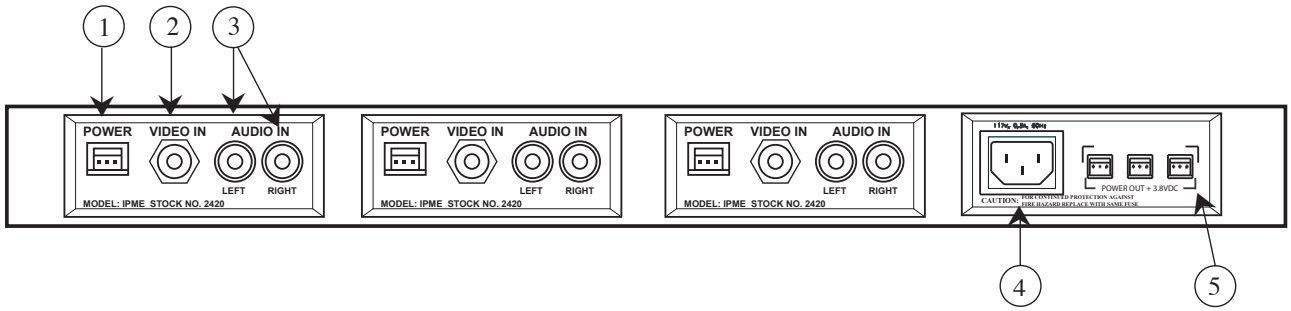
- Modular design allows one to three independent IPTV MPEG-2 Encoder's per rack assembly
- Interoperable MPEG-2 standards compliant video transmission over IP
- "Transport stream over UDP" or "RTP over UDP" IP protocols
- Simultaneously view different video streams in real-time over LAN or WAN infrastructure
- 10baseT Ethernet or 100baseTX Fast Ethernet compatible
- Supports Unicast or Multicast video stream connection types
- Resolution up to 720h x 480v @ 30 fps for DVD quality video
- Configurable video streaming bit rate from 1.5 Mbits/s up to 7.5 Mbits/s
- Design modularity provides the ability to field replace any module with ease
- Simple set-up using Console Menus via RS-232 interface
- Web Interface on IPME Stream Manager for setup and display of IPME settings
- Remote configuration management using standard web browser (HTTP) or Telnet capabilities
- Secure administrator authorization control
- Supports NTSC and PAL video input formats

The Unit

Front Panel

1. **RJ-45 Ethernet Connector** – Connects to LAN or WAN Network
   1A. **Green LED (Left Side)** - Indicates speed status of traffic, on = 100 BaseT, off = 10 BaseT traffic
   1B. **Orange LED (Right Side)** - Indicates link and receive status, on = link up, off = line down, blinking indicates receiver activity
2. **9-Pin RS-232 Serial Connector** – Used for Local and/or Remote Configuration and Management (See Appendix for detailed information on the RS232 connector)

Rear Panel



1. **Power** – 3-pin connector used to supply power to the IPME-2 module. Connect the power cable supplied with the IPME-CH to the IPME-2 module
2. **Video In** – Independent 'F' video input connector
3. **Audio In** – Right Stereo & Left Stereo or Mono RCA input connectors
4. **Power Cord Socket** - The unit power cord plug socket
5. **Power Out Connectors** - 3, 3.8 VDC 3 - Pin power connectors to power IMPE-2 Module

Specifications

IPTV Encoder

Compression: MPEG-2 Standards Compliant, RFC-1889 & RFC-2250

Ethernet: 10BaseT Ethernet or 100BaseTX Fast Ethernet Compatible (Auto-sensing)

Bandwidth Control:

Minimum: 30 fps @ 1.5 Mbits/s, 325 x 240 Resolution

Recommended: 30 fps @ 3.8 Mbits/s, 720 x 480 Resolution

Maximum: 30 fps @ 7.5 Mbits/s, 720 x 480 Resolution

Streaming Modes:

Multicast or Unicast Modes, "Transport Stream over UDP" or "RTP over UDP"

Multicast Sessions: Unlimited Number of Client Viewing Sessions

Packet Rate with Minimum Latency

Input & Output

Video Input Formats: NTSC & PAL

Front Panel Connectors

RJ-45 Ethernet, 10/100

RS-232 Serial Connector

Rear Panel Connectors

Video Input 'F' Female Connector

Audio Input Left/Right RCA Connectors

Power Connector, 3 Pin +3.8 VDC

System Requirements

Standard MPEG-2 Encoding with TCP/IP Protocols, Images can be viewed on a PC with BT's IPClientViewer (MPEG Decoder) Software or an Optional IP Set-top Decoder Box

MPEGLA License Fee is Required

Minimum PC Requirements

Pentium® III 600 MHz or Higher or Equivalent Processor

256 MB RAM

300 MB Hard Disk Space

Windows® 2000 or XP, with Internet Explorer 5.5 and Direct-X 8.1 or Higher

RS-232 Serial Port

10/100 Network Interface Card

General

Power: + 3.8 VDC, 1 AMP

Operating Temperature Range: 0° to +50° C

Storage Temperature Range: -10° to +70° C

Humidity: 0 to 90% RH

Mechanical

Module Dimensions: 4 x 7 Inches
Chassis Dimensions: 19 x 8.25 x 1.75 Inches
Module Weight: 0.8 lbs.
Chassis Weight: 2.725 lbs.
Fully Loaded Weight: 5.125 lbs.

NOTE: The IPME-2 is not intended to function with a PoE (Power over Ethernet) enabled switch or network equipment.

Installation

To install the IPME, perform the following steps:

1. Connect the video source to the Video In "F" connector.
2. Connect a standard Ethernet cable to the Ethernet RJ-45 connector.
   a. The other end of the Ethernet cable should be connected to a switch on your IP network.
3. Connect an audio source to the Stereo Audio "RCA" connectors. The IPME accepts a line level stereo signal.
4. Connect the supplied Power cable of Power Supply module to the Power connector of the IPME.
5. Connect the RS-232 port of the IPME using a 9-pin D-SUB (null modem) connector to the RS-232 serial port of a computer (see Appendix for a detailed pin-out diagram).

   The minimum connections required to the IPME are to have the power connected using the supplied cable from the IPME-CH, a video source connected to Video In "F" Connector input and a RJ-45 connection to the Ethernet connector to the LAN/WAN network. Connection of an audio source to the L/R RCA connectors is optional. The RS-232 connection is also optional once the unit is configured or if using the Blonder Tongue IPME Stream Manager.

Note: First time install/communication requires the use of a serial null modem cable.

Operation

The minimum connections required to the IPME are to have the power connected using the supplied cable from the IPME-CH, a video source connected to Video In "F" Connector input and a RJ-45 connection to the Ethernet connector to the LAN/WAN network. Connection of an audio source to the L/R RCA connectors is optional. The RS-232 connection is also optional once the unit is configured or if using the Blonder Tongue IPME Stream Manager.

Accessing the IPME unit

The IPME unit can be accessed through the RS-232 serial connection using HyperTerminal or through the Ethernet connection using Telnet or the built-in web interface, when enabled.

HyperTerminal is generally an accessory program that comes standard with the Windows® operating system. If HyperTerminal is not installed on your PC it can be installed by opening the Windows Control Panel > clicking Add or Remove Programs > Click Add/Remove Windows Components and install it.

A Telnet session can be accessed from any command (DOS) prompt, if Telnet is enabled.

Access to the IPME unit is Username and Password protected. An Administrator Username and Password is required to make command and control modifications to the Internet Protocol MPEG-2 Encoder. Stop and Start commands through the RS-232 connection also require the proper username and password but may be performed with the unit's web based interface w/o a username and password, (the web interface is described in detail later in this document).

Administrator Defaults

Username — "admin"
Password — "admin"

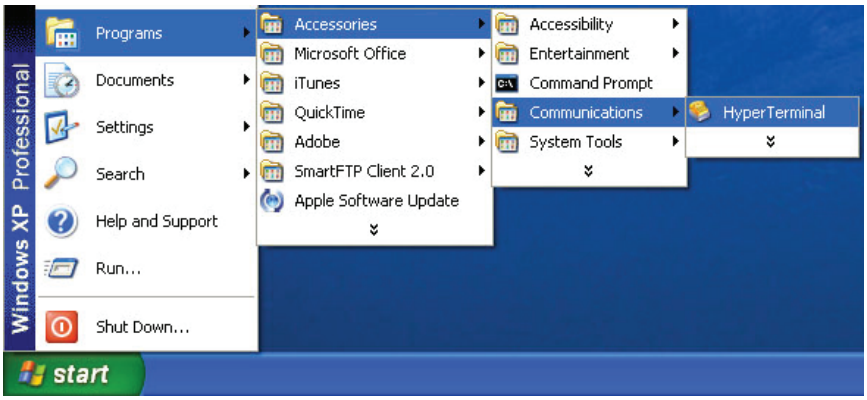
The Administrator Username and Password can be up to 31 characters in length and are case sensitive.
The administrator username and password can be changed using HyperTerminal or Telnet.

NOTE: It is recommended that you change the default values that are shipped with your IPME unit before installing it on your network.

Connecting to the IPME-2 with HyperTerminal

NOTE: If HyperTerminal is not installed on your PC it can be installed by opening the Windows Control Panel > Clicking Add or Remove Programs > Click Add/Remove Windows Components and install it.

1. Connect a null modem serial cable to the RS-232 port of the IPME and to a serial COMM port on your PC (typically the COM1 port). See appendix for null modem serial cable details.
2. Open HyperTerminal.
   a. This is generally found under Accessories > Communications in the Programs Menu of Windows as shown below.

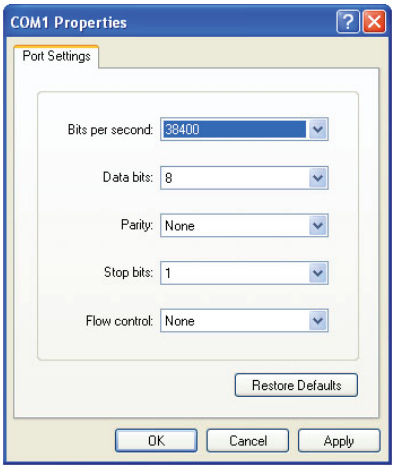


3. HyperTerminal will prompt you to enter a description for your connection the first time you connect. Enter a name for the connection.

4. You can also select an Icon and create a shortcut on your desktop which can be saved to allow you launch HyperTerminal using the same settings easily at a future time.

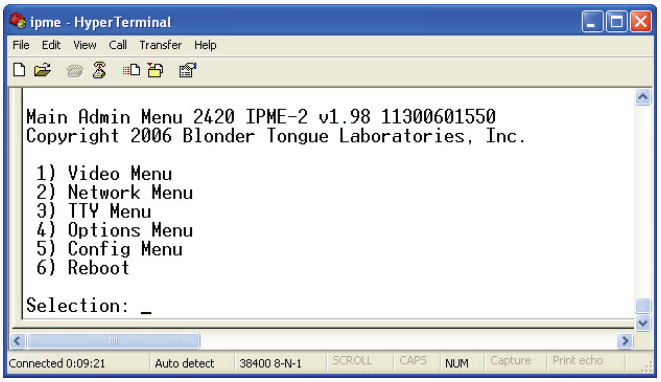
5. Choose the appropriate Connect To COM port on your PC (Typically COM1 or COM2)

6. Configure the Port Settings as shown below in order to communicate with the IPME



7. Click OK to establish HyperTerminal Communication.
   a. Make sure the Power and Serial null modem cable are connected to the IPME
   b. If the correct entries are made the HyperTerminal window screen should go blank
   c. Click the Enter or Return Key

8. The Main Admin Menu Prompt will display in the HyperTerminal program window



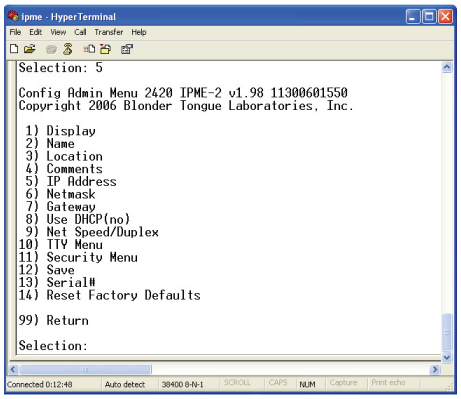
IPME-2 Console Menu Functions

It is important to note that most changes made in the Console Menus are immediately written to memory but some changes will only take effect after they are saved and the unit is rebooted. Selecting the Save option will cause the changes to be saved to Flash memory and only after a reboot will those saved values will be used by the unit. It is recommended to always use the 'Save' command in Console Menu screens it is available and then reboot the unit to put the change into effect. It is also recommended as a good preface to stop the stream prior to saving images. After saving make sure the "verifying done" message is displayed or no error messages are shown.

