


HomePlug® AV
200Mbps PHY

USER'S GUIDE

# Intellon HomePlug® AV

## AVitar User's Guide v4.1

## Table of Contents

**1. INTRODUCTION ..... 3**

**2. INTELLON HOMEPLUG AV AVITAR APPLICATION OVERVIEW ..... 3**

2.1 AVitar and Application Programming Interface ..... 3
2.2 AVitar GUI Tabbed Windows ..... 4
2.3 AVitar Functions ..... 4

**3. AVITAR USE ..... 5**

3.1 AVitar Installation ..... 5
3.2 Common Features of Tabbed Windows ..... 6
*3.2.1 Network Interface Cards (NIC) Selector ..... 6*
3.3 Configuration Tab *(Configuration Window)* ..... 7
*3.3.1 Configuration Fields ..... 7*
*3.3.2 Prescaler File Selection ..... 8*
*3.3.3 Device Personalization Information ..... 8*
*3.3.4 Configuration Checkboxes ..... 9*
3.4 Link Information Tab *(Operation Analysis Window)* ..... 12
*3.4.1 Link Characteristics Box ..... 12*
*3.4.2 Ethernet Controls ..... 12*
*3.4.3 Control and Statistics Groups ..... 13*
3.5 QoS Tab *(Configuration Window)* ..... 14
*3.5.1 Priority Mapping and Priority Thresholds ..... 15*
*3.5.2 Default CAP ..... 16*
*3.5.3 Internet Group Management Protocol (IGMP) Timers ..... 16*
*3.5.4 Time To Live (TTL) Value in MME ..... 16*
3.6 Debug Message Viewer *(Operation Analysis Window)* ..... 17
3.7 Network Information Tab *(Operation Analysis Window)* ..... 18
*3.7.1 Central Coordinator (CCo) Information ..... 18*
*3.7.2 Selected Station (STA) Information ..... 18*
*3.7.3 Topology ..... 18*
3.8 Interface Configuration Tab *(Configuration Window)* ..... 20
*3.8.1 Override Defaults Checkbox ..... 20*
*3.8.2 Flow Control Box ..... 20*
*3.8.3 Host Traffic Metering ..... 20*
*3.8.4 PHY Address Selection ..... 21*
*3.8.5 Low Power Mode Features Configuration ..... 21*
*3.8.6 Bandwidth Limiting ..... 22*
*3.8.7 Multiport Switch ..... 23*
3.9 Encryption Configuration Tab *(Configuration Window)* ..... 24
*3.9.1 Default ..... 24*
*3.9.2 Enhanced ..... 24*
*3.9.3 Custom ..... 24*
*3.9.4 ALVN Membership Mask ..... 25*
*3.9.5 Exit Default ..... 25*
*3.9.6 Reject Default ..... 25*
*3.9.7 Chaining ..... 25*

3.10 CONNECTION INFORMATION TAB *(OPERATION ANALYSIS WINDOW)* ..... 26
*3.10.1 Connection Select* ..... *26*
*3.10.2 Transmission and Reception Statistics* ..... *27*
3.11 BRIDGE INFORMATION *(OPERATION ANALYSIS WINDOW)* ..... 28
*3.11.1 Select Station* ..... *28*
3.12 ENCRYPTION TAB *(CONFIGURATION WINDOW)* ..... 29
3.13 DIAGNOSTICS TAB *(EVENT LOG)* ..... 30
*3.13.1 Three Sub-tabs* ..... *30*
3.14 LED MANAGER TAB *(CONFIGURATION WINDOW)* ..... 31
*3.14.1 GPIO Configuration* ..... *31*
*3.14.2 Event Behavior Map* ..... *33*
*3.14.3 LED Behavior Wizard* ..... *34*
*3.14.4 LED Event-Behavior Map* ..... *35*
3.15 MULTI-MASTER ISOLATION TAB *(CONFIGURATION WINDOW)* ..... 36
*3.15.1 Currently Non-MDU* ..... *36*
*3.15.2 Currently MDU Master* ..... *37*
*3.15.3 Currently MDU Slave* ..... *38*

**4. REVISION HISTORY ..... 39**

**APPENDIX A: INT6X00 AMPLITUDE MAP MODIFICATION ..... 40**

**APPENDIX B: ACRONYMS AND ABBREVIATIONS ..... 41**

# 1. Introduction

This AVitar User's Guide is provided to assist users in understanding and using the AVitar software as a tool in configuring and testing Intellon ICs running HomePlug AV firmware  Included in this document is a description of the AVitar's capabilities and discussions of each tabbed window of the AVitar's Graphical User Interface (GUI). This user guide will be updated concurrently with iterations of the AVitar software.

For your reference:

Appendix A discusses amplitude map modification.

Appendix B contains a list of acronyms and abbreviations used throughout this document.

# 2. Intellon HomePlug AV AVitar Application Overview

## 2.1 AVitar and Application Programming Interface

The Intellon HomePlug AV AVitar is a Windows application that serves as an interface between a human operator or another application and Intellon HomePlug AV ICs. It provides a Graphical User Interface (GUI) to a set of Application Programming Interfaces (APIs) that manipulate the Parameter Information Block (PIB) and exercise the set of Management Message Entries (MMEs) required to send and receive the necessary or desired information. MMEs are used for station-to-station control communication and, particularly in this control context, are also used for control messages to and from the AVitar application, which is functioning as a Higher Layer Entity (HLE). The AVitar enables the user to perform configuration functions, such as update runtime firmware, view and/or modify various static and runtime parameters, and conduct operation analysis to display performance and network statistics.

As illustrated in Figure 1, the AVitar includes both the PIB API and the Control API, which function as the PIB Manager and MME Generator/Parser respectively. The PIB is a file which is used to input parameters to some of the Control API operations. The Intellon-provided API code can be embedded in an application to operate under a custom host/GUI that utilizes a select set of API functions, MMEs and PIB data.

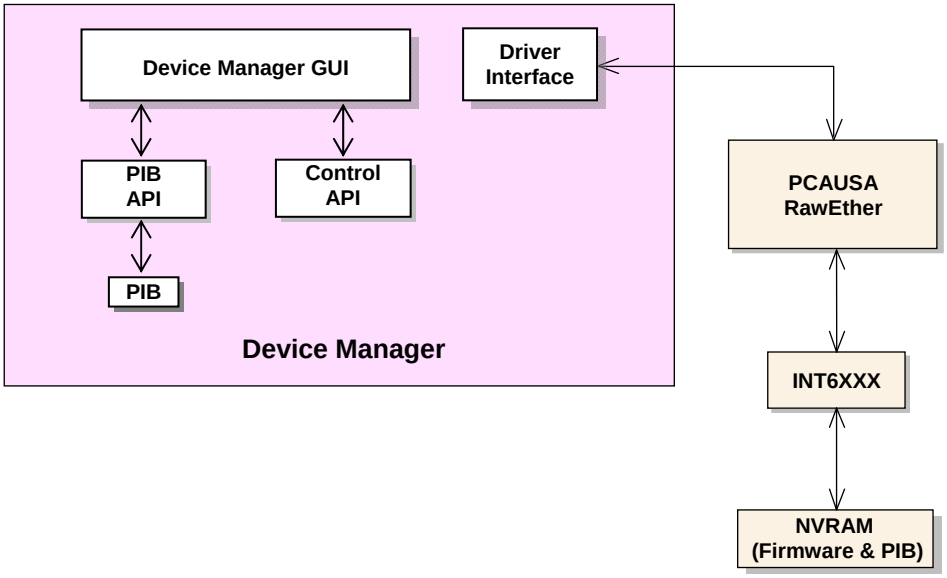



**Figure 1: Intellon HomePlug AV AVitar Blocks**

The AVitar Graphical User Interface (GUI) application is an example of how the APIs can be utilized. The GUI application uses both Application Programming Interfaces for device configuration and testing. This eliminates the need to engage in low-level programming, saving time, money and effort.

The PIB API functions as a PIB manager which manages a file containing PIB parameters. Through the API/PIB Manager, these parameters can be modified. The PIB file is a temporary storage area in which to perform modifications. Via the

AVitar Control API, the modified PIB file contents can then be loaded to the NVRAM using the Write Module operation. The AVitar can also copy the PIB in the NVRAM to the temporary PIB file for modification by using the AVitar Control API Read Module operation. The PIB and the Firmware may be selected for update at the same time.

The Control API is used to process requests to and responses from HomePlug AV ICs. Operations include: uploading and downloading PIB information, uploading and downloading MAC firmware, gathering operation statistics information and stream setup and teardown. In the above AVitar application, the third-party PCAUSA RawEther components are used to allow transmission and reception of raw Ethernet frames in the Windows OS environments.

Designers who wish to build their own Windows-based software application utilizing one or both the APIs described above will require additional software to handle the transmission and reception of raw Ethernet frames. This software can be developed internally or purchased from a third party source, such as PCAUSA. This code must be licensed directly from PCAUSA. Ordering information is online at: http://www.rawether.net/oem/intellon/
Part Number: SKU 008-003 – RawEther for Windows SDK – Intellon OEM Version

## 2.2 AVitar GUI Tabbed Windows

The AVitar uses logically organized tabbed windows and clearly labeled groups and fields to provide easy access to parameters and operation statistics. *Note that these tabbed windows may change with version updates.*

The AVitar GUI application windows are classified in three basic groups: Configuration, Operation Analysis and Event Log Management.

## 2.3 AVitar Functions

Figure 2 shows the Configuration, Operation Analysis, and Event Log management functions of the DM. These functions are executed via the buttons and fields of the three AVitar GUI tabbed windows.

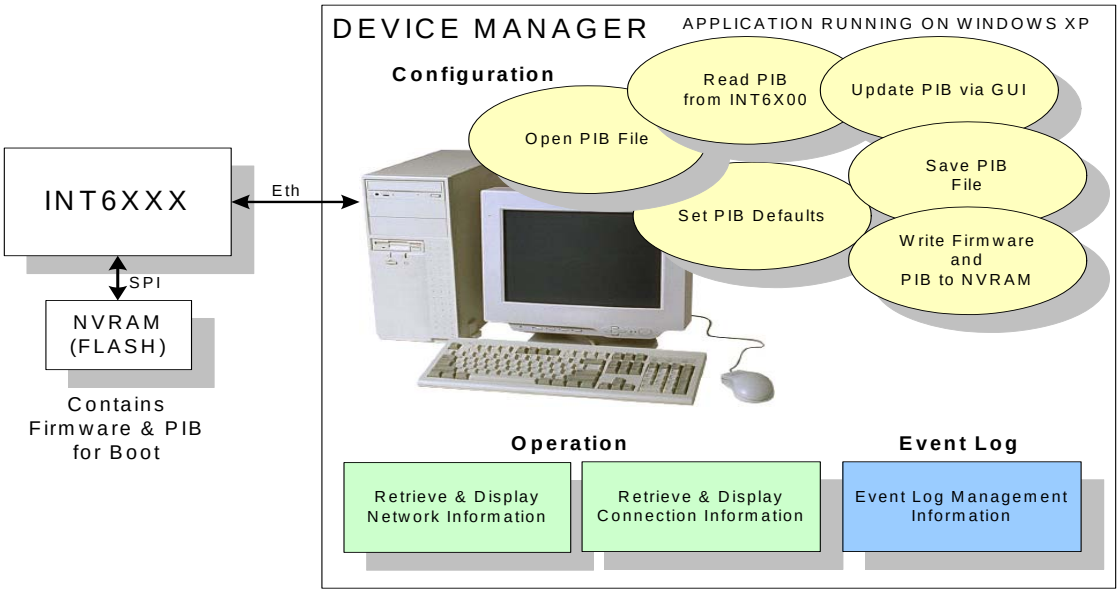



**Figure 2: Intellon HomePlug AV AVitar Functions**

The AVitar is used to modify firmware and variable values that reside in the external non-volatile flash memory (NVRAM). In a typical configuration, HomePlug AV ICs may boot from this NVRAM at startup, receiving operating instructions and parameters. The Parameter Information Block (PIB), residing in the NVRAM, contains variable values that are used to configure the operation of the chip. PIB variables are mapped to the fields of the tabbed GUI windows, enabling easy value inspection and modification.