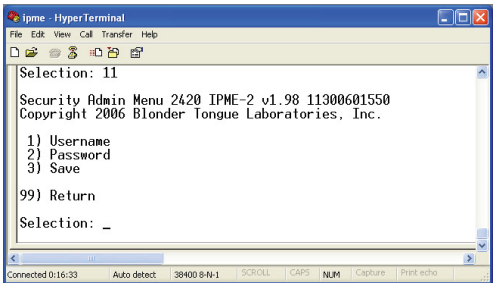
Setting the Administrator Username & Password

It is recommended that you change the default username and password values that are shipped with your IPME unit before installing it on your network.

- Select the Config Menu from the Main Admin Menu — Selection 5 and press Enter



- Select the Security Menu from the Config Menu — Selection 11 and press Enter



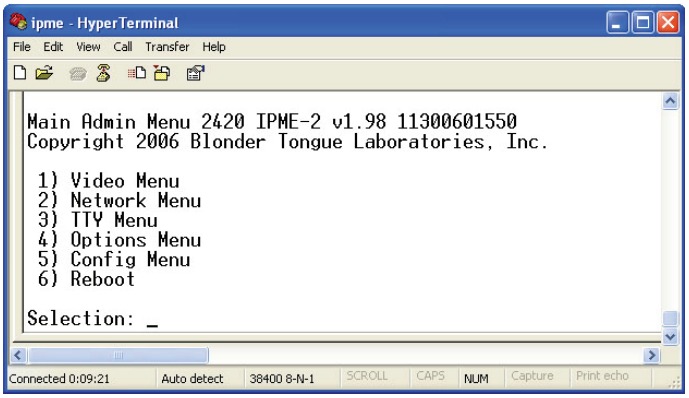
- Select 1 to change the Username (U/N)
  - The current U/N will be displayed
  - Enter a new U/N and press Enter or just press Enter to keep the same U/N

- Select 2 to change the Password (P/W)
  - The prompt will be displayed blank and your entry will be visible in plain text
  - Enter a new P/W and press Enter
  - Re-Enter the password to confirm your entry

- You must save the new settings in order for them to take effect
  - Select 3 and press Enter
  - It is recommended to reboot the IPME unit – Select 6 from the Main Admin Menu

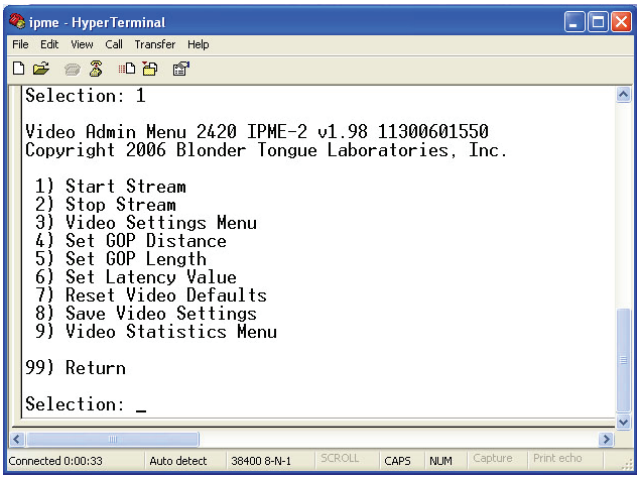
NOTE: The Username and Password can be up to 31 characters in length and are case sensitive.

Main Admin Menu



1. **Video Menu —** Displays the Video Admin Menu
2. **Network Menu —** Displays the Network Admin Menu
3. **TTY Menu —** Displays the TTY Menu
4. **Options Menu —** Displays the Options Admin Menu
5. **Config Menu —** Displays the Config Admin Menu
6. **Reboot —** Causes the IPME to Reboot allowing all changes saved to flash memory to take effect

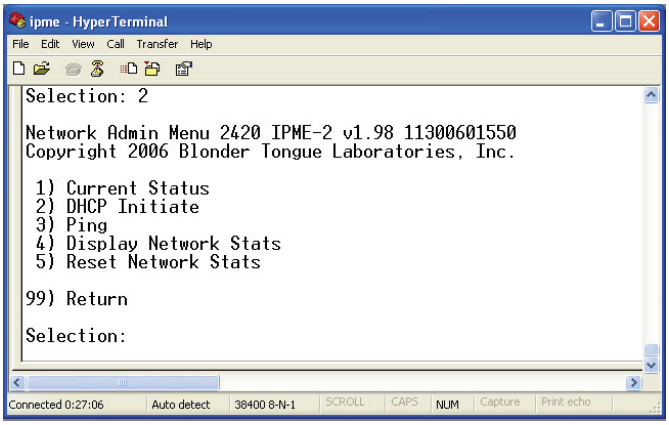
Video Admin Menu — *Selection 1 of Main Admin Menu*



1. **Start Stream —** starts the IPME stream with stored values
   i. If you attempt to start an IPME stream that does not have a valid video source and system integrity testing is enabled, the console window will display the streaming text saying “Video Source Not Connected”
   ii. If that happens, Type 2 and press Enter to Stop the Stream and restore use of the console menus. Using the Scroll Lock key on most keyboards also stops the streaming text
2. **Stop Stream —** Stops the IPME Stream
3. **Video Settings Menu —** Displays the Video Settings Menu
4. **Set GOP Distance —** Sets the Video GOP (Group of Pictures) distance. Valid values ranger from 0 to 3
   i. More detailed information on GOP can be found later in this manual including recommended settings

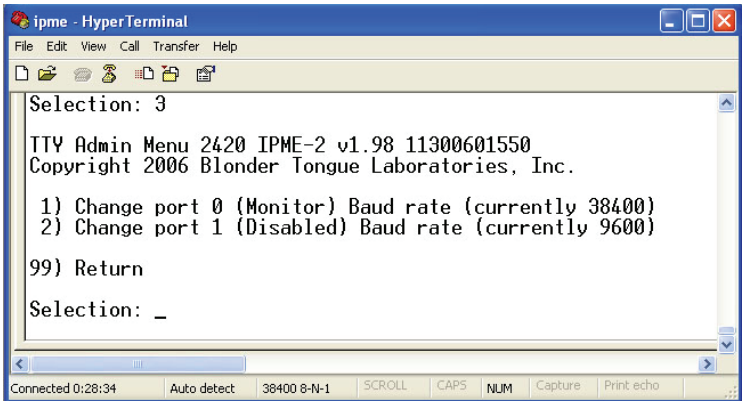
5. **Set GOP Length —** Sets the Video GOP length. Valid values ranger from 1 to 19
   i. More detailed information on GOP can be found later in this manual including recommended settings
6. **Set Latency Value —** Sets the values for how long buffers can be held in memory before transmission. This is an advanced setting. Improperly set values can result in unusable encoding
   i. More detailed information on Latency Value can be found later in this manual
7. **Reset Video Defaults —** This selection resets all the video settings to the factory default values
8. **Save Video Settings —** Saves the current Video settings to flash memory
9. **Video Statistics Menu —** Displays the Video Statistics Menu
99. **Return —** This command is used to navigate back to the previous console menu

Network Admin Menu — *Selection 2 of Main Admin Menu*



1. **Current Status —** Displays IPME's Network parameters including: Ethernet Port; Hardware Address; IP Address; Netmask; Gateway; Broadcast IP, Network Address; Link Status; Speed and Duplex
2. **DHCP Initiate —** Displays the Port, Protocol and Task numbers if DHCP is enabled
3. **Ping —** Provides a "Ping" to a given IP address with a specified size and number of packets and VLAN ID
   a. Uses the default values for Count, Length & VLAN ID if Enter is pressed for each value
   b. A Ping is a computer network tool used to test whether a particular host is reachable across an IP network. It works by sending ICMP "echo request" packets ("Pings") to the target host and listening for ICMP "echo response" replies
4. **Display Network Stats —** Displays the Ethernet Statistics including In / Out Octets and Packet Breakdown as well as Ethernet Errors
5. **Reset Network Stats —** Resets the Ethernet Statistics
99. **Return —** This command is used to navigate back to the previous console menu

TTY Admin Menu — *Selection 3 of Main Admin Menu*

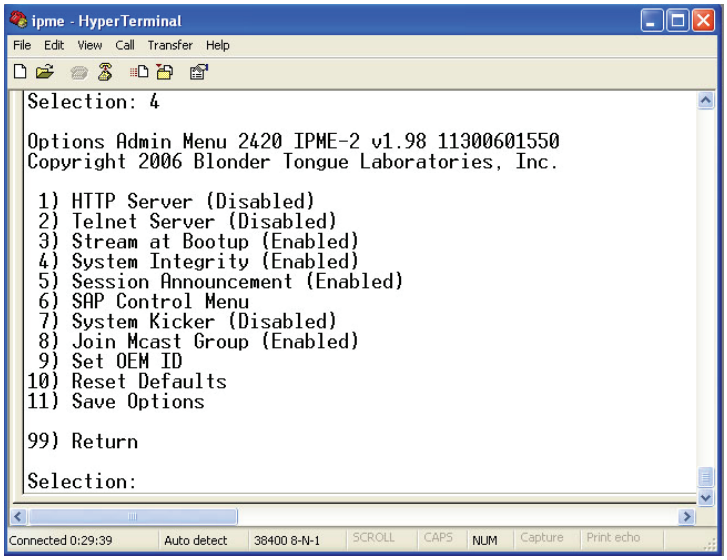


1. **Change port 0 (Monitor) Baud rate (currently 38400) —** sets the baud rate. Valid values must be multiples of 1200
2. **Change port 1 (CamControl) Baud rate (currently 9600) —** sets the baud rate. Valid values must be multiples of 1200

99. **Return —** This command is used to navigate back to the previous console menu

Options Admin Menu — *Selection 4 of Main Admin Menu*

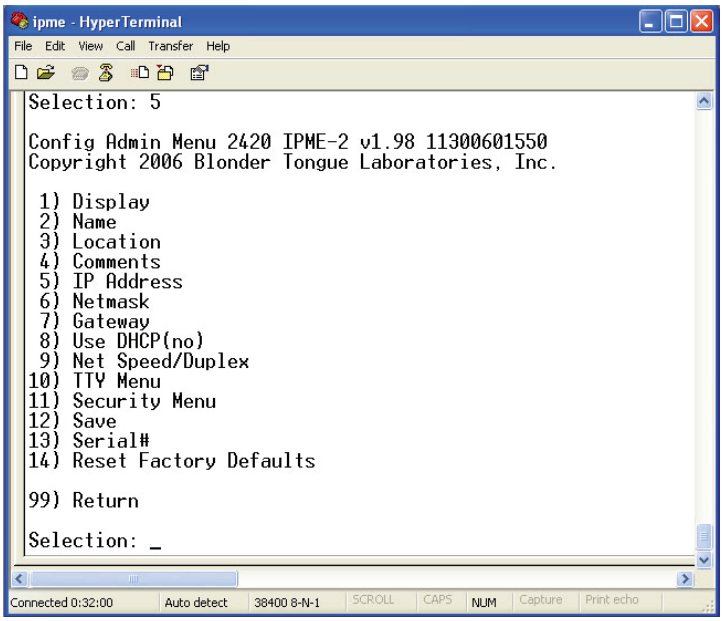
1. **HTTP Server —** Enables or Disables the HTTP Server The (Enabled) / (Disabled) functions acts a toggle switch
2. **Telnet Server —** Enables or Disables the Telnet Server
3. **Stream at Bootup** — Enables or Disables the Stream at Bootup mode
4. **System Integrity —** Enables or Disables the System Integrity testing mode
5. **Session Announcement —** Enables or Disables the Session Announcement mode (Not Used)
6. **SAP Control Menu —** Displays the SAP Control Admin Menu, (detailed separately)
7. **System Kicker —** Enables or Disables the Session Announcement mode (Not Used)
8. **Join Mcast Group —** Enables or Disables the Join Mcast Group mode
    a. If enabled, the IPME sends a join request to the router/switch to request membership into the IP multicast group



9. **Set OEM ID —** Used to permit the setting of a OEM Product ID/Version and company copyright information (displayed on each console menu)
10. **Reset Defaults —** Restores the factory defaults for the Options Admin Menu settings
11. **Save Options** — Saves all Options Admin Menu settings to flash

99. **Return —** This command is used to navigate back to the previous console menu

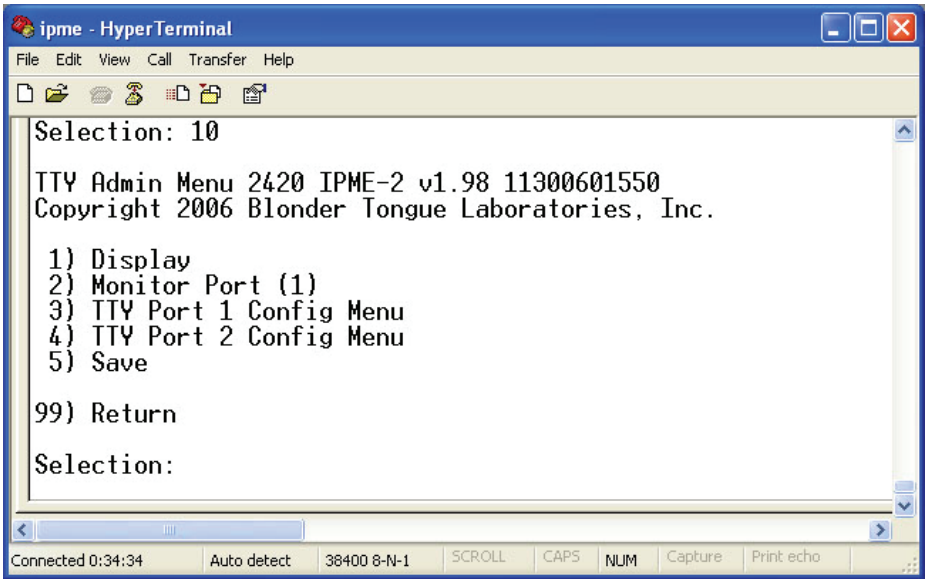
Config Admin Menu — *Selection 5 of Main Admin Menu*



1. **Display —** Displays the Port, Hardware Address, IP Address, Netmask and Gateway IP Address
2. **Name —** Allows an optional string to describe the IPME, which will be displayed in the IPME web interface page
3. **Location —** Allows an optional string to describe the IPME, which will be displayed in the IPME web interface page
4. **Comments —** Miscellaneous note or comments regarding the IMPE-2
5. **IP Address —** Sets the IP Address
6. **Netmask —** Sets the Netmask
7. **Gateway —** Sets the Gateway IP Address
8. **Use DHCP —** Displays whether DHCP is being used (yes or no) and provides the ability to modify this variable
9. **Net Speed/Duplex —** Sets the Network Speed. The default setting is AutoNegoiate
    a. It is not recommended to manually set the Network Speed
10. **TTY Menu —** Displays the TTY Menu, (detailed separately)
11. **Security Menu —** Displays the Security Menu, (detailed separately)
12. **Save —** Saves the current configuration to flash memory
13. **Serial # —** *Displays the IPME Serial Number*
14. ***Reset Factory Defaults*** *— Resets factory defaults*

99. **Return —** *This command is used to navigate back to the previous console menu*

TTY Admin Menu — *Selection 10 of Config Admin Menu*



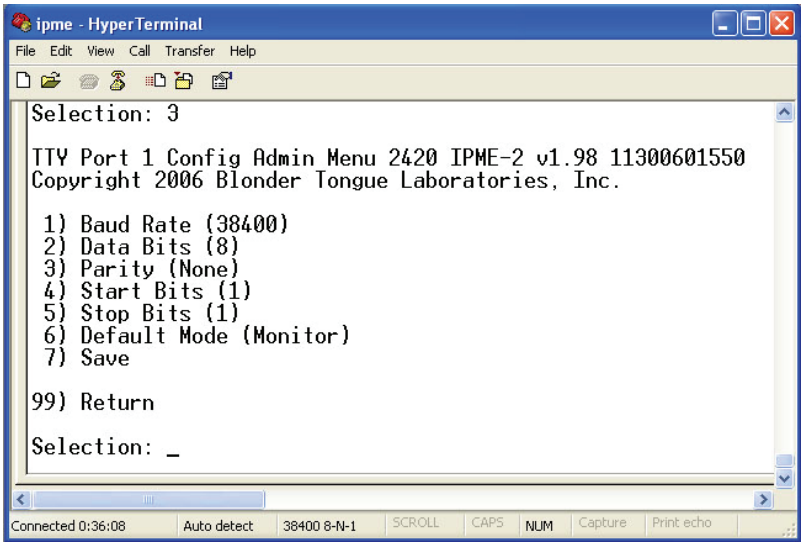
1. **Display** — Displays the Port, Baud Rate, Parity, Bits, Start, Stop and Mode of both ports
2. **Monitor Port** — Sets the Monitor Port
3. **TTY Port 1 Config Menu** — Displays the TTY Port 1 Config Menu, (detailed separately)
4. **TTY Port 2 Config Menu** — Displays the TTY Port 2 Config Menu, (detailed separately)
5. **Save** — Saves the current configuration to flash memory

99. **Return** — This command is used to navigate back to the previous console menu

TTY Port 1 Config Admin Menu — *Selection 3 of TTY Admin Menu*

1. **Baud Rate** — Sets the Baud Rate
2. **Data Bits** — Sets the Data Bits
3. **Parity** — Sets the Parity
4. **Start Bits** — Sets the Start Bit
5. **Stop Bits** — Sets the Stop Bit
6. **Default Mode** — Sets the Port Mode
7. **Save** — Saves the current configuration to flash memory

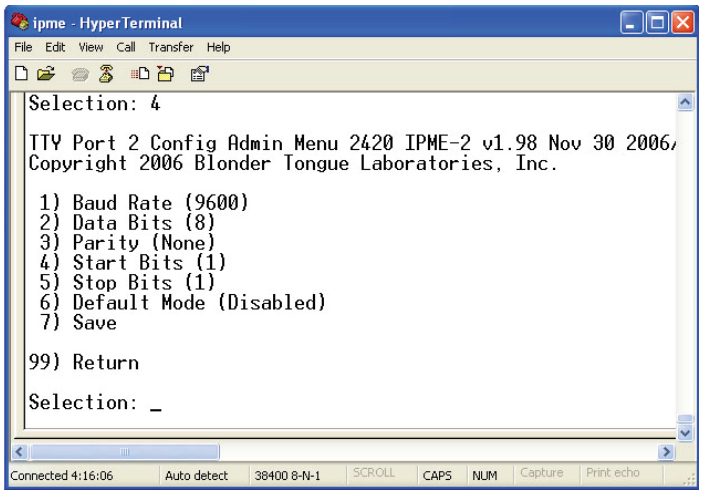
99. **Return** — This command is used to navigate back to the previous console menu



TTY Port 2 Config Admin Menu — *Selection 4 of TTY Admin Menu*

1. **Baud Rate** — Sets the Baud Rate
2. **Data Bits** — Sets the Data Bits
3. **Parity** — Sets the Parity
4. **Start Bits** — Sets the Start Bit
5. **Stop Bits** — Sets the Stop Bit
6. **Default Mode** — Sets the Port Mode
7. **Save** — Saves the current configuration to flash memory

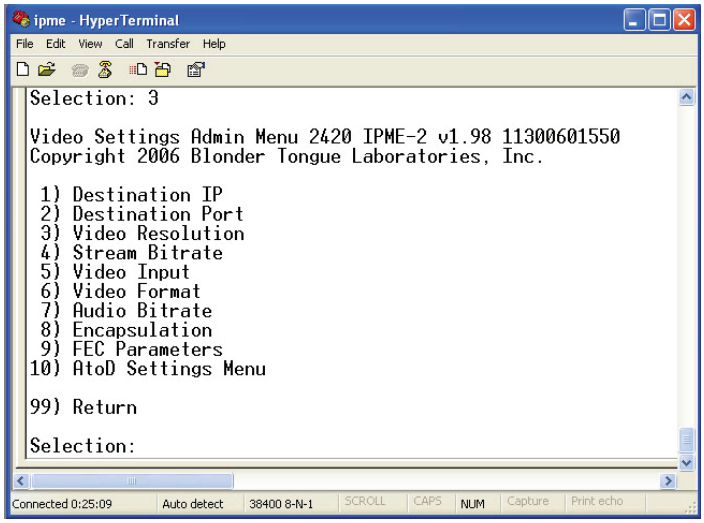
99. **Return** — This command is used to navigate back to the previous console menu



Video Settings Admin Menu — *Selection 3 of Video Admin Menu*

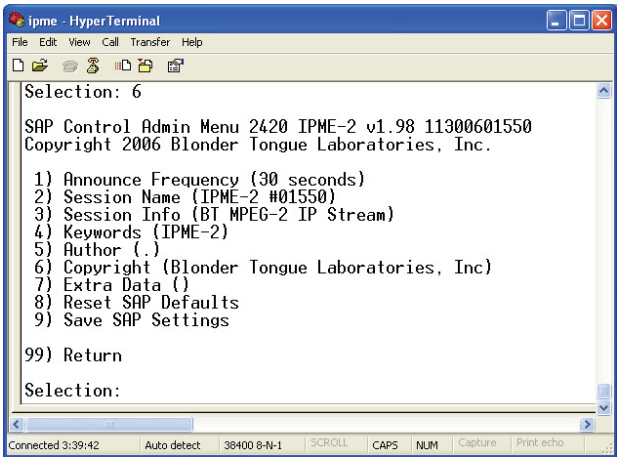
1. **Destination IP** — Sets the Destination IP address
2. **Destination Port** — Sets the Destination/UDP Port number
3. **Video Resolution** — Sets the resolution
4. **Stream Bitrate** — Sets the Stream Bitrate
5. **Video Input** — Sets the Video Input type
6. **Video Format** — Sets the Video Format type
7. **Audio Bitrate** — Sets the Audio Bitrate
8. **Encapsulation** — Sets the stream Encapsulation type
9. **FEC Parameters** — Sets the FEC Parameters
10. **AtoD Settings Menu** — Displays the AtoD Settings Menu, (detailed separately)

99. **Return** — This command is used to navigate back to the previous console menu



SAP Control Admin Menu — *Selection 3 of Video Admin Menu*

SAP (Session Announcement Protocol) is a protocol for broadcasting multicast session information. This menu contains the selections that administer the session information that is broadcast by SAP. Session information is broadcast only if the "Session Announcement" selection under the Options Admin Menu is "Enabled".