*Note: Additional functionality may be added to the AVitar in future releases.*

# 3. AVitar Use

## 3.1 AVitar Installation

The following describes the installation of the AVitar software.

1. The user installing the AVitar software must have administrative rights on the PC.
2. AVitar software runs on Windows XP or Vista 32-bit only. Vista 64-bit is not supported.
3. A network card must be installed and enabled before continuing.
4. Locate the AVitar Software folder on the Intellon Customer FTP site.
5. Download and unzip the AVitar software.
6. Note the following files:
    - avitar.exe
    - Installer.bat
7. Execute Installer.bat; various files will be copied to appropriate system directories.
8. Launch the AVitar by double clicking on avitar.exe. If it fails to launch, the probable cause is that .NET 1.1 redistributable is not installed. .NET Framework 1.1 Redistributable is freely downloadable from: http://www.microsoft.com/downloads/results.aspx?pocId=&freetext=.NET+redistributable&DisplayLang=en
9. The installation is now complete.

NOTE: To install AVitar on machines with Windows Vista 32-bit only, the user must have administrator privileges and User Account Control (UAC) disabled see Figure 3 below.

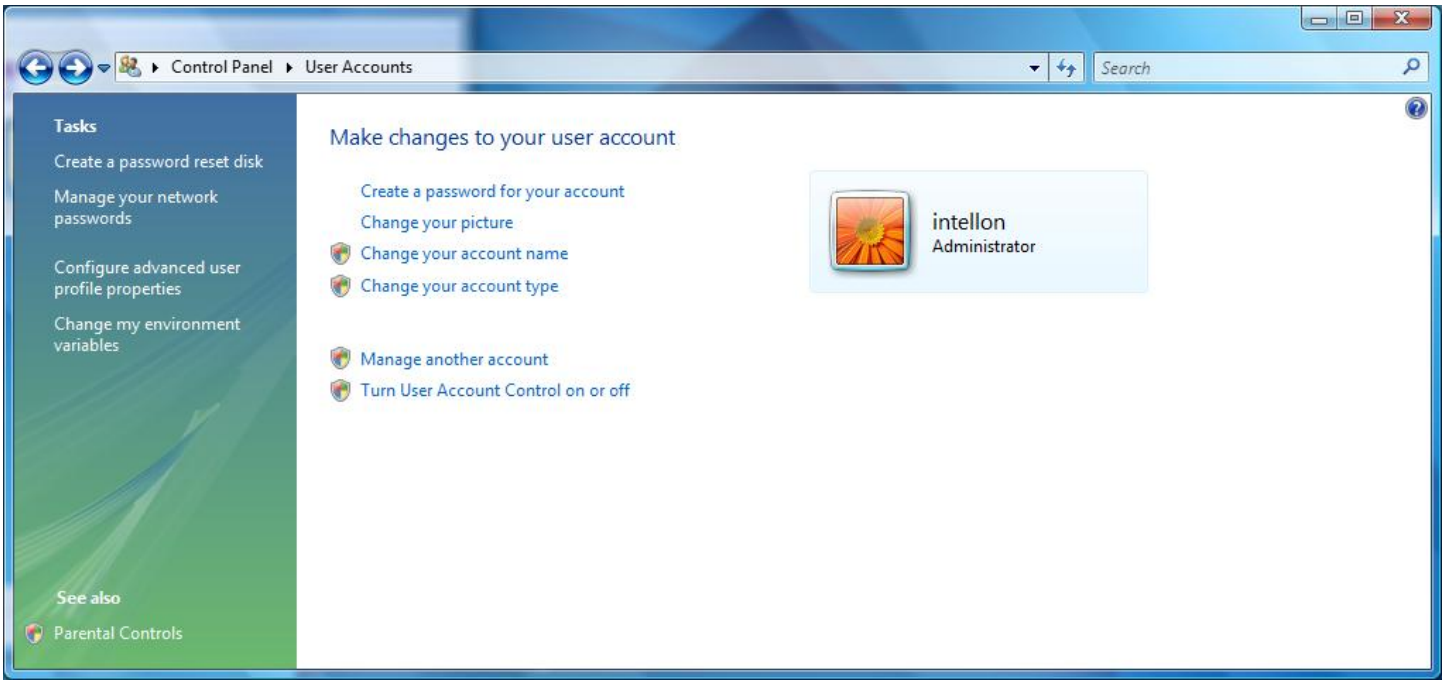



**Figure 3: Disable User Account Control**

## 3.2 Common Features of Tabbed Windows

### 3.2.1 Network Interface Cards (NIC) Selector

As shown in Figure 4, the lower left (with red outline) of the panel provides for selection of Network Interface Cards and connected devices. The name of the network cards are displayed in the network interface drop-down.

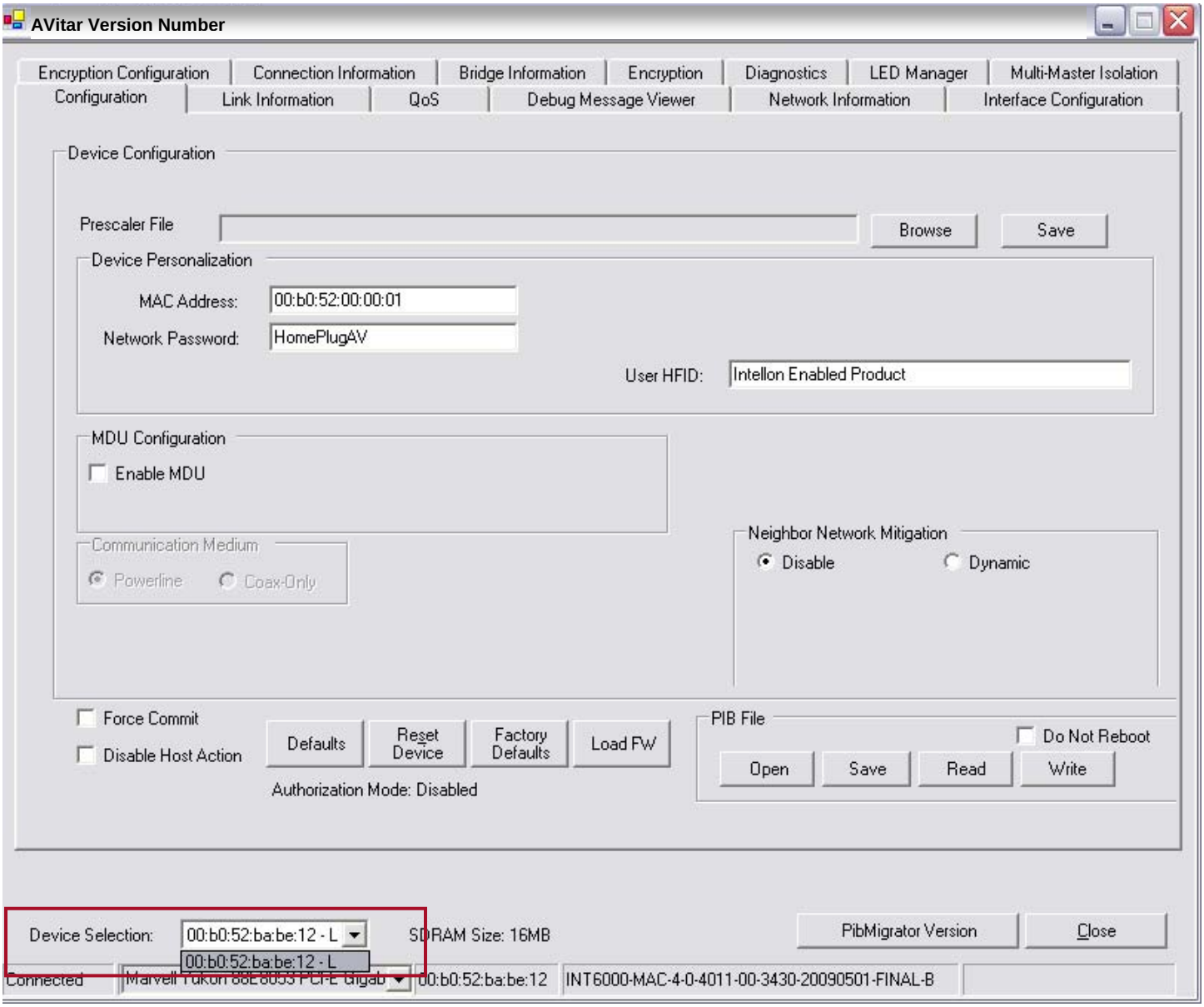



**Figure 4: Viewing and Selecting a Network Interface Card**

## 3.3 Configuration Tab *(Configuration Window)*

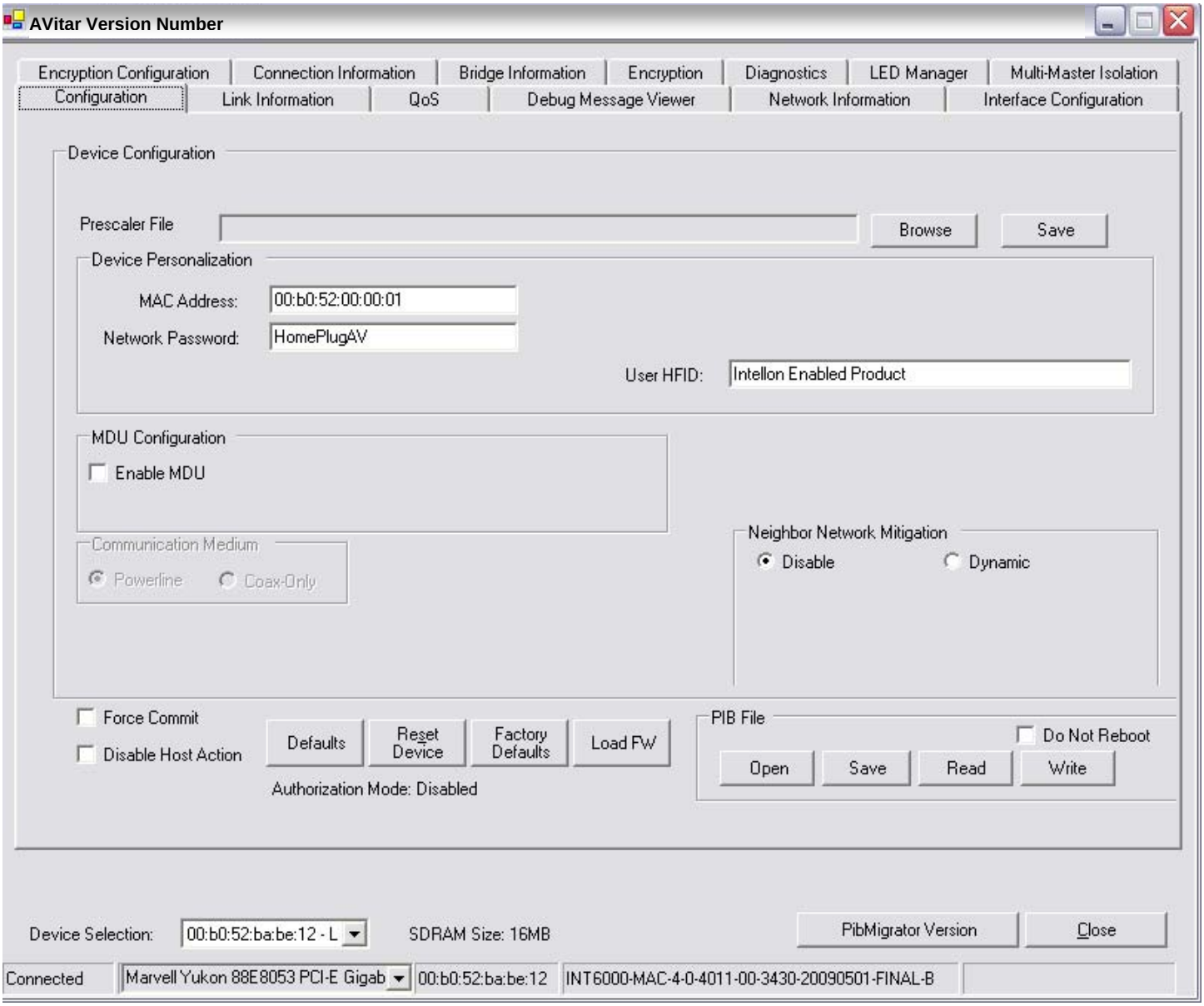



**Figure 5: Configuration Tab Window**

### 3.3.1 Configuration Fields

The AVitar GUI tabbed window labeled 'Configuration' is shown in Figure 5. Areas available for configuration using this window include:

- File Selection: Prescaler files
- Device Personalization Information
  - MAC Address
  - Network Password
  - User HFID
- MDU Configuration Checkboxes
  - Enable MDU: Master or Slave radial buttons
  - Communication Medium: Powerline or Coax-Only radial buttons
- Connected Device Identification

- PibMigration Version Reports PIB migration version.

Fields provided on this window, in the areas listed above, allow updating or changing of PIB variables values. These changes are made to the locally stored (the PIB image in the DM's memory) PIB and are not loaded to the NVRAM until the Write PIB Function is selected.

*Note: The AVitar and the firmware contain code that interprets the values of the PIB. See below. This shared PIB management code has a version number, as does the firmware file, and the firmware (SW version). The version codes must match for update (Write) to occur successfully.*

***To upgrade a remote device, both the PIB and the MAC firmware should be updated at the same time. It is very important to follow this step as failure to do so will result in the device being forced into an isolated network.***

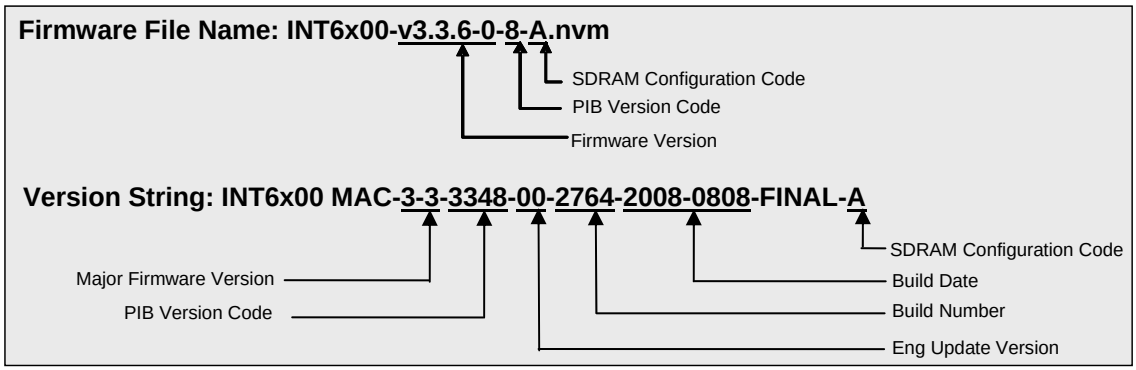



**Figure 6: Firmware and Version Strings**

To enable download of the PIB to a device, the AVitar will compare the connected device's SW version information to those compatible with the DM's version of the PIB management code. Valid combinations will allow the Write functionality to download and commit the PIB to NVRAM. Invalid combinations will be reported to the user upon pressing the Write button and the write operation will be cancelled.

### 3.3.2 Prescaler File Selection

Browse buttons are used to locate the Prescaler files.

### 3.3.3 Device Personalization Information

The Personalization Information area of the Configuration Tab window allows the configuration of: MAC Address, Network Password, User HFID, MDU Master or Slave.

The 'User HFID' text box allows the user to create and manage a Human Friendly Identifier (HFID) of up to 64 characters.

The MDU Configuration is used to enable and specify the special MDU functionality. Checking the "Enable MDU" checkbox will expose the 'Master' and 'Slave' radio buttons, providing a toggle choice. This enables the user to configure the CCo as a Master and all STAs as slaves, Slaves can no longer communicate with each other; they can only communicate with the Master. This function must be deliberately enabled by checking the Enable MDU box.

#### 3.3.3.1 Managing MAC Addresses

The MAC Address is a writable entity. To write it, you must be working with a PIB that matches the DM's version of the PIB. The upgrade process will preserve the running MAC address, so modifying the address is generally not needed.

Running in a flash-less environment is an exception. When prompted for the PIB with the 'Bootloader' a non-default MAC address must be accessible. The address is accomplished with either a non-default MAC address in the selected PIB, or a non-default MAC address in the exposed MAC address field.

Downloading firmware now requires an accompanying PIB.

***WARNING:*** *If new firmware encounters an unacceptable PIB upon coming out of reset, the MAC Address status bar will display (00:b0:52:00:00:03). This creates an unrecoverable scenario.*

**NOTE:** The recommended procedure for upgrading firmware is to use the *Load FW* button. This procedure will automatically first read the running PIB and save the existing MAC address. The user will be prompted for a selection of PIB and firmware which will be down loaded to the device including the correct MAC address. Status of the transfer and commit stages of the procedure are provided in the status bar on the lower right of the form.

### 3.3.4 Configuration Checkboxes

#### 3.3.4.1 Force Commit

The user should check this box when they want to force writing the firmware and or PIB to flash in the scenario where the firmware was started from the Bootloader.

#### 3.3.4.2 Disable Host Action Checkbox

This provides the user with the option to disable the DM's responsive functionality with respect to the Host Action Indications received from the Bootloader or Softloader. See following description of the Host Action Indication behavior.

**Host Action Indication Functionality**
The Host Action Indication functionality is associated with an unsolicited Host Action MME which is sent to the host from the FW. When the *Disable Host Action* checkbox is not selected, the AVitar will react to the reception of these messages.

* In a flash-less environment, the ROM-based Bootloader will respond to the AVitar's discovery process. The AVitar will form a connection with the device evidenced with the default MAC address (00:b0:52:00:00:01) and the appearance of *Bootloader* in the version string textbox found at the bottom middle of the form.

The Bootloader will periodically send Host Action Indications to the AVitar based on its state. Initially, the Bootloader will ask for SDRAM configuration. Based on the user's selection of the SDRAM size, which is chosen with the new *SDRAM Size* drop-down, one of two SDRAM configuration files will be downloaded to the Bootloader. This will happen automatically, evidenced by "SDRAM Config updated" message in the bottom right status box. The two configuration files, each associated with 16M or 64M SDRAM sizes are provided by Intellon and are part of the AVitar installation package. They are co-located with the bundle of AVitar files placed in the location chosen during installation. If these files are lost, removed, or otherwise not found in the native directory, a browse window will pop up to for the user to select the desired file.

Subsequent to downloading SDRAM configuration, the Bootloader will request loader information. A browse window for the PIB will first appear. The selected PIB will undergo some validation and be downloaded to the device, evidenced with a PIB update successful status message.

***WARNING:*** *selection of a PIB containing a default MAC address (00:b0:52:00:00:01), will be invalidated and abort the existing session. A new session will be invoked with the reception of a subsequent Host Action request for loader information as part of the periodic behavior.*

The AVitar will next prompt the user with a browse window to select firmware. The selected firmware file will be downloaded as evidenced with a "Downloading firmware" status message and subsequent "Update firmware successful" status message, if successful.

The new firmware will be started, the PIB installed and the version string text box should indicate that the firmware is running with the MAC address provided in the PIB.

Downloading a new PIB or firmware image to the running firmware will stimulate a Host Action request to read one or both modules. In general, the host makes no assumptions regarding the source of the updates, even if the source is itself. The AVitar will read the PIB and or firmware from the device and reset the device. When the device comes out of reset, the Bootloader will repeat its startup procedure. This time, the AVitar will provide the newly read information and prompt the user for missing pieces. When the firmware is started and the PIB is installed, the changes will take effect.

#### 3.3.4.3 Neighbor Network Mitigation

This feature will allow multiple AVLNs to operate at full bandwidth when they are co-located.

- **Disable:** Run at default output power and correlation threshold.
- **Dynamic:** Iterative algorithm which adjusts the Output Power and Correlation Threshold values automatically until the beckons of the neighboring AVLNs are not longer detected.
  *Notes: may take up to 17 minutes for the algorithm to converge, additionally these values are not stored to flash. Subsequent reboots will restart the algorithm*

#### 3.3.4.4 Device Action Buttons

- **Defaults:** Loads default PIB values into AVitar's current working PIB.
- **Reset Device:** Clicking on this button will force a device reset.
- **Factory Defaults:** Clicking on this button will restore the factory defaults.
- **Load FW:** This button provides the user with an option to download firmware to upgrade or downgrade across PIB and FW versions. See following description of the Upgrade behavior. The upgrade functionality provides the user with a simple means to migrate back and forth between firmware versions. Clicking on the *Load FW* button will first read the PIB running on the device. An abbreviated set of personality attributes will be retained which includes: MAC address, NMK, and DAK. The user is prompted to select a new PIB with the appearance of a browse window. The selected PIB will be modified with the retained personality information, previously read from the running device. The user must next select the new firmware with the appearance of a browse window. The selected PIB will establish a version for which this selected firmware must match in terms of PIB compatibility.
- **Authorization Mode:** Indicates if Selected Upgrade feature is enabled. Selective Upgrade feature to be included in future firmware release.

  *Warning – configuration information exclusive of the abbreviated set of personality information will not migrate to the new PIB.*

  The new PIB and firmware will be downloaded to the device and committed. The device will reset and the new firmware should start running as evidenced by the version string textbox at the bottom center of the form.