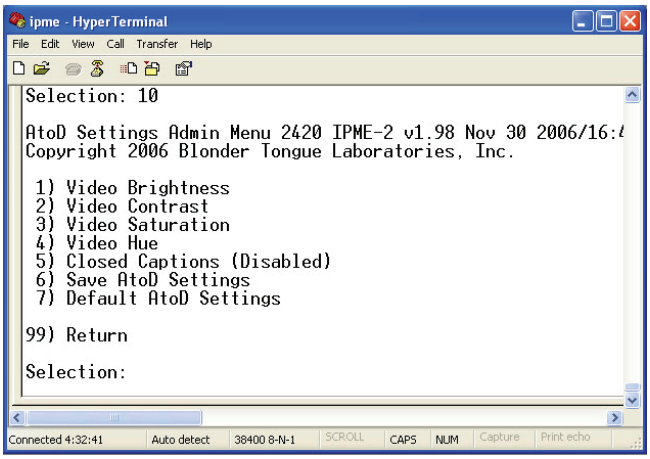


1. **Announce Frequency —** The time period after which the SAP is broadcast
2. **Session Name —** By default the IPME-2 SN# is displayed, this can be adjusted to a more suitable description to be broadcast if desired
3. **Session Info —** Provides for additional information on the broadcast session
4. **Keywords —** By default the product name is listed
5. **Author —** Available to display the SAP creator information, if desired
6. **Copyright —** Displays the Blonder Tongue Laboratories, Inc. Copyright
7. **Extra Data —** Available to display extra data information, if desired
8. **Reset SAP Data —** Resets the SAP Data
9. **Save SAP Settings —** Saves the current SAP settings to flash memory

99. **Return —** This command is used to navigate back to the previous console menu

AtoD Settings Admin Menu — *Selection 10 of Video Settings Admin Menu*

The AtoD Settings Admin Menu controls the Analog to Digital Converter settings.



1. **Video Brightness —** Adjusts the brightness of the video streamed
2. **Video Contrast —** Adjusts the picture contrast of the video streamed
3. **Video Saturation —** Adjusts the picture saturation of the video streamed
4. **Video Hue —** Adjusts the picture hue of the video streamed
5. **Closed Captions —** Enables or Disables closed captions
   a. If enabled, closed captions are displayed on STB clients
      i. If Enabled, an undesired green line may appear on the top of the Blonder Tongue IPCV PC Software video stream display
   b. This feature is disabled by default
6. **Save AtoD Settings** — Saves the current AtoD settings to flash memory
7. **Default AtoD Settings** — Resets the current AtoD settings to default

99. **Return** — This command is used to navigate back to the previous console menu

Low Latency Information

The IPME unit can be configured for optimized latency settings via the console menu. In the Video Admin menu there are 3 variables that in addition to the setting the bandwidth, control the latency of the stream. The GOP distance and length determine the presence and distribution of frame types (I,P,B) and the latency value setting controls how long buffers can be held in memory before transmission.

The recommended settings for highest quality / low latency optimization applications are as follows:

GOP Distance: 2

GOP Length: 8

Latency Value: 100

Stream Bitrate: 5.5 Mbps

Connecting to the IPME-2 with Telnet

Windows XP Application Note:

This application note should not apply if all Microsoft Windows XP Critical Updates have been applied, Proceed to step 1.

If you attempt to connect to an IPME via Telnet and have not installed all of the available Windows Critical Updates it may be necessary to precede ALL commands, except for the initial Username entry, with a single blank space. This includes the initial Password and all commands entered at the Telnet prompt

1) Open a Telnet session.
   (i) From the Windows Start button, select Run or open the Command Prompt from Programs
2) At the prompt type **telnet xxx.xxx.xxx.xxx**, where xxx.xxx.xxx.xxx is the IP Address of the IPME that you want to connect to. For example: **telnet 192.168.1.5.**
3) Enter the Administrator Username of the IPME
4) Enter the Administrator Password of the IPME. All characters should be hidden with the "*" character
   (i) If you are on a Windows XP based PC and have not installed all of your Windows Critical Updates, you must precede your password entry with a single blank space. See Note above.
5) Navigate the IPME menus
6) End the Telnet session. Click Ctrl +] to return to the prompt, and then type quit

NOTE: By default the Telnet capability is Disabled. It must be first enabled using the Console Menus through the RS-232 cable and connection via HyperTerminal.

IMPE-2 Web Interface

The IPME features an intergrated web interface that can be accessed to make modifications to the IPME status and configuration. The IPME must be located on an IP Network in order to connect to the web interface.

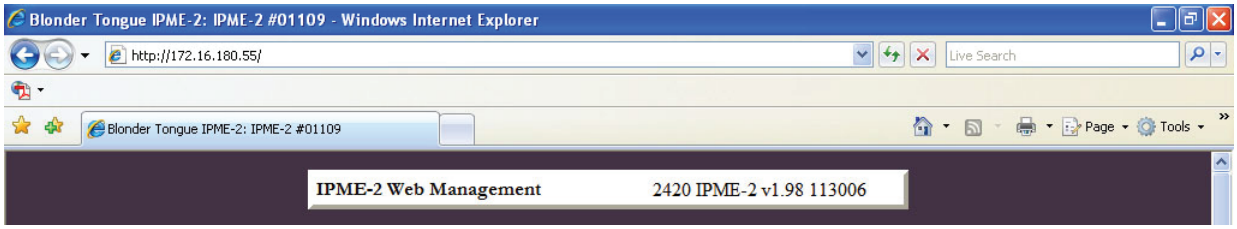
Note: The IPME web interface must be "Enabled" on the console menu prior to attempting to communicate via HyperTerminal or Telnet.

To ENABLE the IPME Web Interface

1. Access the console menu via Telnet or HyperTerminal
2. Access the Options Menu, selection 4
3. Activate the HTTP Server, selection 1 (this feature acts a toggle switch when selected)
4. Save the activation change, selection 12

Access the IPME Web Interface

- Open a standard web browser (such as Microsoft® Internet Explorer or Mozilla FireFox®)
- Enter the IP address of the IPME in the URL field
  - **http://xxx.xxx.xxx** where *xxx.xxx.xxx.xxx* is the IP Address of the IPME
    - Most web browsers only require the actual numerical IP address to be entered and will automatically enter the "http://" prefix.
    - Leading zero's should not be entered, for example 192.168.1.253
    - Click Enter or Go
  - The IPME's web interface should load into your browser window



ATTENTION!

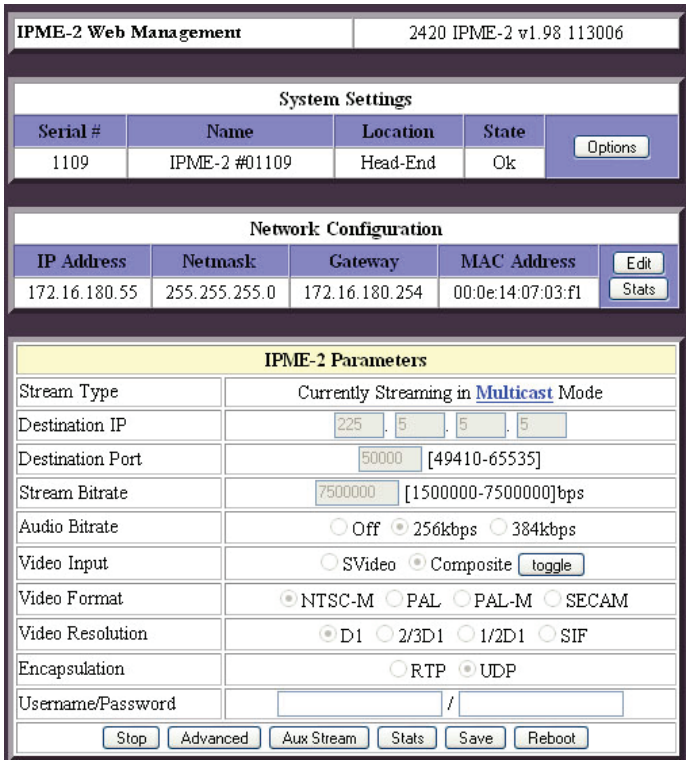
NOTE: It may be necessary to adjust your computer's IP address settings to ensure that the same subnet address is set to permit first-time communication to the IPME.

Adjust your IP address from automatically obtain or another fixed address to 192.168.1.2 (any last digit of 2-254 may be used that is different than encoder) & Subnet Mask to 255.255.0.0

Web Interface Menu

The IPME Web Interface Main Page consists of three sections with several sub-menu sections as follows

- System Settings
  - Options Button - Accesses the Systems Option web page
- Network Configuration
  - Edit Button - Accesses the IP Configuration web page
  - Stats Button - Accesses the Network Stats web page
- IPME Parameters
  - Advanced Button - Accesses the Advanced web page
  - Stats Button - Accesses the Video Stats web page



The IPME Web Management page displays the firmware verison and the date it was installed at the top of the page. It is formatted as IPME.50-x.xx, mm dd year, where x.xx is the Firmware verison.

System Settings Section

Serial Number - Displays the Serial Number of the IPME-2
Name - Displays the IPME-2 Model Name
This field is also user defined and can be set from the System Options page
Location - Displays the Location of the IPME-2
This field is also user defined and can be set from the System Options page.
State - Displays the current state of IPME
Possible States are OK and Needs Reboot
Options Button - Accesses the System Option page (detailed later)

Network Configuration Section

IP Address - Displays the IPME's current IP address
Netmask - Displays the IPME's current Netmask
Gateway - Displays the IPME's current Gateway IP address
MAC Address - Displays the IPME's MAC address
Edit Button - Accesses the IP Configuration page (detailed later)
Stats Button - Accesses the Network Stats page (detailed later)

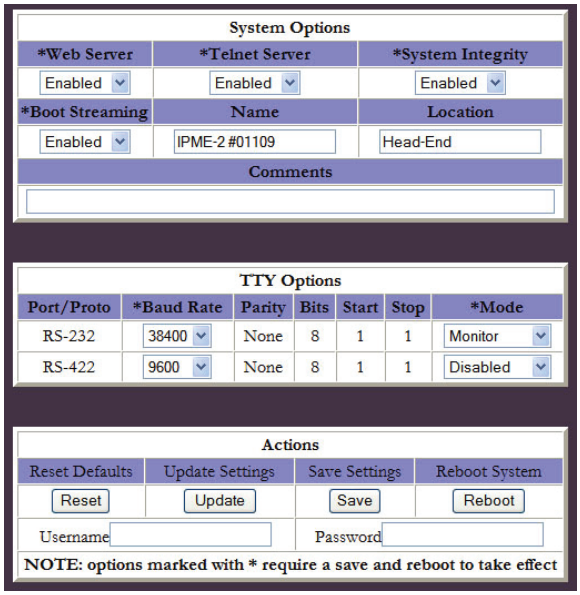
IPME Parameters Section

- Stream Type - Displays the detail on how the Stream Type is transmitted
- Destination IP — Displays the current destination IP address and permits the value to be changed
- Stream Bitrate — Displays the Stream Bitrate and permits this value to be changed
- Audio Bitrate — Displays the Audio Bitrate and permits editing by clicking the desired setting
- Video Input — Displays the current Video Input and permits editing via the toggle button
  - The IPME hardware only provides Composite Video Connections
- Video Format — Displays the current Video Input and permits editing by clicking the desired setting
- Video Resolution — Displays the Video Resolution and permits editing by clicking the desired setting
- Encapsulation — Displays the Encapsulation and permits editing by clicking the desired setting
- Username/Password — Username and Password values are required for Reboot and other IPME Administrative privileges and are entered here
- Encapsulation — Displays the Encapsulation and permits editing by clicking the desired setting

- **Interactive Buttons**
  - o Start — Starts the IPME IP transmit stream with the programmed values
  - o Advanced — Accesses the Advanced page (detailed later)
  - o Stats — Accesses the Video Stats page (detailed later)
  - o Save — Saves all IPME Parameter section values to flash memory
    - If the IPME is streaming, the new settings will not take effect until the stream is stopped and restarted
  - o Reboot — Reboots and applies any value changes from flash memory to take effect