#### 3.3.4.5 PIB File Group Box

- **Open**: (PIB File group) Clicking on this button opens the PIB file and displays its variable values so they can be examined and modified. Clicking on the Open button causes a File Open dialog to appear. After a file is selected, that file is opened, validated for conformance with the AVitar's format and all PIB variables in the window are set accordingly.
- **Save**: (PIB File group) Clicking on this button saves the modified PIB file. Clicking the Save button causes a File Save dialog to appear and will save a copy of the PIB to the user determined file location with the appropriate file type extension.
- **Read**: (Device Configuration group) Clicking on this button executes a read operation of the PIB data existing in the chipset. If the PIB contents from the CHIPSET are invalid (non-existent or the PIB version does not match the runtime version), an appropriate PIB Contents MME is returned. Based on the returned status, the AVitar will either perform the Set PIB Defaults action or indicate the version mismatch to the user for subsequent MAC FW download. If the PIB Contents MME is valid, all fields are updated on the appropriate tabbed windows of the DM.
- **Write**: (Device Configuration group) Clicking on this button executes a write operation of the PIB data and the firmware, in case the 'Download MAC Firmware' ***and 'Download PIB file'*** check box is checked, to the NVRAM (Flash RAM external to the CHIPSET). Clicking the Write button causes the existing values contained in the PIB to be sent to the NVRAM using the Download MMEs. Checksums are used to validate the integrity of the download process. Following download and receipt of an NVRAM Update Complete MME from the CHIPSET, an appropriate message is displayed to indicate success or failure. The contents of the Image File are downloaded to the NVRAM along with the contents of the PIB.
- **Do Not Reboot Checkbox**: Invokes flash background writes. Flash writes are executed in background and device continues to operate uninterrupted. Future flash writes are blocked while there are pending background writes.

#### 3.3.4.6 PIB Migration Utility

The PIB Migration Utility is a new feature that allows users to easily update from an older PIB version to the newest version of PIB. The PIB Migration Utility is automatically launched from AVitar when upgrading an adapter's FW. This allows AVitar to interoperate between FW revisions. Optionally it can be called as a standalone command line utility. With this utility, the user will be able to migrate easily between PIB and FW versions. The new copy of the migrated PIB will be created in a user-selected location under a user-selected file name.

The PIB Migration Utility can be run as a free-standing utility and also can be executed from within the AVitar. The utility will handle the migration of older PIBs (from v2.0) to the latest PIB version. The utility saves the new PIB in a separate PIB file by adding a suffix to the original file name. The original PIB file will be preserved.

In future releases, the source code will support an ANSI subset of the language used so that it can be compiled and built for Windows and Linux.

The PIB Migration Utility cannot be used to downgrade the PIB from a newer (higher) version of the PIB to an older (lower) version. The utility assumes that PIB of older releases shall not be modified.

## 3.4 Link Information Tab *(Operation Analysis Window)*

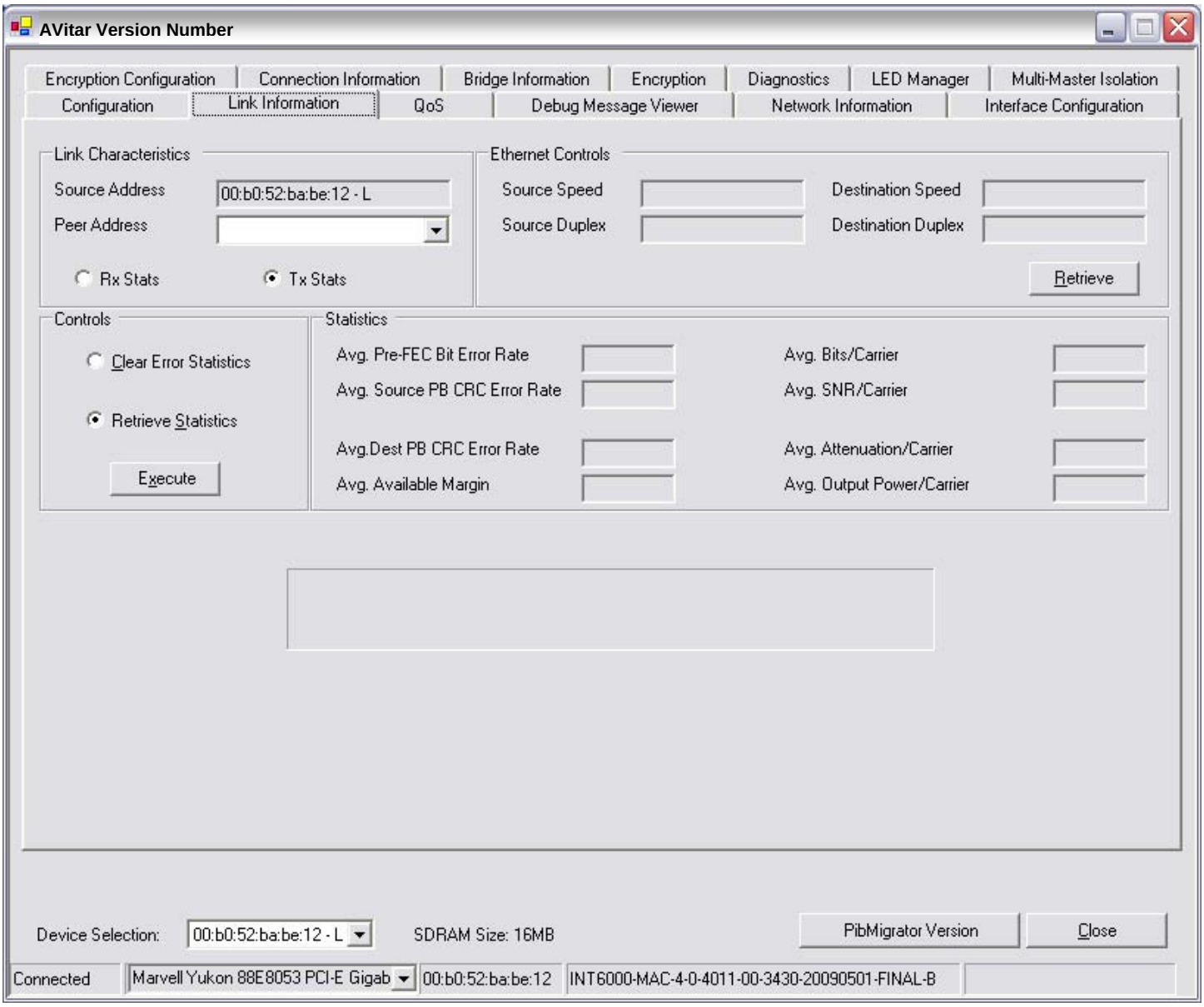



**Figure 7: Link Information Tab Window**

### 3.4.1 Link Characteristics Box

The context of the link is identified with the Source and Peer Address boxes in the Link Characteristics group box. The Source Address defaults to the address of the device selected in the Device Selection box on the lower left of the tab and the Peer Address is selected from a drop-down list.

Receive (Rx) versus transmit (Tx) statistics is controlled with the two radio buttons found in the Link Characteristics group box.

### 3.4.2 Ethernet Controls

The Ethernet Controls are populated once the Retrieve button is pushed and indicate the PHY settings of both ends of the link.

### 3.4.3 Control and Statistics Groups

The members of the Statistics group are populated or cleared based on the radio button selection in the Controls group and the pressing of the Execute button. The lower status window provides feedback regarding the processing of the activity.

'Avg. Available Margin', in the Statistics group box, only has relevance in the receive context.

## 3.5 QoS Tab *(Configuration Window)*

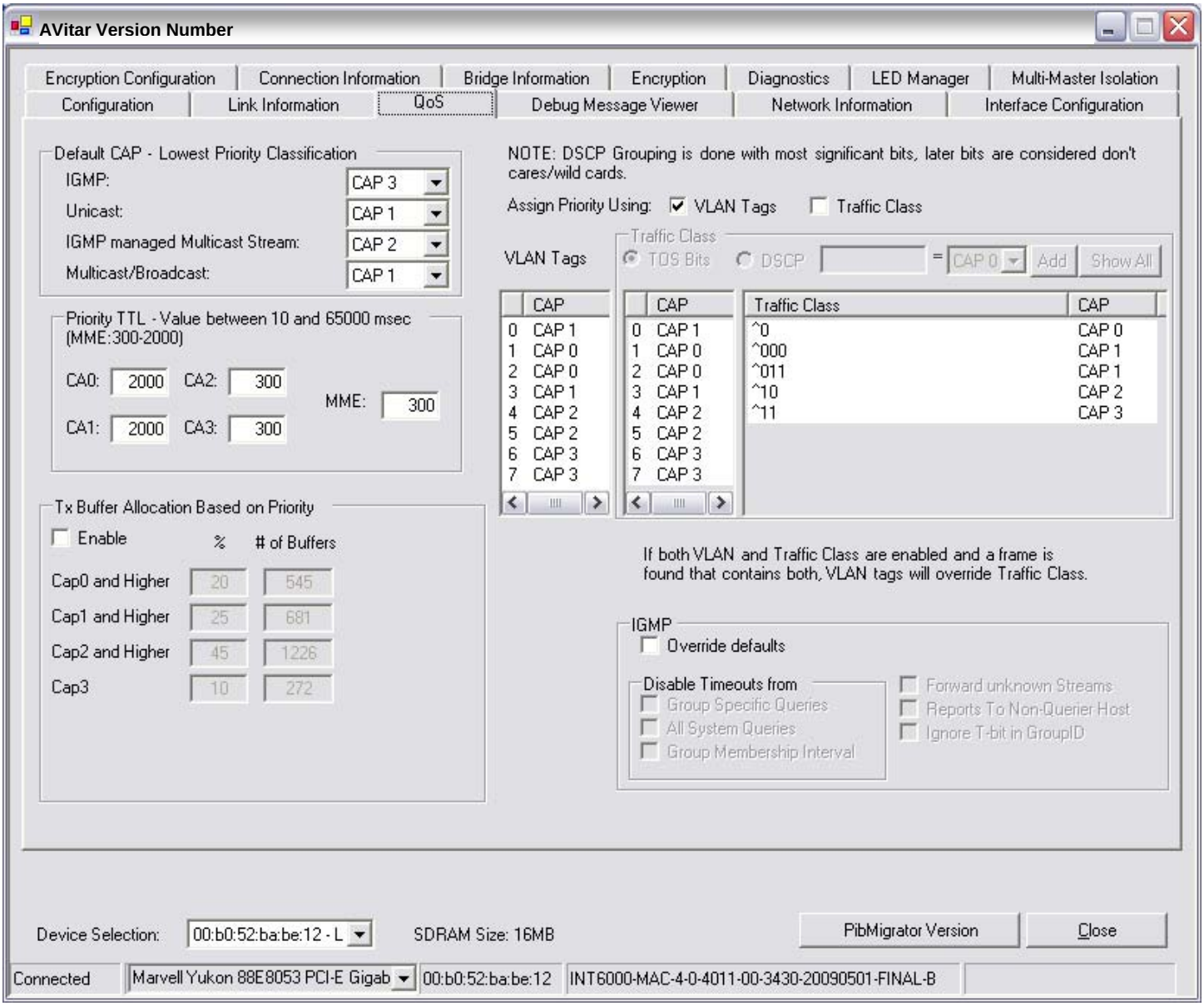



**Figure 8: QoS Tab Window**

QoS requirements are different for various data types such as streaming video or music, voice and raw data. To provide higher QoS for streaming data, priority levels can be set using tags at the beginning of data frames. Virtual Local Area Network (VLAN) 802.1p priority tags on Ethernet frames are used to specify 8 (0 – 7) levels of 'user priority'. HomePlug AV powerline allows for 4 levels of Channel Access Priority (CAP (0 – 3)). Therefore, the 8 levels of VLAN Ethernet tags must be mapped to the 4 levels of CAP priority, where CAP 3 is the highest priority and CAP 0 is the lowest. CAP 3 priority might be used for voice and network management frames, CAP 2 is used for streaming video and music while CAP 1 and CAP 0 are used for data. Mapping VLAN tags or TOS bits to CAP levels is easily done using the VLAN Priority Mapping function on the QoS tab window.

### 3.5.1 Priority Mapping and Priority Thresholds

Mapping includes VLAN, TOS and DSCP.

The 'Traffic Class' group presents the option to map Channel Access Priority (CAP) to the classic Internet Protocol (IP)Type of Service (TOS) bits or the new Differentiated Services Code Point (DSCP) values. These configuration elements are conveyed in the PIB and must be written or saved to preserve them. Checking the '*Traffic Class*' checkbox will enable the 'Traffic Class' TOS Bits column.

TOS and DSCP mapping is mutually exclusive, controlled with the radio buttons.

#### 3.5.1.1 DSCP Mapping

The DSCP mappings contain a full set of all combinations of 8 bits or 256 individual mappings. The management of the DSCP mappings can be configured individually and offers a grouping facility to simplify and condense the presentation. The rightmost button toggles between '*Group*' and '*Show All*' for these modes.

The grouping algorithm will bundle sets identified by common leading bit values, having the same mapping. More specific entries, i.e. having a longer set of common leading bit values may appear after a less specific entry in the group list. In so doing, the more specific entries override the mapping found in the less specific entry above.

Mapping entries are added by keying in a set of leading bit values in the textbox found to the right of the '*DSCP*' radio button. Map a CAP selection with the dropdown box found to the right of the '=' sign - then press the '*Add*' button. The regular expression '^' (carrot) symbol can optionally be used to start the set of leading bit values as shown in Figure 8.

Mapping entries are deleted by adding a less specific entry. This action highlights the importance of the sequence in which entries are added. Re-adding a *less* specific entry which appears above one or several *more* entries will delete all the more specific entries.

#### 3.5.1.2 Priority Thresholds

The Priority Threshold feature (Tx Buffer Allocation Based on Priority) allows the specification of priority queue thresholds, also called buffer high water marks, in order to control the sharing of buffers between the traffic classes. The buffer space is managed according to the specified percentages for CAP 0, CAP 1, CAP 2 and CAP 3. The threshold test is performed immediately after a frame is classified. An example will be helpful to explain how the algorithm allocates memory and manages frames being queued for transmit.

- The buffer memory is divided into three segments (controlled by different parameters) as follows:
  1. Memory reserved exclusively for receive (TotalRxRAM) – default is 20%
  2. Memory reserved exclusively for transmit (TotalTxRAM) – default is 15%
  3. Memory shared between both transmit and receive (TotalFreeRAM)
- Total free memory for transmit is calculated as TotalTxRAM + TotalFreeRAM
- For the example, assume the total free memory for transmit yields 1000 buffers
- The memory is allocated as follows using the priority threshold parameters:
  1. CAP 0 and higher = 40%
  2. CAP 1 and higher = 30%
  3. CAP 2 and higher = 20%
  4. CAP 3 = 10%

Converting these percentages into number of buffers yields the following:

1. CAP 0 and higher = 400
2. CAP 1 and higher = 300
3. CAP 2 and higher = 200
4. CAP 3 = 100

From the above numbers, if the TotalTxRAM used is less than 400, CAP 0 will get through. If the TotalTxRAM used is greater than 400, even if CAP 0 is not using all of these 400 buffers, CAP 0 will not get through. Continuing, CAP 1 will get through if less than 700 buffers and used, and so on. The numbers generated by the amount of free RAM and the assigned percentages guarantee that lower priority frames will be dropped if the amount of used RAM reaches the sum of allocated buffers for the lower priorities.

### 3.5.2 Default CAP

The 'Default CAP' group allows for default priority mapping of packets that do not have a VLAN TAG (or have VLAN and TOS disabled). Settings are available for Unicast (directed to a host).

- IGMP - (default CAP 3) - sets the channel access priority for IGMP frames - these are the group management frames, not the stream data
- Unicast - (default CAP 1) - sets the default channel access priority for Unicast frames not matching any other classification or mapping.
- IGMP managed Multicast Stream (Fixed to CAP 2) - sets the default channel access priority for stream data belonging to a snooped IGMP multicast group.
- Multicast/Broadcast - sets the default CAP for multicast frames not in a snooped group and for broadcast frames.

After making CAP settings, clicking the Write button will commit these, along with the values from the Configuration tab, to NVRAM on the connected device.

### 3.5.3 Internet Group Management Protocol (IGMP) Timers

IGMP group tables are built by snooping IGMP report/join messages that traverse the network. In order to age out groups that are not in use, the maximum query timer (125 seconds * 2 default robustness) plus the maximum report expected time in the Query message (10 seconds default) is used (260 seconds). Routers can generate "Group Specific" or "All Systems" queries. The 'IGMP' group includes controls to disable aging through the query timeouts. Checking the 'Override Defaults' box enables the user to disable the aging of the multicast groups by checking the appropriate disable mechanism. When "Group Specific query" is checked, the specific multicast group will not be aged out from the table through the time value for that group. When "All Systems query" is checked, then the time value will not be applied to all groups in the table for aging. When "Group Membership Interval" is checked, then the timer value for any station's response to a query in a given group will be disabled – i.e. the stream to that station will continue indefinitely.

### 3.5.4 Time To Live (TTL) Value in MME

The 'TTL Value' determines the maximum life span (Time To Live) of each packet in the buffer of the AV device that will be sent over the powerline subsequently. This value can be varied from 10 msec to 65,000 msec which can be mapped to different levels of Channel Access priority traffic. The default values used are stored in the PIB file as shown below:

| | | |
|---|---|---|
| CA0 traffic: | 2000 msec | (used for TCP data traffic) |
| CA1 traffic: | 2000 msec | (used for TCP data traffic) |
| CA2 traffic: | 300 msec | (used for UDP video/music traffic) |
| CA3 traffic: | 300 msec | (used for VoIP traffic) |
| MME traffic: | 300 msec | (used for HomePlug and Intellon Vendor Specific MMEs) |

Intellon highly recommends that the 300 msec and 2,000 msec default settings not be changed because they are optimized for the above stated traffic. Intellon highly recommends that the TTL value for MME be left at 300 msec. Under high traffic conditions, there is a low probability that an MME might not get transmitted due to collisions on the wire. Under these conditions, increasing the TTL to its maximum of 2,000 msec may resolve this. However, given that MMEs are always transmitted at the highest priority resolution slot, this condition will most likely not be encountered.

### 3.5.6 Priority Hierarchy

The device allows for multiple concurrent priority selections. Table below shows order of the priority that would be used in case there are multiple priority selections.

| Unicast Packets | Multicast Packets |
|---|---|
| IP Port | IP Port |
| MAC Address | VLAN |
| VLAN | TOS |
| TOS | |

This means that if IP Port 2525 is assigned to CAP 2, then all other settings for that packet is ignored and that packet is assigned a CAP2 priority for transmission.

## 3.6 Debug Message Viewer *(Operation Analysis Window)*

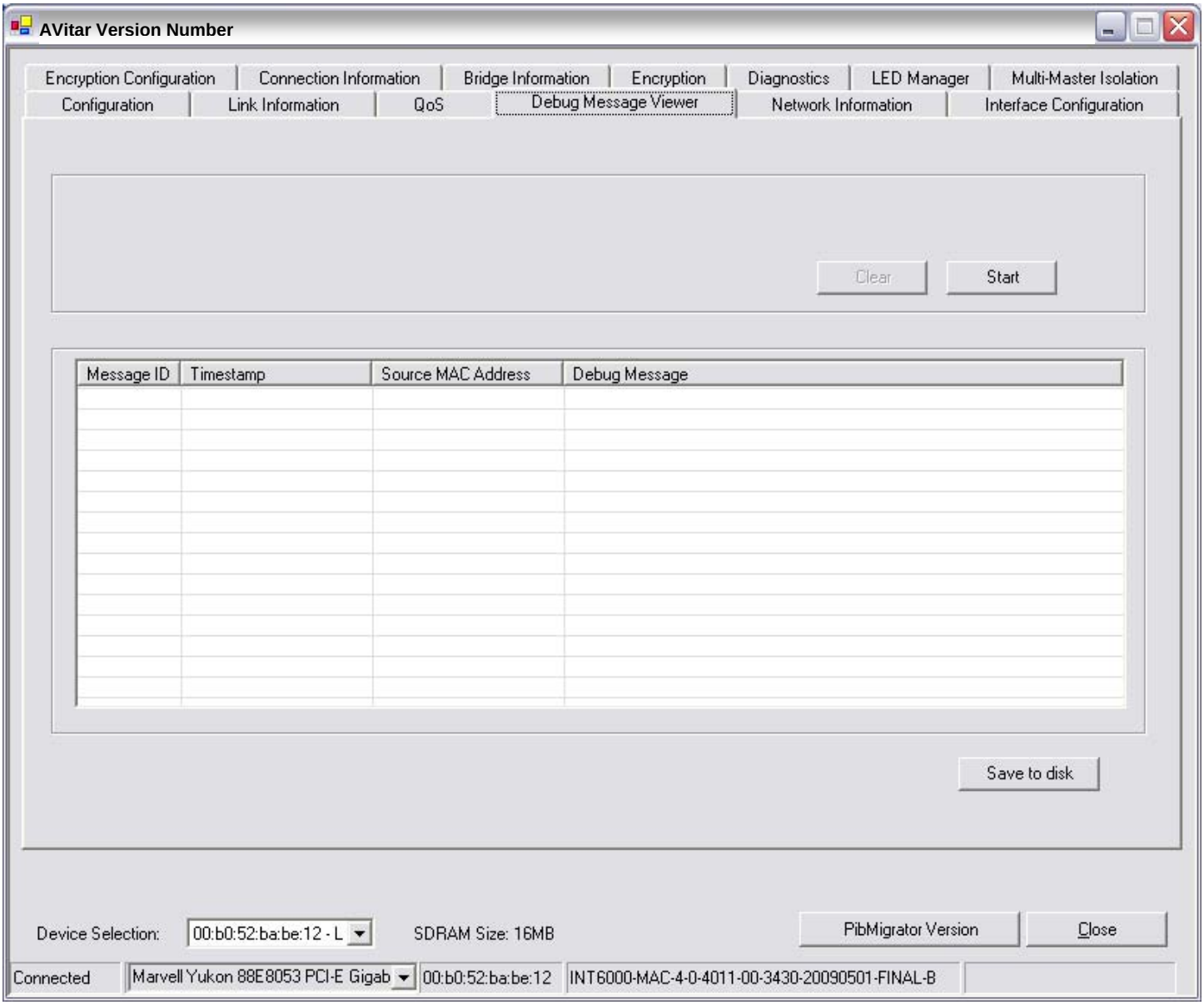



**Figure 9: Debug Message Viewer Tab Window**

When used in conjunction with special debug versions of firmware, the Debug Message Viewer Tab displays internal firmware messages which can be helpful for problem troubleshooting. To enable message display select the "Start" button; messages are displayed as they are received. Each message has a sequential message ID, a message received timestamp, the MAC Address of the sending station and the actual debug message. Debug messages can be quite cryptic, but they have contextual meaning that Intellon Firmware Engineers may find helpful when troubleshooting difficult problems. When Debug Messages reception is enabled, the "Start" button will change to a "Stop" button. To stop Debug Messages from being displayed, click the "STOP" button. The button text will return to "Start." The clear button clears messages from the message list.

Note the Debug Message List will grow without bound as long as the message display is enabled (started) and there is a device sending messages. This means that Debug Message Logging is not meant to be enabled indefinitely as eventually the logging will exhaust the systems memory causing undesirable results. It is expected that the operator will "Stop" and "Clear" message logs prior to exhausting system memory.