Systems Options Page

Click the button on the right side of the System Settings section to access

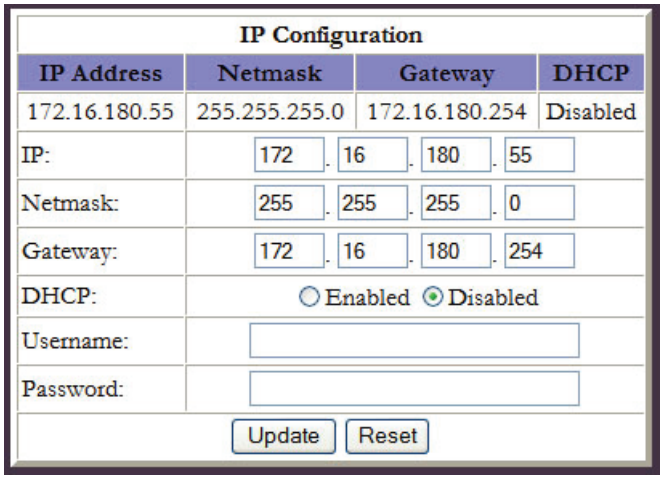


System Options Section

- Web Server — Displays the Web Server functionality, this can be Enabled or Disabled
- Telnet Server — Displays the Telnet functionality, this can be Enabled or Disabled
- System Integrity — Displays the System Integrity functionality, this can be Enabled or Disabled
- Boot Streaming — Displays the Boot Streaming functionality, this can be Enabled or Disabled
- Name — Displays the current IPME Name, this value can be user modified
- Location — Displays the current IPME Location, this value can be user modified
- Comments — Displays additional Comments, this value can be user modified
  - o This field is also user defined and can be set from the System Options page

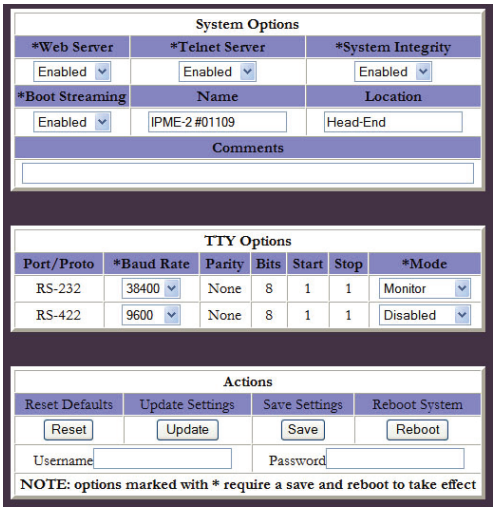
- **Interactive Buttons**
  - o Start — Starts the IPME IP transmit stream with the programmed values
  - o Advanced — Accesses the Advanced page (detailed later)
  - o Stats — Accesses the Video Stats page (detailed later)
  - o Save — Saves all IPME Parameter section values to flash memory
    - If the IPME is streaming, the new settings will not take effect until the stream is stopped and restarted
  - o Reboot — Reboots and applies any value changes from flash memory to take effect

IP Configuration Page



Systems Options Page

Click the button on the right side of the System Settings section to access



System Options Section

- Web Server — Displays the Web Server functionality, this can be Enabled or Disabled
- Telnet Server — Displays the Telnet functionality, this can be Enabled or Disabled
- System Integrity — Displays the System Integrity functionality, this can be Enabled or Disabled
- Boot Streaming — Displays the Boot Streaming functionality, this can be Enabled or Disabled
- Name — Displays the current IPME Name, this value can be user modified
- Location — Displays the current IPME Location, this value can be user modified
- Comments — Displays additional Comments, this value can be user modified
  - o This field is also user defined and can be set from the System Options page

TTY Options Section

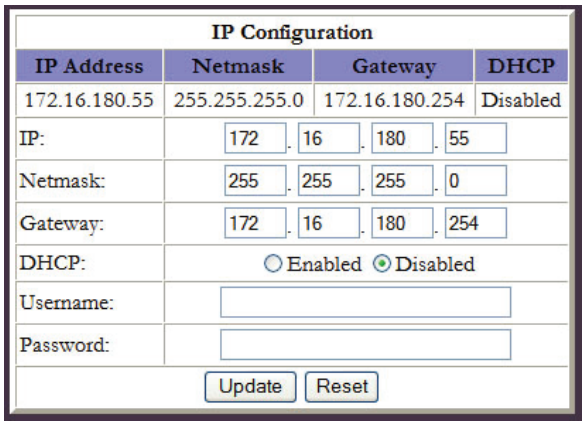
- Port/Proto — Displays the two IPME ports. 0/RS-232 and 1/RS-422
- Baud Rate — Shows the current Baud Rate for each port and allows this value to be changed
- Parity — Shows the current Parity for each port
- Bits — Shows the current Bits for each port
- Start — Shows the current Start bits for each port
- Stop — Shows the current Stop bits for each port
- Mode — Shows the current Mode for each port and allows this value to be changed

Action Settings

- Reset Defaults — Causes all the System Options, TTY Options, and Digital Inputs / Output options to be reset to factory default values
- Update Settings — Causes all the System Options, TTY Options, and Digital Inputs / Output options to be saved to memory. These changes take effect immediately but will not be saved across an IPME reboot. If the IPME is streaming, the new settings will not take effect until the stream is stopped and restarted
- Save Settings — Causes all the System Options, TTY Options, and Digital Inputs / Output options to be saved to Flash.

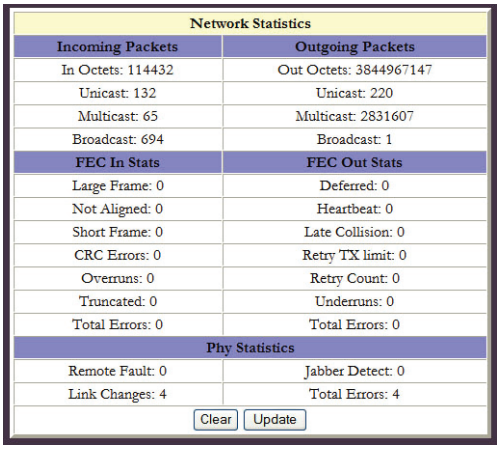
Note: Changed fields marked with an asterisk (*) do not take effect immediately and require an IPME reboot

IP Configuration Page

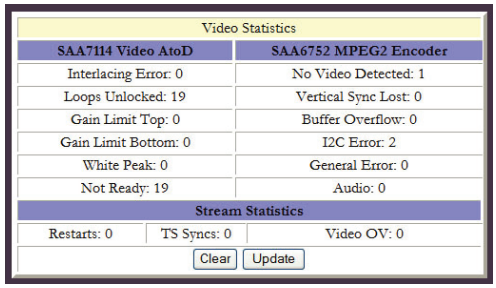


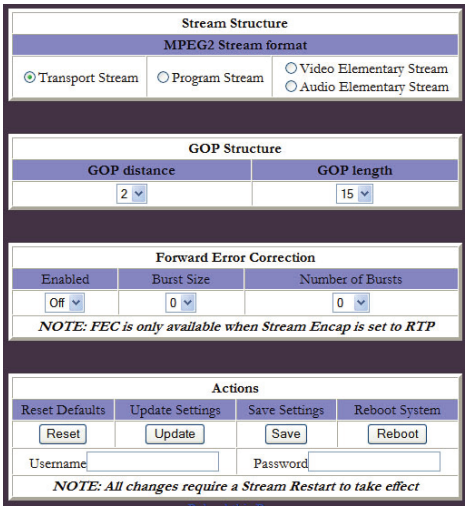
- IP Address | Netmask | Gateway | DHCP header – displays the IPME's current IP Configuration settings.
- IP – displays the IP address that is used when DHCP is disabled and allows the address to be changed.
- Netmask – displays the Netmask that is used when DHCP is disabled and allows the address to be changed.
- Gateway – displays the Gateway that is used when DHCP is disabled and allows the address to be changed.
- DHCP – displays the current DHCP mode and allows the mode to be changed.
- Username – enter the Username associated with the IPME, which is required for IP configuration.
- Password – enter the Password associated with the IPME, which is required for IP configuration.
- Update – causes all the IP Configuration settings to be saved to Flash. After a successful Update, the IPME must be rebooted for the changes to take effect.
- Reset – This does NOT cause the IP Configuration values to be reset to factory default values, but only resets the values that were displayed when the web page was first opened.

Network Statistics Page



Video Statistics Page





GOP Structure

- GOP Distance — displays the current GOP Distance and allows the value to be edited. See Section 5.3 for information on valid GOP settings
- GOP Length — displays the current GOP Length and allows the value to be edited. See Section 5.3 for information on valid GOP settings

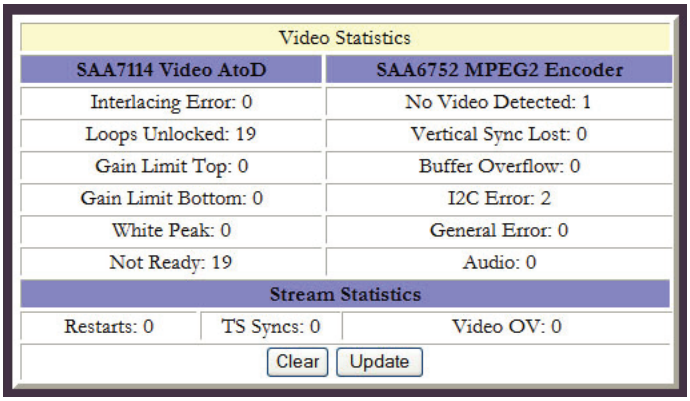
Forward Error Correction

- Enabled — displays the current FEC mode (On or Off) and enables the setting of this mode
- Burst Size — displays the current Burst Size and allows this value to be set
- Number of Bursts — displays the current Number of Bursts and allows this value to be set

Actions

- Reset Defaults – resets all the Advanced setting values to factory default values. If the IPME is streaming the new settings will not take effect until the stream is stopped and restarted
- Update Settings — saves all the current Advanced Settings to memory. These changes take effect immediately but will not be saved across an IPME reboot
- Save Settings — saves Advanced settings to Flash and requires an IPME reboot to take effect

Video Statistics Page



IPME-2 Factory Default Settings

Default Video Settings

Destination IP: 225.168.1.253
Destination Port: 50000
Video Resolution: 0=D1
Stream Bitrate: 3800000
Video Input: 1=Composite
Video Format: 0=NTSC
Audio Bitrate: 1=256Kbps
Encapsulation: 1=UDP

Default AtoD Settings

Video Brightness: 128
Video Contrast: 68
Video Saturation: 64
Video Hue: 0
Closed Captions: Disabled

Default Options Settings

HTTP Server (Disabled)
Telnet Server (Disabled)
Stream at Bootup (Enabled)
System Integrity (Enabled)
Session Announcement (Enabled)
System Kicker (Disabled)
Join Mcast Group (Enabled)

Default Config Settings

Location: Head-End
IP Address: 192.168.1.253
Netmask: 225.255.255.0
Gateway: 0.0.0.0
Use DHCP: no

Default Security Settings

Username: admin
Password: admin

Static IP Configuration

IPME-2

Static IP Addressing is recommended for setup of the IPME IP Configuration.

Note: In order to configure your IPME with a static IP Address, you will need to ensure that its DHCP functionality is Off. By factory default, DHCP is off.

To assign a static IP Address to the IPME, follow these steps from the RS232 Console Menu:

1. From the Main Admin Menu select the "Video Menu" option, by pressing 1 and Enter
   a) Ensure that the Stream is Stopped, by pressing 2 ("Stop Stream" option) and Enter.
2. From the Main Admin Menu, select the "Config Menu" option, by pressing 5 and Enter.
   a) Set the "IP Address" for the unit
   b) Set the "Netmask"
   c) Set the "Gateway", to the default gateway.
   d) Select the "Save" option and Enter, to save configuration changes.
   e) To return, press 99 and Enter.
3. From the Main Admin Menu, select the "Reboot" option, by pressing 6, and Enter.
4. From the Main Admin Menu select the "Video Menu" option, by pressing 1 and Enter
   a) Ensure that the Stream is Stopped, by pressing 2 ("Stop Stream" option) and Enter.
   b) From the Video Admin Menu select the "Video Settings Menu" option, by pressing 3 and Enter.
   c) From the Video Settings Admin Menu,
      i. Set the "Destination IP" to either the Unicast or Multicast IP Address of the stream.
      ii. Set the 'Destination Port" to an un-used port.
      iii. To return, press 99 and Enter.
   d) Select "Save Video Settings" to store video settings.
   e) To return to the Main Admin Menu, press 99 and Enter.
5. From the Main Admin Menu, select the "Reboot" option, by pressing 6, and Enter.