## 3.7 Network Information Tab *(Operation Analysis Window)*

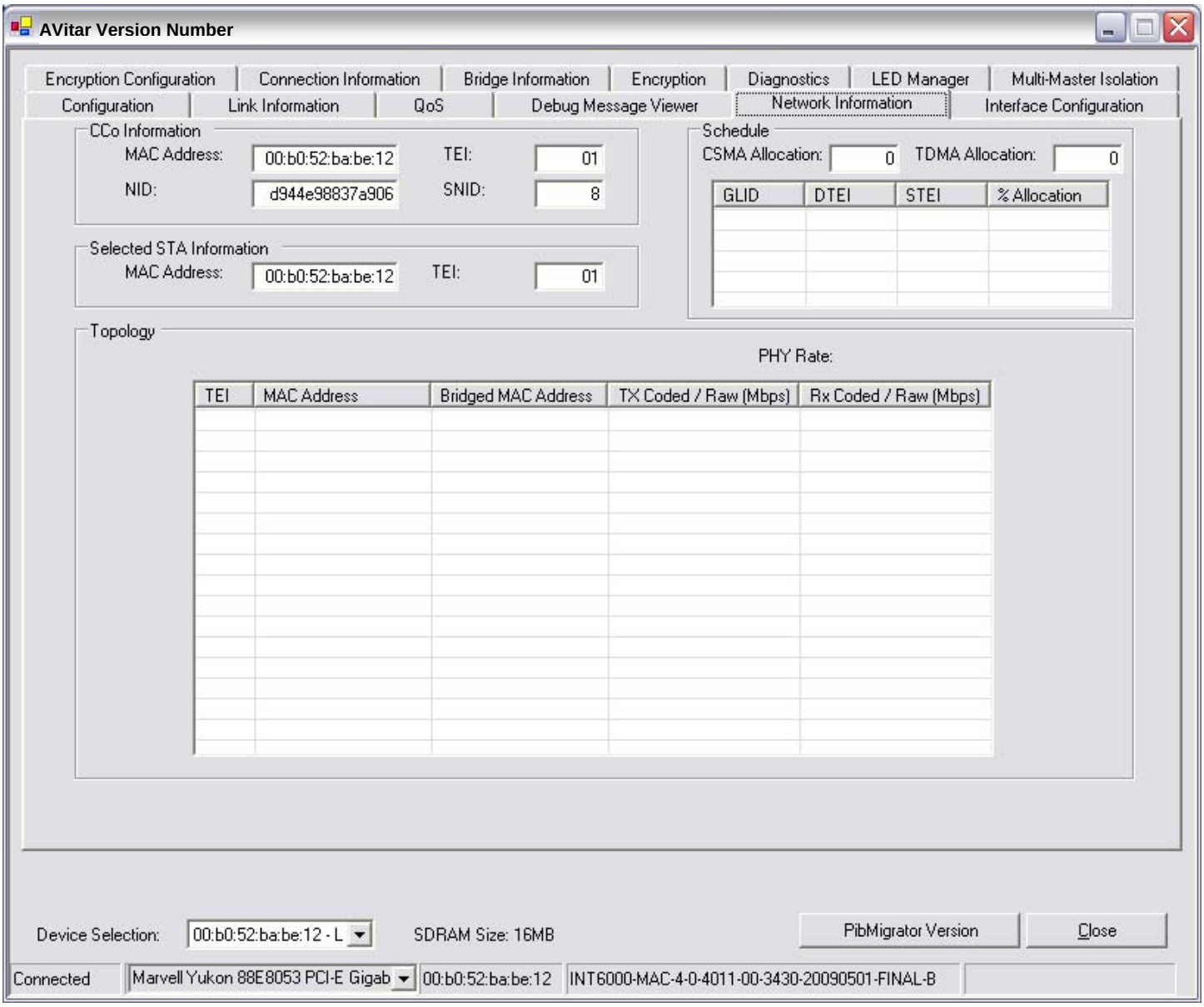



**Figure 10: Network Information Tab Window**

This window is an Operation Analysis window that reveals Network information in three categories: CCo Information, Connected STA Information and Topology.

### 3.7.1 Central Coordinator (CCo) Information

The 'CCo Information' group reveals the MAC address and TEI of the CCo in the network. In addition, it shows the Network ID (NID) and Sub-Network ID (SNID), which are HomePlug AV logical network identifiers.

### 3.7.2 Selected Station (STA) Information

The 'Selected STA Information' group shows the MAC Address and TEI for the station upon which the AVitar is running.

### 3.7.3 Topology

The 'Topology' group shows the TEI, MAC Address, Bridged MAC Address and the transmit (Tx) and receive (Rx) Coded and Raw PHY rates for all nodes on the network (other than the local STA). The 'Coded' rates exclude FEC bits. The

'Raw' rate is the actual channel bit rate. The Raw rate is determined by carrier bit loading and the applied HomePlug AV Tone Mask which utilizes 917 carriers out of a possible 1155. If all carriers were to be utilized with maximum bit loading on all 1155 carriers, the Raw channel rate would be approximately 250 Mbps. With the HomePlug AV Tone Mask applied, the maximum Raw channel rate is approximately 200 Mbps (198 Mbps maximum actual).

## 3.8 Interface Configuration Tab *(Configuration Window)*

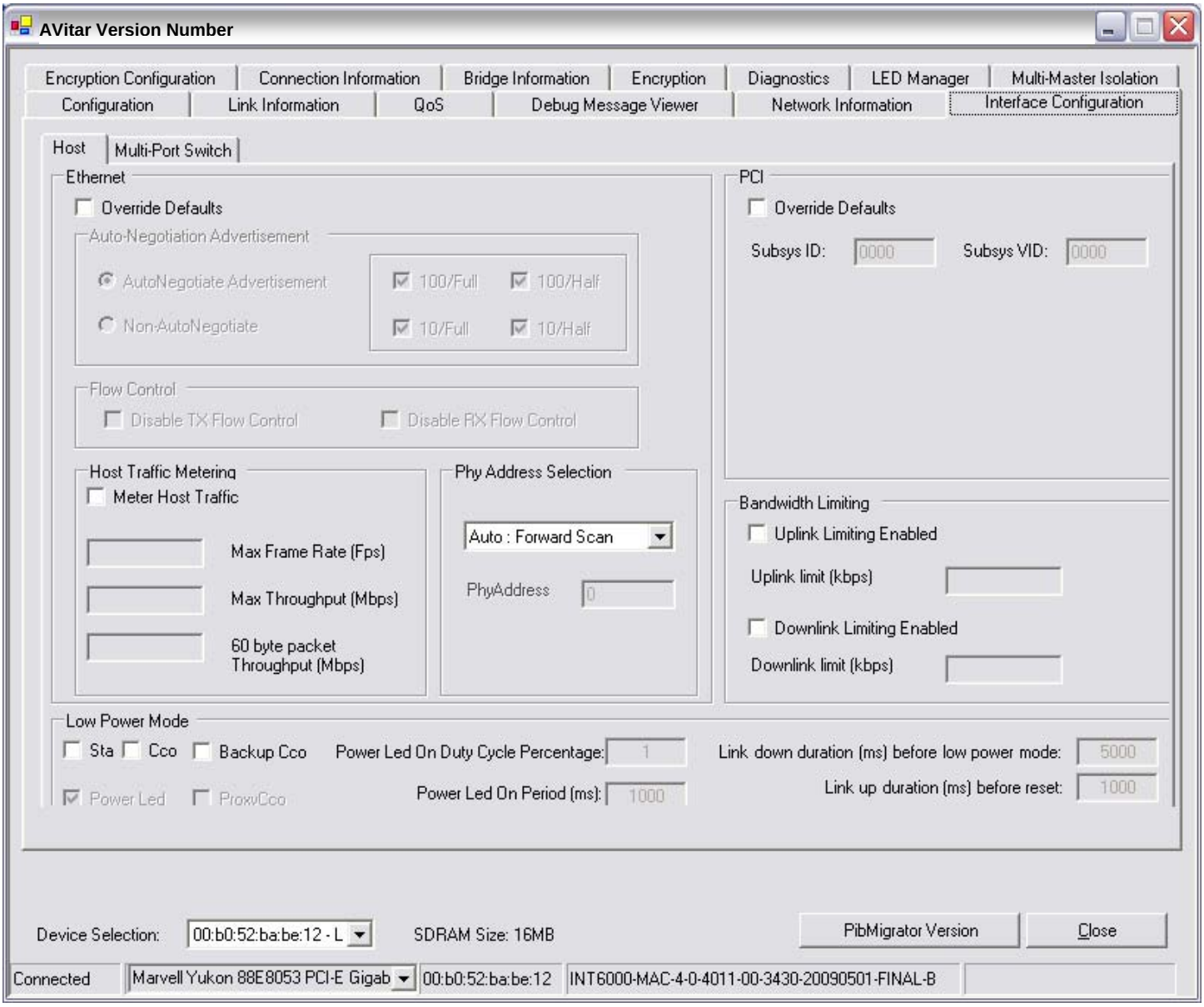



**Figure 11: Interface Configuration Tab Window**

### 3.8.1 Override Defaults Checkbox

The *Override Defaults* checkbox enables the Flow Control box.

### 3.8.2 Flow Control Box

The *Disable pause support* checkbox is used to disable flow control. Flow Control should only be enabled if auto-negotiation is enabled.

### 3.8.3 Host Traffic Metering

The 'Host Traffic Metering' group is by default unchecked. When it is checked on, it allows the maximum frames per second (Fps) for the outbound traffic flow through the Ethernet interface to be set. This is a fixed parameter for all packet sizes and CAP levels. Based on the number selected in this field, the maximum and minimum throughput of the outbound Ethernet interface (for 1514-byte and 60-byte packets respectively) will be shown on the fields below in the panel.

The maximum allowed frames per second (Fps) is 37500 and the minimum is 2000. The default value is set to the maximum 37500 Fps. Running a TCP test using the maximum packet size (1514 bytes) between two nodes under clean line conditions shows the following results:

- 37500 Fps: 54.3 Mbps
- 4000 Fps: 42.6 Mbps
- 2000 Fps: 21.9 Mbps

These values are provided for reference only and results may vary depending on the test platform used.

### 3.8.4 PHY Address Selection

If the INT6x00 is connected to a managed switch via MII this selects the default management PHY address.

### 3.8.5 Low Power Mode Features Configuration

- **Device Role – STA, CCo, Backup CCo**: Only go into lower power state if this field is checked AND you are a STA, CCo, and/or Backup Cco.
- **Power LED – Duty Cycle**: Percent (%) of time when LED is on for the "blink" period when in low power mode.
- **Power LED – Blink when in low power mode**: If checked, the power LED will blink in low power mode. If not checked, power LED will remain on.
- **Power LED – On Period**: Length of blink period of power LED when in Low Power mode.
- **Link Up/Down Timer – Time before Low Power Mode**: Count down timer after the Ethernet link goes down before low power mode is enabled.
- **Link Up/Down Timer – Time before Device Reset**: Countdown timer after the Ethernet link is restored before the device wakes back up.

NOTES:

1. The Power LED ON period is also the polling loop period for monitoring the Ethernet link status. Therefore, for quick response, it is NOT recommended to set this to more than 5 seconds.
2. Low Power Mode is not supported on Multi-port Ethernet Devices with the INT6xxx device configured for MAC mode operation

#### 3.8.5.1 How Stand By Mode/Low Power Mode Works

**Stand By Mode** is a feature the enables the device to enter in Low Power Consumption when the Ethernet cable is removed.