IPME Stream Manager Setup (optional hardware unit)

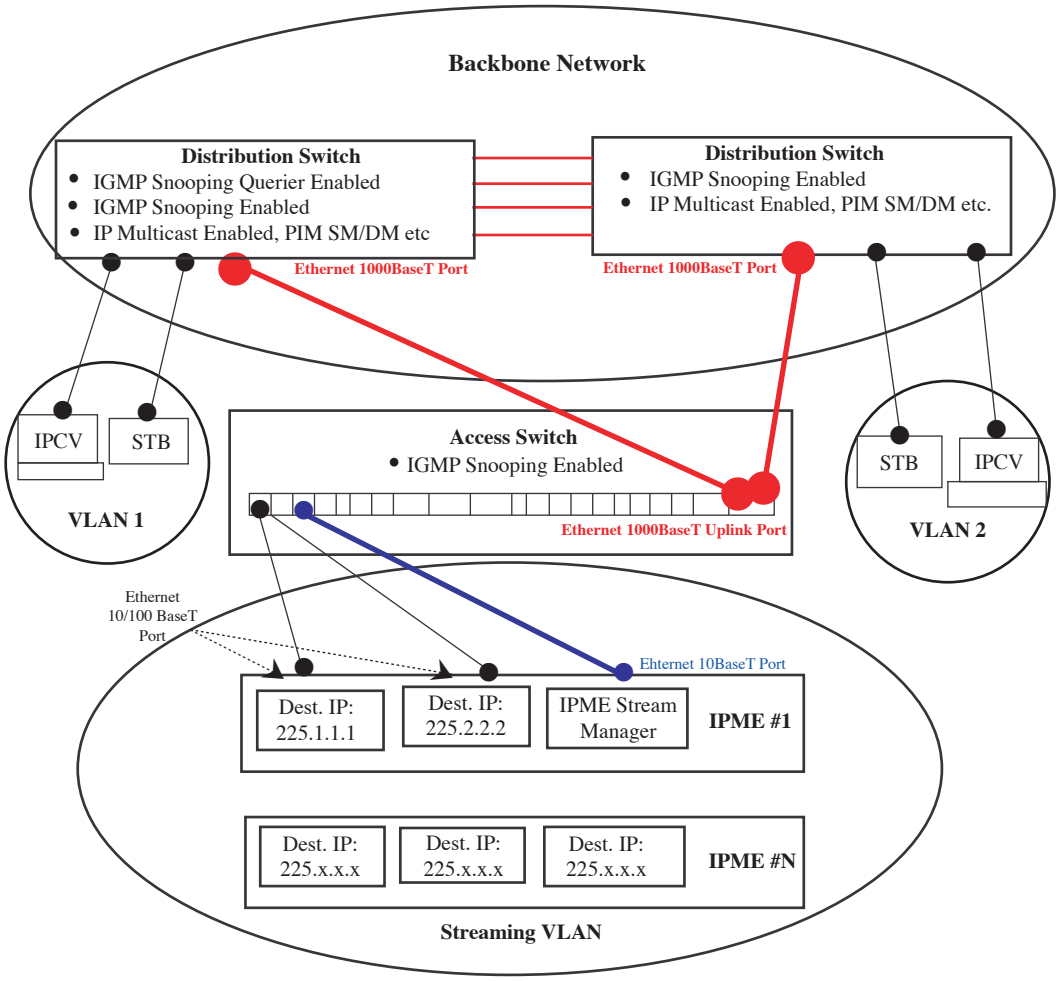
Only the use of Static IP Addressing is supported by the IPME Stream Manager.

1. From the "**Address Bar**" of Internet Explorer, access the **Admin** url of the IPME Stream Manager. E.g. http://192.168.1.100/Admin.htm
2. To statically assign the **IP Address** of the IPME Stream Manager
   a) For **IP Type**: select **Fixed**
   b) For **IP Address**: enter the IP Address for the IPME Stream Manager
3. Type in the **Subnet Mask**
4. Type in the **Default Gateway**
5. Change the **Admin ID** and **Admin Password**, to gain administrator privileges
6. Change the **View ID** and **View Password** for viewer (non-administrative) privileges
7. Change the **FTP ID** and **FTP Password** to a user name for access to ftp privileges
8. Click the "**Save**" button, to save changes.
9. Power-cycle the IPME Stream Manager for the changes to be effective

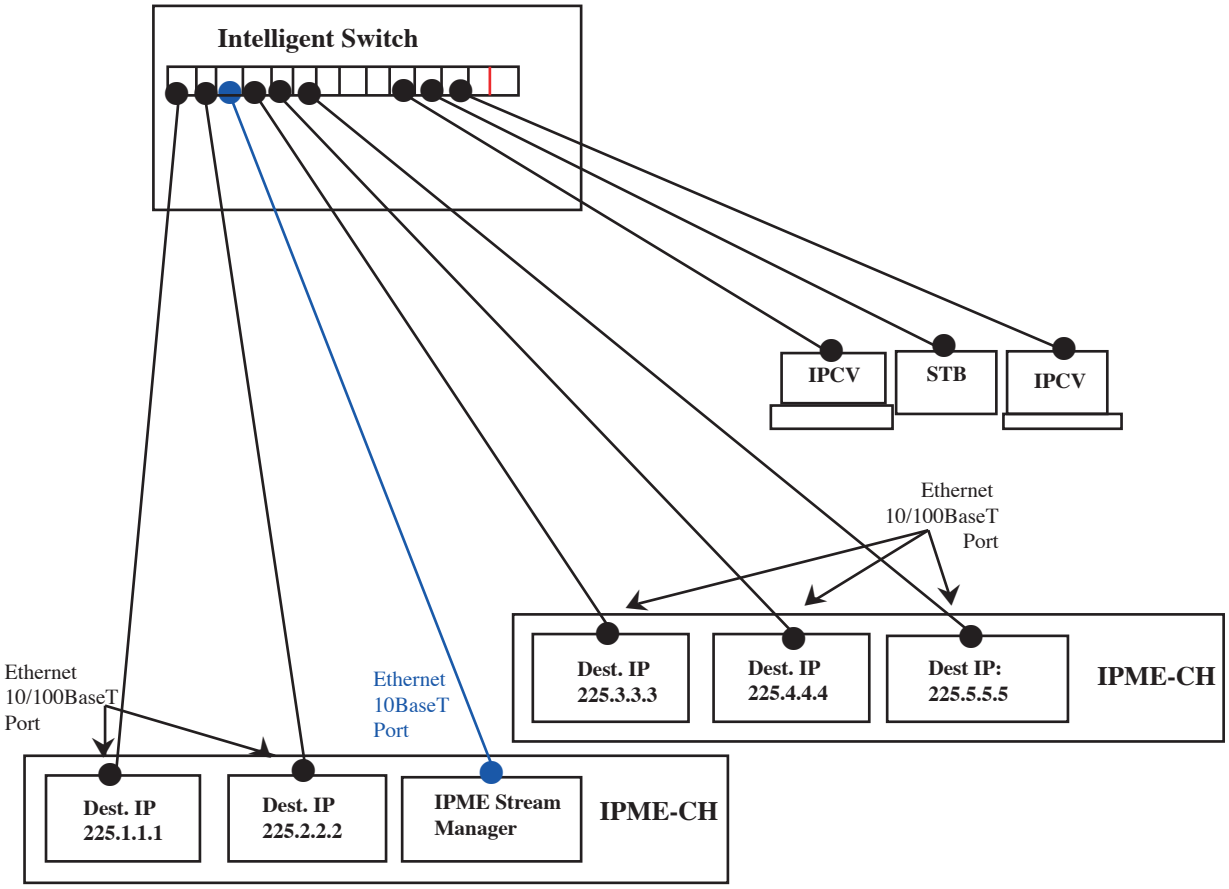
NOTE: See the IPME Stream Manager Instruction Manual documention for additional configuration and set-up details

Networking Diagram Examples

Typical Commercial Network Architecture Example — consists of streaming IPME-2 units with an optional Stream Manager in 2 VLAN's



Typical Closed Network Architecture Example — consists of streaming IPME-2 units in a single switch network environment



Switch Examples:
Cisco Catalyst 2950T-24
Lantech FE-24F2GBTM
Lantech FE-A801FM

- Switch requires IGMP Snooping Querier capability enabled
- Switch requires IGMP Snooping capability

Background Network Connection Information

Internet Protocol (IP) Multicast

Internet Protocol (IP) multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to multiple hosts.

IP Multicast delivers source traffic to multiple receivers without adding any additional burden on the source or the receivers while using the least network bandwidth of any competing technology. Multicast packets are replicated in the network by routers enabled with Protocol Independent Multicast (PIM) and other supporting multicast protocols resulting in the most efficient delivery of data to multiple receivers possible. All alternatives require the source to send more than one copy of the data. Some even require the source to send an individual copy to each receiver. If there are thousands of receivers, even low-bandwidth applications benefit from using IP Multicast. High-bandwidth applications, such as MPEG video, may require a large portion of the available network bandwidth for a single stream. In these applications, the only way to send to more than one receiver simultaneously is by using IP Multicast.

Multicast Group Concept

Multicast is based on the concept of a group. An arbitrary group of receivers expresses an interest in receiving a particular data stream. This group does not have any physical or geographical boundaries—the hosts can be located anywhere on the network. Hosts that are interested in receiving data flowing to a particular group must join the group using IGMP. Hosts must be a member of the group to receive the data stream.

IP Multicast Addresses

Multicast addresses specify an arbitrary group of IP hosts that have joined the group and want to receive traffic sent to this group.

IP Class D Addresses

The Internet Assigned Numbers Authority (IANA) controls the assignment of IP multicast addresses. It has assigned the old Class D address space to be used for IP multicast. This means that all IP multicast group addresses will fall in the range of 224.0.0.0 to 239.255.255.255.

Globally Scoped Address

The range of addresses from 224.0.1.0 through 238.255.255.255 are called globally scoped addresses. They can be used to multicast data between organizations and across the Internet.

Some of these addresses have been reserved for use by multicast applications through IANA. For example, 224.0.1.1 has been reserved for Network Time Protocol (NTP).

Limited Scope Addresses

The range of addresses from 239.0.0.0 through 239.255.255.255 contains limited scope addresses or administratively scoped addresses. These are defined by RFC 2365 to be constrained to a local group or organization. Routers are typically configured with filters to prevent multicast traffic in this address range from flowing outside an autonomous system (AS) or any user-defined domain. Within an autonomous system or domain, the limited scope address range can be further subdivided so those local multicast boundaries can be defined. This also allows for address reuse among these smaller domains.

Unicast and Multicast Transmissions over the Network

A Unicast transmission sends IP packets to a single recipient on a network. A Multicast transmission sends IP packets to a group of hosts on a network. If the streaming video is to be distributed to a single destination, then you would select the Unicast mode when you go to start your IPME transmission. If you want to view the stream at multiple concurrent locations, then you would select the Multicast mode.

Since Multicasting is a relatively new technology, however, some legacy devices that are part of your network might not support Multicasting.

Before using the IPME in Multicast streaming mode, check the functional specifications of your network infrastructure to ensure that the Multicast stream will not create major traffic on your network. Verify that your backbone switch supports Internet Group Messaging Protocol (IGMP) snooping, which allows the core of your network to ignore the traffic streams that Multicasting may generate.

IGMP and IGMP Snooping — Internet Group Management Protocol

IGMP is a session-layer (Layer 3) protocol used to establish membership in a Multicast group and can register a router to receive specific Multicast traffic. (Refer to RFC 1112 and RFC 2236 for information on IGMP versions 1 and 2.)

IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Hosts identify group memberships by sending IGMP messages to their local multicast router. Under IGMP, routers listen to IGMP messages and periodically send out queries to discover which groups are active or inactive on a particular subnet. IGMP comes in three versions (v1,v2,v3), of which v2 is used by the IPClientViewer and IPME Stream Manager.

A Layer 2 switch supporting IGMP Snooping can passively snoop on IGMP Query, Report, and Leave (IGMP version 2) packets transferred between IP Multicast Routers/Switches and IP Multicast hosts to determine the IP Multicast group membership. IGMP snooping checks IGMP packets passing through the network, picks out the group registration, and configures Multicasting accordingly.

Without IGMP Snooping, Multicast traffic is treated in the same manner as a Broadcast transmission, which forwards packets to all ports on the network. With IGMP Snooping, Multicast traffic is only forwarded to ports that are members of that Multicast group. IGMP Snooping generates no additional network traffic, allowing a significant reduction in the Multicast traffic passing through your switch.

If your network is based on a switch or a hub that does not support IGMP Snooping, the IPME streams will still function as designed but your network may be subjected to high traffic loads and condensed collision domain due to the broadcasting action used by the older switch or hub. If this is the case, you may wish to isolate the streaming nodes within the network so that the streams may be viewed without crossing the normal network traffic along its path.

Otherwise, for a general performance improvement, you may consider upgrading your network core to a switch that is Multicast aware.

IGMP Version 2

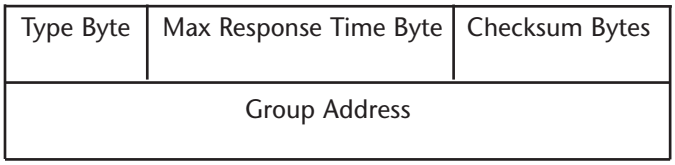
IGMPv2 is defined by IETF RFC 2236. It is the earliest IGMP version used to support IPTV. The key advantage of IGMPv2 over the older IGMPv1 is the addition of the Leave Group Message allowing a host to immediately signal its request to leave a multicast group. This is a major requirement in IPTV applications where bandwidth is at a premium and the forwarding of inactive multicast groups across a broadband connection can lead to periods of congestion and poor video quality.

IGMPv2 is designed to support Any Source Multicast (ASM) networks. In an ASM network, the IGMP host specifies the multicast group that it wishes to join, and listens to all traffic in that group regardless of who is sending the traffic.

IGMPv2 is backwards compatible with IGMPv1.

IGMPv2 Frames

The packet format for IGMPv2 is shown below. It is a simple packet format containing the Type of packet, a Maximum Response Time (MRT), Checksum, and Group Address.



IGMPv2 Packet Format Example

The Type field indicates what message is being sent, and is discussed below. The Maximum Response Time indicates how long the sender should wait for a response. The Group Address specifies which multicast group this frame refers to.

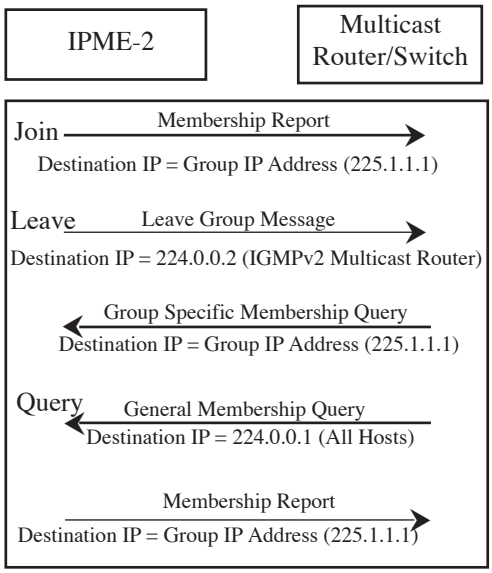
There are three types of IGMPv2 packets (ignoring IGMPv1 backwards compatibility):

- Membership Report, which is used by a host to JOIN a group or to respond to Membership Queries. Membership Reports may be sent by an IGMP host without prompting (unsolicited) or in response to a Membership Query (solicited). For IGMPv2, Membership Reports have a Type of 0x16
- Leave Group Message, which is used by a host to explicitly LEAVE a multicast group. Leave Group Messages have a Type of 0x17
- Membership Query, which is sent by the multicast router to determine if any hosts are listening to a group. All membership Queries have the Type field set to 0x11. There are two types of Membership Queries
  - o General Query asks whether any host is listening to any group
  - o Group-Specific Query is used to determine whether any host is listening to a specific multicast group

IGMPv2 makes use of two reserved multicast addresses:

- 224.0.0.1 is used by the IGMP router to send messages to "all multicast hosts" (otherwise known as "all systems")
- 224.0.0.2 is used by the IGMP host to send messages to "all multicast routers"

IGMPv2 Operation



IGMPv2 Operation Example Using IGMPv2 w/ Optional IPCV & IPME-SM

IGMPv2 Basic Operations:

• JOIN: When an IGMPv2 host needs to join a group [such as the IPCV wishing to view a new channel], it will send an unsolicited Membership Report destined to the group it wishes to join. Upon receiving the membership report, the multicast router will begin forwarding the channel out the appropriate interface (if it is not already being forwarded out that interface).

• LEAVE: When an IGMPv2 host leaves a group [such as the IPCV is no longer watching a channel], it will send out a Leave Group Message to the 224.0.0.2 multicast router address listing the group to leave in the Group Address field. The router will immediately respond on the logical interface with a Group-Specific Query to the multicast group address to determine if any hosts are still wishing to receive this specific multicast group. The MRT value will determine the timeout period to wait for a host response to the query. If no response is received within the MRT interval, the router will no longer forward that multicast group out that specific interface.

• QUERY: The General Membership Query is issued periodically to the all-hosts 224.0.0.1 multicast address to determine which groups are currently being used by IGMPv2 hosts. The MRT is used to specify the timeout interval that the router will wait for host responses to the query. If no host responds during the MRT interval, then packet forwarding stops for any groups not required out an interface. The General Membership Query is typically used to recover from error conditions such as a IPCV being shut down and not able to send a Leave Group message or Leave Group messages being dropped by the access elements. This provides a self-healing mechanism for IGMP to synchronize multicast state within the network.

PIM

Protocol Independent Multicast (PIM) is a collection of multicast routing protocols, each optimized for a different environment. There are two main PIM protocols, PIM Sparse Mode and PIM Dense Mode. A third PIM protocol, Bi-directional PIM, is less widely used.

Typically, either PIM Sparse Mode or PIM Dense Mode will be used throughout a multicast domain. However,

they may also be used together within a single domain, using Sparse Mode for some groups and Dense Mode for others. This mixed-mode configuration is known as Sparse-Dense Mode. Similarly, Bi-directional PIM may be used on its own, or it may be used in conjunction with one or both of PIM Sparse Mode and PIM Dense Mode.

All PIM protocols share a common control message format. PIM control messages are sent as raw IP datagrams (protocol number 103), either multicast to the link-local ALL PIM ROUTERS multicast group, or unicast to a specific destination.

PIM Sparse Mode

PIM Sparse Mode (PIM-SM) is a multicast routing protocol designed on the assumption that recipients for any particular multicast group will be sparsely distributed throughout the network. In other words, it is assumed that most subnets in the network will not want any given multicast packet. In order to receive multicast data, routers must explicitly tell their upstream neighbors about their interest in particular groups and sources. Routers use PIM Join and Prune messages to join and leave multicast distribution trees.

PIM-SM by default uses shared trees, which are multicast distribution trees rooted at some selected node (in PIM, this router is called the Rendezvous Point, or RP) and used by all sources sending to the multicast group. To send to the RP, sources must encapsulate data in PIM control messages and send it by unicast to the RP. This is done by the source's Designated Router (DR), which is a router on the source's local network. A single DR is elected from all PIM routers on a network, so that unnecessary control messages are not sent.

One of the important requirements of PIM Sparse Mode, and Bi-directional PIM, is the ability to discover the address of a RP for a multicast group using a shared tree. Various RP discovery mechanisms are used, including static configuration, Bootstrap Router, Auto-RP, Anycast RP, and Embedded RP.

PIM-SM also supports the use of source-based trees, in which a separate multicast distribution tree is built for each source sending data to a multicast group. Each tree is rooted at a router adjacent to the source, and sources send data directly to the root of the tree. Source-based trees enable the use of Source-Specific Multicast (SSM), which allows hosts to specify the source from which they wish to receive data, as well as the multicast group they wish to join. With SSM, a host identifies a multicast data stream with a source and group address pair (S,G), rather than by group address alone (*,G).

PIM-SM may use source-based trees in the following circumstances:

- For SSM, a last-hop router will join a source-based tree from the outset
- To avoid data sent to an RP having to be encapsulated, the RP may join a source-based tree
- To optimize the data path, a last-hop router may choose to switch from the shared tree to a source-based tree

PIM-SM is a soft-state protocol. That is, all state is timed-out a while after receiving the control message that instantiated it. To keep the state alive, all PIM Join messages are periodically retransmitted.

There have been many implementations of PIM-SM and it is widely used.

PIM Dense Mode

PIM Dense Mode (PIM-DM) is a multicast routing protocol designed with the opposite assumption to PIM-SM, namely that the receivers for any multicast group are distributed densely throughout the network. That is, it is assumed that most (or at least many) subnets in the network will want any given multicast packet. Multicast data is initially sent to all hosts in the network. Routers that do not have any interested hosts then send PIM Prune messages to remove themselves from the tree.

When a source first starts sending data, each router on the source's LAN receives the data and forwards it to all its PIM neighbors and to all links with directly attached receivers for the data. Each router that receives a forwarded packet also forwards it likewise, but only after checking that the packet arrived on its upstream interface. If not, the packet is dropped. This mechanism prevents forwarding loops from occurring. In this way, the data is flooded to all parts of the network.

Some routers will have no need of the data, either for directly connected receivers or for other PIM neighbors.

These routers respond to receipt of the data by sending a PIM Prune message upstream, which instantiates Prune state in the upstream router, causing it to stop forwarding the data to its downstream neighbor. In turn, this may cause the upstream router to have no need of the data, triggering it to send a Prune message to its upstream neighbor. This 'broadcast and prune' behavior means that eventually the data is only sent to those parts of the network that require it.

Eventually, the Prune state at each router will time out, and data will begin to flow back into the parts of the network that were previously pruned. This will trigger further Prune messages to be sent, and the Prune state will be instantiated once more.

PIM-DM only uses source-based trees. As a result, it does not use RPs, which makes it simpler than PIM-SM to implement and deploy. It is an efficient protocol when most receivers are interested in the multicast data, but does not scale well across larger domains in which most receivers are not interested in the data.

PIM Dense Mode (PIM DM) is less common than PIM-SM, and is mostly used for individual small domains.

Bi-directional PIM

Bi-directional PIM (BIDIR-PIM) is a third PIM protocol, based on PIM-SM. The main way BIDIR-PIM differs from PIM-SM is in the method used to send data from a source to the RP. Whereas in PIM-SM data is sent using either encapsulation or a source-based tree, in BIDIR-PIM the data flows to the RP along the shared tree, which is bi-directional - data flows in both directions along any given branch.

BIDIR-PIM's major differences from PIM-SM are as follows.

- There are no source-based trees, and in fact no (S,G) state at all. Therefore there is no option for routers to switch from a shared tree to a source-based tree, and Source-Specific Multicast is not supported
- To avoid forwarding loops, for each RP one router on each link is elected the Designated Forwarder (DF). This is done at RP discovery time using the DF election message
- There is no concept of a Designated Router
- No encapsulation is used
- The forwarding rules are very much simpler than in PIM-SM, and there are no data-driven events in the control plane at all

The main advantage of BIDIR-PIM is that it scales very well when there are many sources for each group. However, the lack of source-based trees means that traffic is forced to remain on the possibly inefficient shared tree.