#### 3.8.5.2 Stand By Mode/Low Power Mode Enablement

The user can set a device in Stand By Mode (or Low Power Mode) by navigating to the **Interface Configuration** Tab → **Host** Tab. In ***Low Power Mode*** Pane check **Sta, CCo Backup CCo**.




**Figure 12: Interface Configuration Tab – Low Power Mode**

If the 'Low Power Mode' **Sta, Cco, Backup Cco** is checked the 'Power Led' is checked, by default it will flash the Power Led at a rate specified by Power Led On Duty Cycle Percentage and Power Led On Period. To override which Led to flash (by default it is the Power Led) see the standby mode on the LED Manager Tab in Section 3.14.

#### 3.8.5.3 Stand By Mode/Low Power Mode LED Behavior

The user can set the LED Behavior of the device during Stand By Mode (or Low Power Mode). The LED Behavior pattern parameters modifiable by the user are:

- **Pulse Duty Cycle** (expressed in percentages)
- **Pulse Period** (expressed in milliseconds)
- **Link Down Time before device enters Low Power Mode** (expressed in milliseconds)
- **Link Up Time after device leaves Low Power Mode** (i.e. after the user plugs-in the Ethernet cable) (expressed in milliseconds)

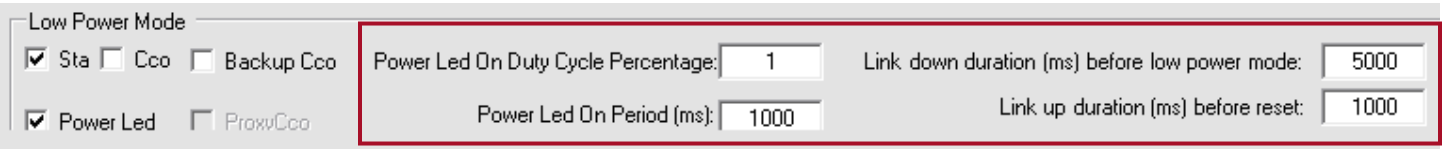
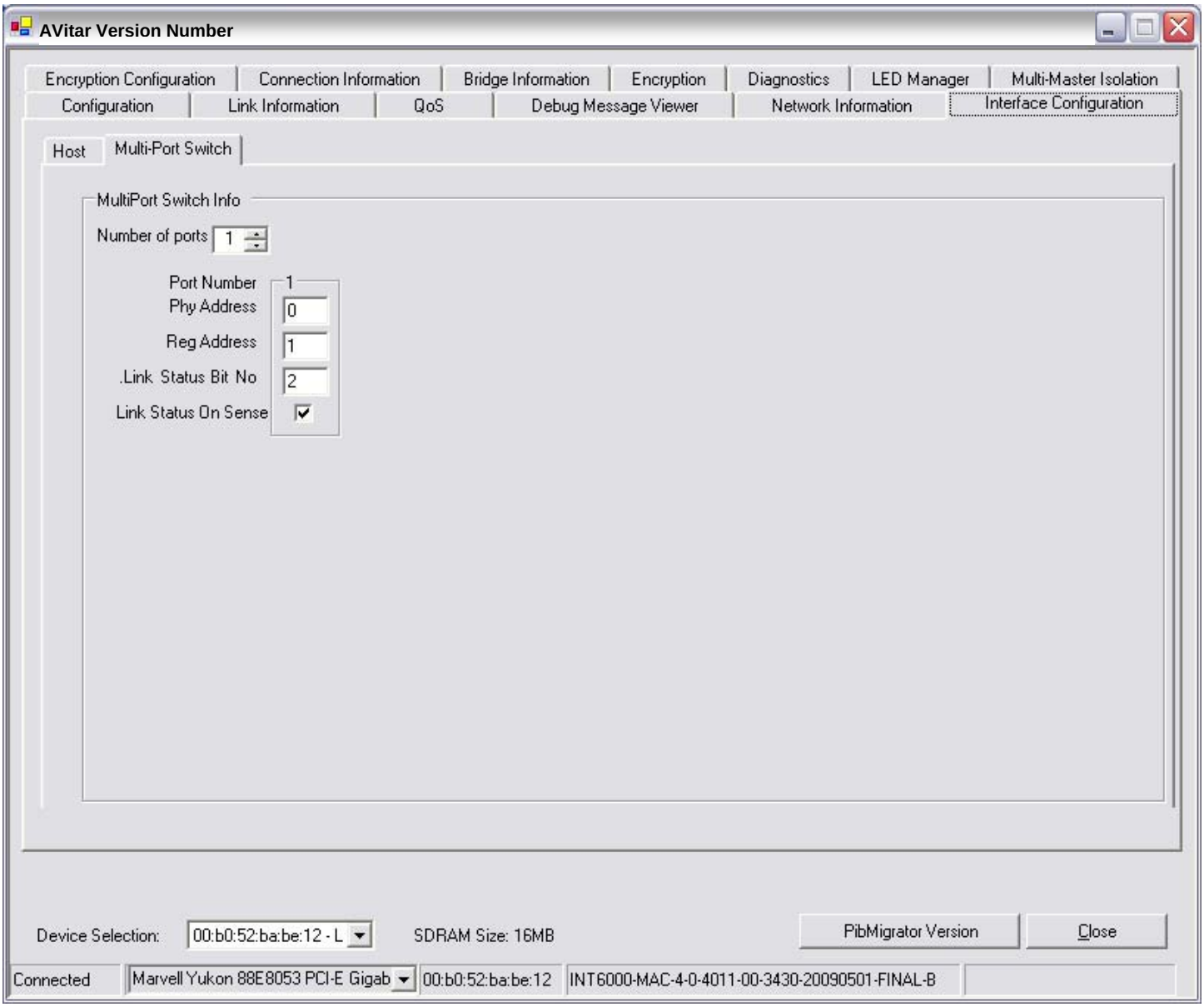



**Figure 13: Interface Configuration Tab – Low Power Mode LED Behavior**

### 3.8.6 Bandwidth Limiting

Bandwidth Limiting is EoC/MDU only feature. It limits the rate at which the slave may receive and transmit traffic. The minimum is 2 Mbps, the maximum value is 16 Mbps in increments of 64 Kbps.

### 3.8.7 Multiport Switch




3.8.7.1 Number of Ports: Specifies the physical number of Ethernet PHY ports present on the multi-port PHY device

3.8.7.2 PHY Address: Specifies hardware PHY address used by the switch chip that corresponds to Port Number

3.8.7.3 Reg Address: Specifies hardware register address used by the switch chip that corresponds to Port Number

3.8.7.4 Link Status bit: Specifies which bit location within the Register Address reports the Ethernet Link status

3.8.7.5 Link Status ON Sense: describes how the device firmware interprets the Link status bit. If the box is checked, a link status bit equal to 1 means the Ethernet link is up. If the box is blank (not checked), a link status bit equal to 0 means the Ethernet link is up.

NOTE: The multi-port switch devices needs to configure the INT6xxx device for MAC mode operation to enable firmware access to the switch chip MDIO interface.

## 3.9 Encryption Configuration Tab *(Configuration Window)*

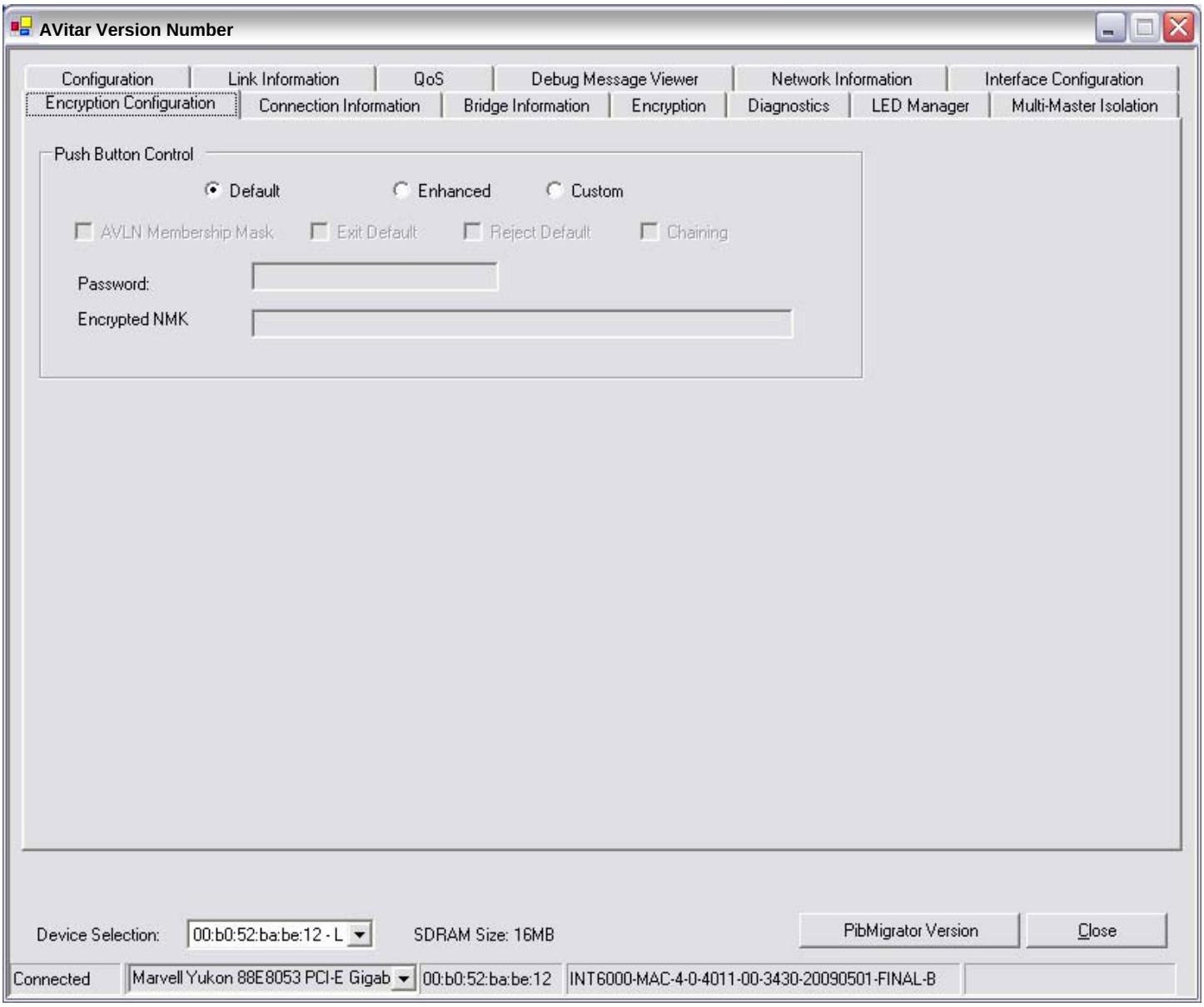



**Figure 14: Encryption Configuration Tab Window**

This tab allows configuration of the push button mating operation and behavior.

### 3.9.1 Default

Allows push button mating to act as per previous FW release – i.e. do NOT change default NMKs, single pair mating only, obey the membership bit.

### 3.9.2 Enhanced

Enables the following fields in their default configuration

### 3.9.3 Custom

Enables the following fields and allows overrides of their default configuration. Additionally, each device shall have the space to store a vendor-specific default password. The features above shall be applied to both the default password of HomePlugAV and a vendor-specific default password

### 3.9.4 ALVN Membership Mask

Ignore the AVLN membership bit. The AVLN membership bit forces devices that have ever been in a network to act as if they are still in a network – i.e. it is always an adder. This setting allows the device to be configured to ignore this field.