Mixed-mode PIM Configurations

Typically, PIM-SM, PIM-DM or BIDIR-PIM would be used alone throughout a multicast domain. However it is possible to use a combination of the three by distributing multicast groups between the different protocols. Each group must operate in either sparse, dense or bi-directional mode; it is not possible to use a single group in more than one mode at once. Given such a division, the protocols coexist largely independent of one another.

The one way in which the protocols interact is that the same PIM Hello protocol is used by each, and is only run once on each link. The information learned from the Hello message exchange must be shared among the three routing protocols.

The method used to distribute groups between the three protocols is outside the scope of the PIM protocols and is a matter of local configuration. Note that it is important that every router in the domain has the same assignment of groups to protocols. The following techniques are used:

• The Bootstrap Router (BSR) protocol, used for RP discovery, has been extended to add a "Bi-directional" bit for each group range. This method may be used to assign groups between sparse and bi-directional modes if using BSR

• Routers may be configured to use dense mode if the RP discovery mechanism (whatever that may be) fails to find an available RP for a group, and to use sparse or bi-directional mode otherwise

• Router may be manually configured with group ranges for sparse, dense and bi-directional modes

Group of Pictures (GOP)

The Group of Pictures (GOP) in the IPME environment is defined by Distance and Length as follows:

The GOP frame distance determines the type and frequency of the order of individual frames. A single frame can be an Intracoded Frame (I Frame), a Predicted Frame (P Frame), or Bidirectional Predicted Frame (B Frame). The type and order of frame is determined by the frame distance.

For example:

Distance = 0 would be I Frames only. (I I I I I I I I I...)

Distance = 1 would be I and P Frames. (IPP....PPIPP...)

Distance = 2 would be all frames. (IBP...BP..)

Distance = 3 would be all frames with many B Frames (IBBP...BBP)

Distance 3 would yield the highest compression, distance 0 would have the most detail.

The second parameter in question is the GOP Frame Length. The length defines the number of frames in a single repeating GOP structure. In the case where distance = 0, the length has no real effect because there are only I Frames in the GOP to begin with. In the other cases the length will define how many of each frame will appear in the structure before it repeats.

If distance = 1 and length = 2, the GOP structure will be a repeating pattern like “IP IP IP IP IP”. If distance = 1 and length = 3, the GOP structure will be a repeating pattern like “IPP IPP IPP”, and for length = 4 then ”IPPP IPPP IPPP”. The same is true for distances 2 and 3, as the length will determine the number of frames between I Frames.

The following is a list of potential values:

Distance = M, Length = N

Real Closed GOP: M,N (2,3 2,5 2,7 2,9 2,11 2,13 2,15 2,17 2,19 3,4 3,7 3,10 3,13 3,19)

Non-Editable GOP: M,N (2,4 2,6 2,8 2,10 2,12 2,14 2,16 2,18 3,6 3,9 3,12 3,15 3,16 3,18)

All other configurations are undefined (not necessarily bad or illegal, just undefined)

IPME GOP Structure

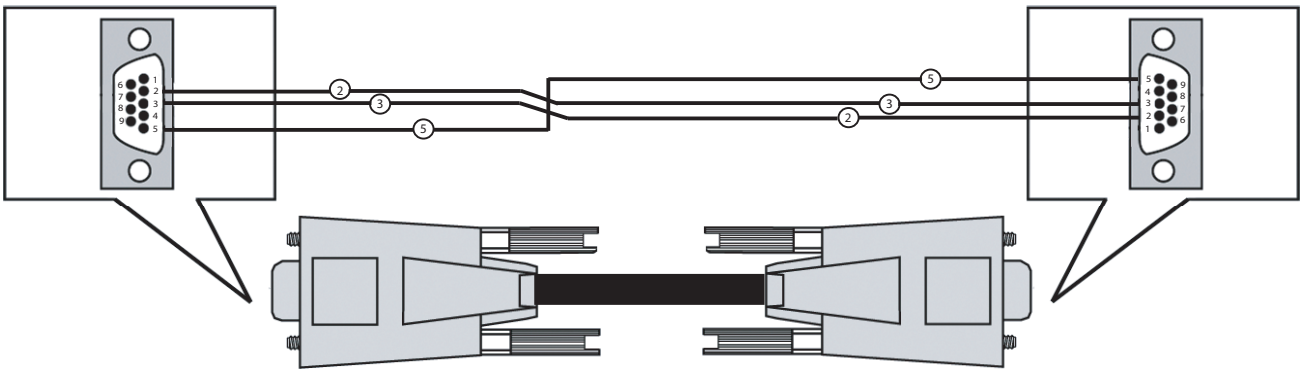
The factory default values are: N = 2, M = 15. For lower latency video transmission, the following setting is recommended: N = 2, M = 3, this will reduce encode latency from approximately 200 ms to approximately 100 ms.

To modify the GOP settings in an IPME unit, access the Console Menu (via Serial connection or Telnet) and go to the Options menu. The Options menu provides two GOP configuration items: Set GOP Distance and Set GOP Length.

Use these menu options to set the values to the appropriate setting and then save the options to store the settings to the flash. The GOP settings can be viewed and set from the IPME Web Management pages under the Options button.

Appendix A

RS-232 Null Modem Cable / Connector Diagram and Pin Assignment



Connector 1	Connector 2	Function
2	3	Rx□Tx
3	2	Tx➧Rx
5	5	Signal ground

Notes

Notes

Notes

Limited Warranty

Blonder Tongue Laboratories, Inc. (BT) will at its sole option, either repair or replace (with a new or factory reconditioned product, as BT may determine) any product manufactured by BT which proves to be defective in materials or workmanship or fails to meet the specifications which are in effect on the date of shipment or such other specifications as may have been expressly agreed upon in writing (i) for a period of one (1) year from the date of original purchase (or such shorter period of time as may be set forth in the license agreement specific to the particular software being licensed), with respect to iCentral™ (hardware and software) and all other software products (including embedded software) licensed from BT, (ii)) for a period of one (1) year from the date of original purchase, with respect to all MegaPort™, IPTV products, and fiber optics receivers, transmitters, couplers and integrated receiver/distribution amplifiers (including TRAILBLAZER™, RETRO-LINX™ and TWIN STAR™ products) as well as for DigiCipher ® satellite receivers, and (iii) for a period of three (3) years from the date of original purchase, with respect to all other BT products. Notwithstanding the foregoing, in some cases, the warranty on certain proprietary sub-assembly modules manufactured by third-party vendors and contained in BT products and on certain private–label products manufactured by third-parties for resale by BT are of shorter duration or otherwise more limited than the standard BT limited warranty. In such cases, BT's warranty with respect to such third-party proprietary sub-assembly modules and private-label products will be limited to the duration and other terms of such third-party vendor's warranty. In addition, certain products, that are not manufactured but are resold by BT, carry the original OEM warranty for such products. The limited warranty set forth in this paragraph does not apply to any product sold by BT, which at the time of sale constituted a Refurbished/Closeout Product.

(b) BT will at its sole option, either repair or replace (with a new or factory-reconditioned product, as BT may determine) any product sold by BT which at the time of sale constituted a refurbished or closeout item ("Refurbished/Closeout Product"), which proves to be defective in materials or workmanship or fails to meet the specifications which are in effect on the date of shipment or such other specifications as may have been expressly agreed upon in writing, for a period of ninety (90) days from the date of original purchase. Notwithstanding the foregoing, in some cases the warranty on third party software and on certain proprietary sub-assembly modules manufactured by third-party vendors and contained in BT products and on certain private–label products manufactured by third-parties for resale by BT are of shorter duration or otherwise more limited than the BT limited warranty for Refurbished/Closeout Products. In such cases, BT's warranty for Refurbished/Closeout Products constituting such third party software, third-party proprietary sub-assembly modules and private-label products will be limited to the duration and other terms of such third-party vendor's warranty. In addition, notwithstanding the foregoing, (i) certain Refurbished/Closeout Products that are not manufactured (but are resold) by BT, carry the original OEM warranty for such products, which may be longer or shorter than the BT limited warranty for Refurbished/Closeout Products. All sales of Refurbished/Closeout Products are final.

To obtain service under this warranty, the defective product, together with a copy of the sales receipt or other satisfactory proof of purchase and a brief description of the defect, must be shipped freight prepaid to: Blonder Tongue Laboratories, Inc., One Jake Brown Road, Old Bridge, New Jersey 08857.

This warranty does not cover damage resulting from (i) use or installation other than in strict accordance with manufacturer's written instructions, (ii) disassembly or repair by someone other than the manufacturer or a manufacturer-authorized repair center, (iii) misuse, misapplication or abuse, (iv) alteration, (v) lack of reasonable care or (vi) wind, ice, snow, rain, lightning, or any other weather conditions or acts of God.

OTHER THAN THE WARRANTIES SET FORTH ABOVE, BT MAKES NO OTHER WARRANTIES OR REPRESENTATIONS OF ANY KIND, EXPRESS OR IMPLIED, AS TO THE CONDITION, DESCRIPTION, FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR AS TO ANY OTHER MATTER, AND SUCH WARRANTIES SUPERSEDE ANY ORAL OR WRITTEN WARRANTIES OR REPRESENTATIONS MADE OR IMPLIED BY BT OR BY ANY OF BT'S EMPLOYEES OR REPRESENTATIVES, OR IN ANY OF BT'S BROCHURES MANUALS, CATALOGS, LITERATURE OR OTHER MATERIALS. IN ALL CASES, BUYER'S SOLE AND EXCLUSIVE REMEDY AND BT'S SOLE OBLIGATION FOR ANY BREACH OF THE WARRANTIES CONTAINED HEREIN SHALL BE LIMITED TO THE REPAIR OR REPLACEMENT OF THE DEFECTIVE PRODUCT F.O.B. SHIPPING POINT, AS BT IN ITS SOLE DISCRETION SHALL DETERMINE. BT SHALL IN NO EVENT AND UNDER NO CIRCUMSTANCES BE LIABLE OR RESPONSIBLE FOR ANY CONSEQUENTIAL, INDIRECT, INCIDENTAL, PUNITIVE, DIRECT OR SPECIAL DAMAGES BASED UPON BREACH OF WARRANTY, BREACH OF CONTRACT, NEGLIGENCE, STRICT TORT LIABILITY OR OTHERWISE OR ANY OTHER LEGAL THEORY, ARISING DIRECTLY OR INDIRECTLY FROM THE SALE, USE, INSTALLATION OR FAILURE OF ANY PRODUCT ACQUIRED BY BUYER FROM BT.

All claims for shortages, defects, and non-conforming goods must be made by the customer in writing within five (5) days of receipt of merchandise, which writing shall state with particularity all material facts concerning the claim then known to the customer. Upon any such claim, the customer shall hold the goods complained of intact and duly protected, for a period of up to sixty (60) days. Upon the request of BT, the customer shall ship such allegedly non-conforming or defective goods, freight prepaid to BT for examination by BT's inspection department and verification of the defect. BT, at its option, will either repair, replace or issue a credit for products determined to be defective. BT's liability and responsibility for defective products is specifically limited to the defective item or to credit towards the original billing. All such replacements by BT shall be made free of charge f.o.b. the delivery point called for in the original order. Products for which replacement has been made under the provisions of this clause shall become the property of BT. Under no circumstances are products to be returned to BT without BT's prior written authorization. BT reserves the right to scrap any unauthorized returns on a no-credit basis. Any actions for breach of a contract of sale between BT and a customer must be commenced by the customer within thirteen (13) months after the cause of action has accrued. A copy of BT's standard terms and conditions of sale, including the limited warranty, is available from BT upon request. Copies of the limited warranties covering third-party proprietary sub-assembly modules and private-label products manufactured by third-parties are also available from BT on request. DigiCipher ® is a registered trademark of Motorola Corp. (**Rev 0509)**

BLONDER TONGUE LABORATORIES, INC.

One Jake Brown Road
Old Bridge, NJ 08857-1000 USA
(800) 523-6049 • (732) 679-4000 • FAX: (732) 679-4353
www.blondertongue.com