### 3.9.5 Exit Default

The device shall check upon each button-press if its NMK is the hash of the default password HomePlugAV. If so, the device would leave the network and become a joiner. If the device is unable to successfully join a network, it is either because the encryption push button mating timeout period expired, the device tried to join an adder and was rejected, the device became an adder and then failed to join a joiner, or the encryption period was cancelled via a subsequent button press, then the device shall return to the default network.

### 3.9.6 Reject Default

Devices shall either propagate or accept either the password HomePlugAV or the password hash stored as the vendor-specific default password.

### 3.9.7 Chaining

A device, upon becoming an adder, shall remain in the adder state for the duration of the encryption period, or until the encryption button is pressed again to cancel during the encryption period. During that time, the adder shall add every joiner that asks. If the encryption button is pressed to cancel the chaining, as long as one device has been added the adder shall behave as if there has been a successful add. Each time the chained adder adds a device, the adder shall restart the encryption period timer such that one encryption period remains.

## 3.10 Connection Information Tab *(Operation Analysis Window)*

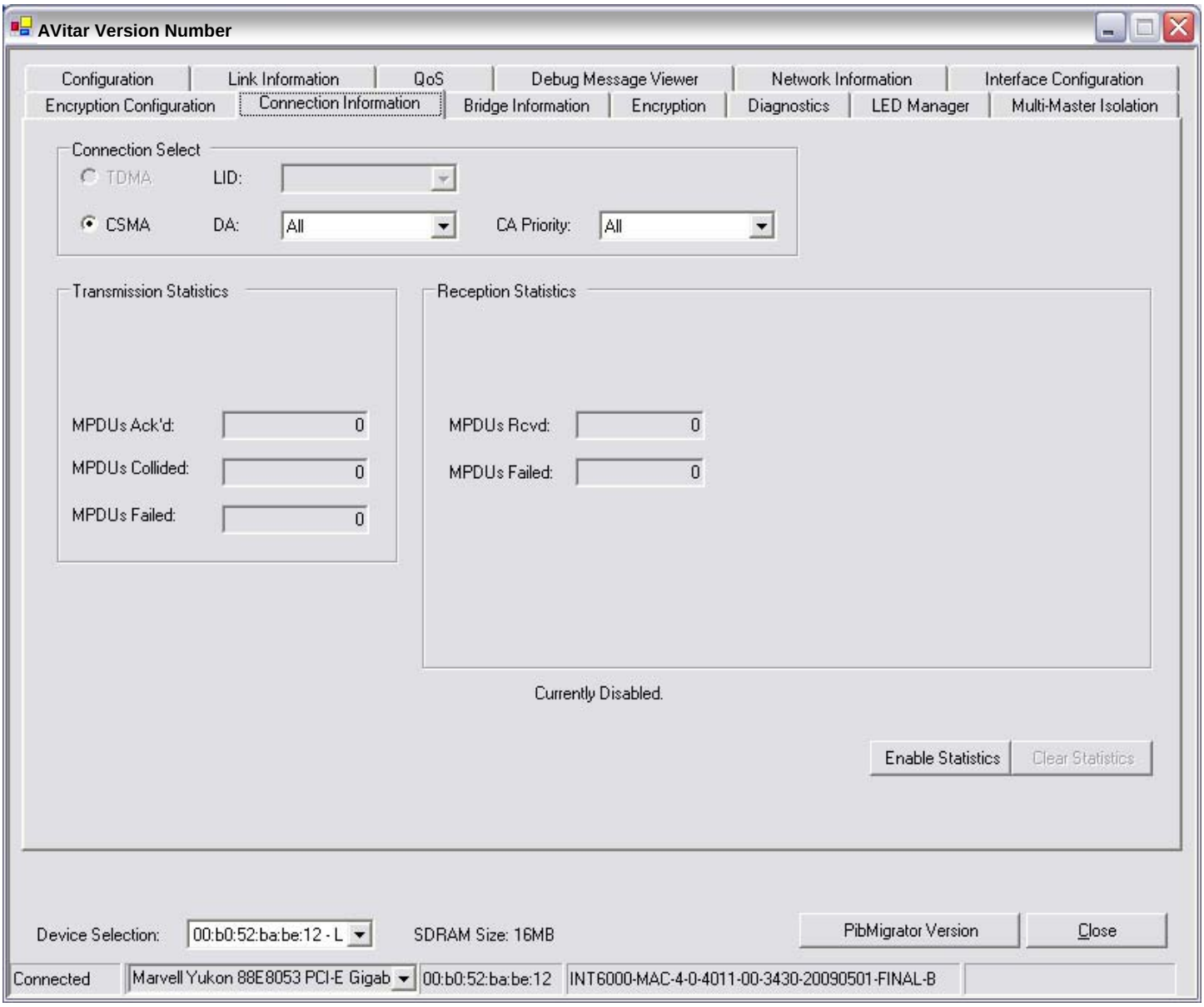



**Figure 15: Connection Information Tab Window**

The Connection Information window is used to acquire statistics for both transmit and receive operations in the local or remote network.

### 3.10.1 Connection Select

The 'Connection Select' group is used to identify the type of connection (TDMA or CSMA) before statistics are acquired. The TDMA radio button is grayed out because it is not supported in this version of the AVitar. When CSMA is selected, the Destination Address (DA) drop-down menu may be used to select ALL devices or specific devices in the network. In addition, Channel Access (CA) priority can be defined using the second drop-down menu. The AVitar allows only certain valid combinations that can be selected by the user. The following table describes the combinations.

| Device Selection | Destination Address (DA) | Channel Access priority | Allowed |
|---|---|---|---|
| Local device | All | All | Yes |
| Local device | Remote device | All | Yes |
| Local device | Remote device | CA0 or CA1 or CA2 or CA3 | Yes |
| Local device | Local device | Any | No |
| Remote device | All | All | Yes |
| Remote device | Local device | All | Yes |
| Remote device | Local device | CA0 or CA1 or CA2 or CA3 | Yes |
| Remote device | Remote device | Any | No |

### 3.10.2 Transmission and Reception Statistics

The 'Transmission and Reception Statistics' groups return operational data regarding MPDUs and packet data unit handling. Results shown in these fields provide valuable connection quality information.

| | |
|---|---|
| **Transmission Statistics** | |
| MPDUs Ack'd | MPDUs sent with SACK received |
| MPDUs Collided | MPDUs sent with no SACK received |
| MPDUs Failed | MPDUs sent with SACK 'out of resources' received |
| **Reception Statistics** | |
| MPDUs Recvd | MPDUs received and acknowledged |
| MPDUs Failed | MPDUs not received due to out resources (SACK sent) |

The 'Enable Statistics' button is used to acquire the operational data and the 'Clear Statistics' button is used to clear the fields of data. The values shown by the AVitar is a cumulative total of the packet data that was collected from the start of either the 'Enable Statistics' button or the 'Clear Statistics' button click.

## 3.11 Bridge Information *(Operation Analysis Window)*

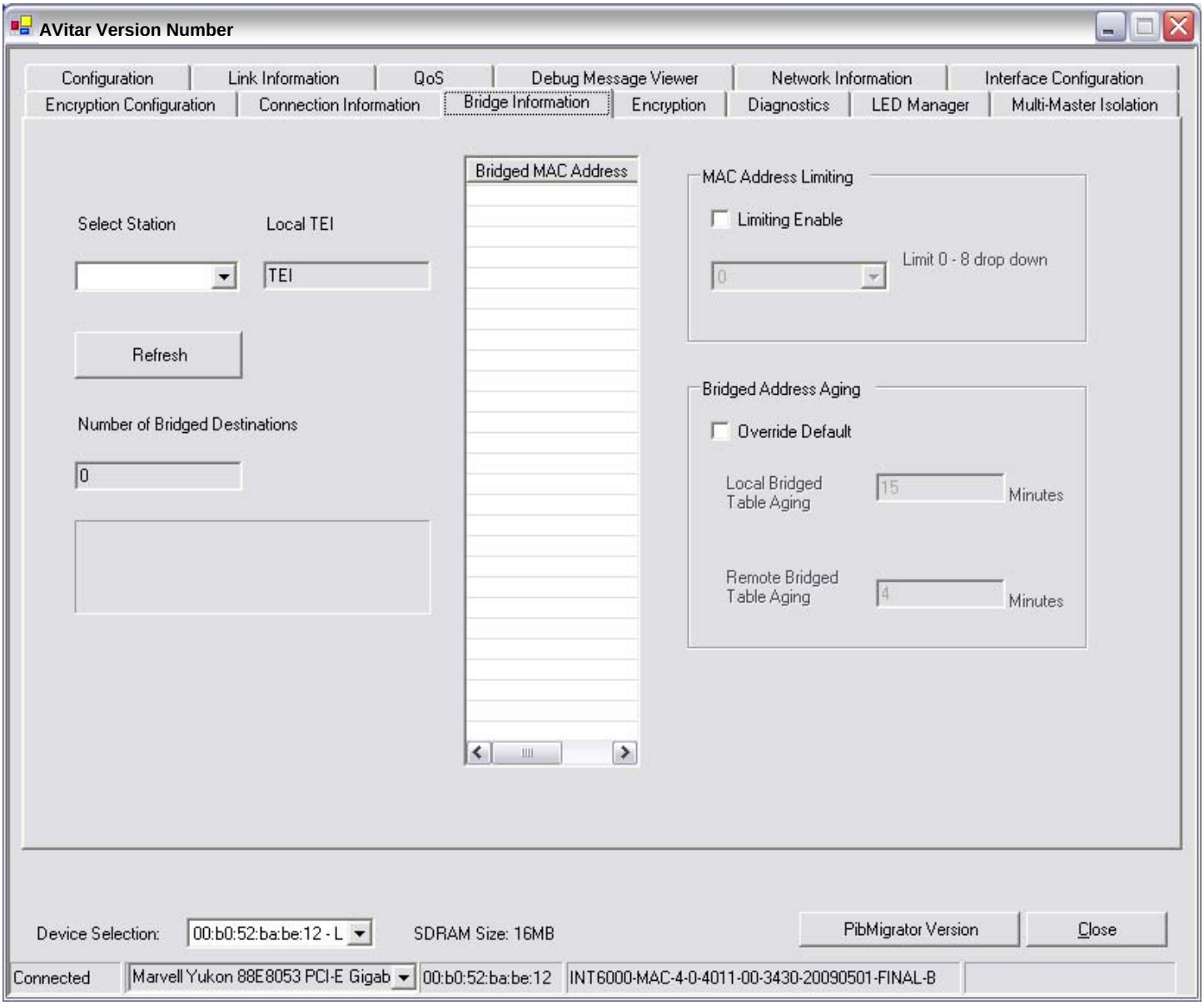



**Figure 16: Bridge Information Tab Window**

### 3.11.1 Select Station

The 'Select Station' group is used to identify the MAC address of the device that Bridging Information should be displayed. A list of MAC address that the device is bridging for is displayed on the right under the "Bridged MAC Address" list. The device's Local TEI and number of Bridged Destinations are shown on the left of the screen below the "Refresh" button.

Pressing the "Refresh" button can be used to update the display.

The MAC Address Limiting group is used to limit the number of MAC addresses that the selected station will bridge for. Setting the Select Value to zero will disable all traffic from passing through the device from the host to the powerline. Mac Management traffic is never limited and will always be processed.

The Bridged Address Aging control is used to override the bridge timers for both remote devices and local devices.

## 3.12 Encryption Tab *(Configuration Window)*

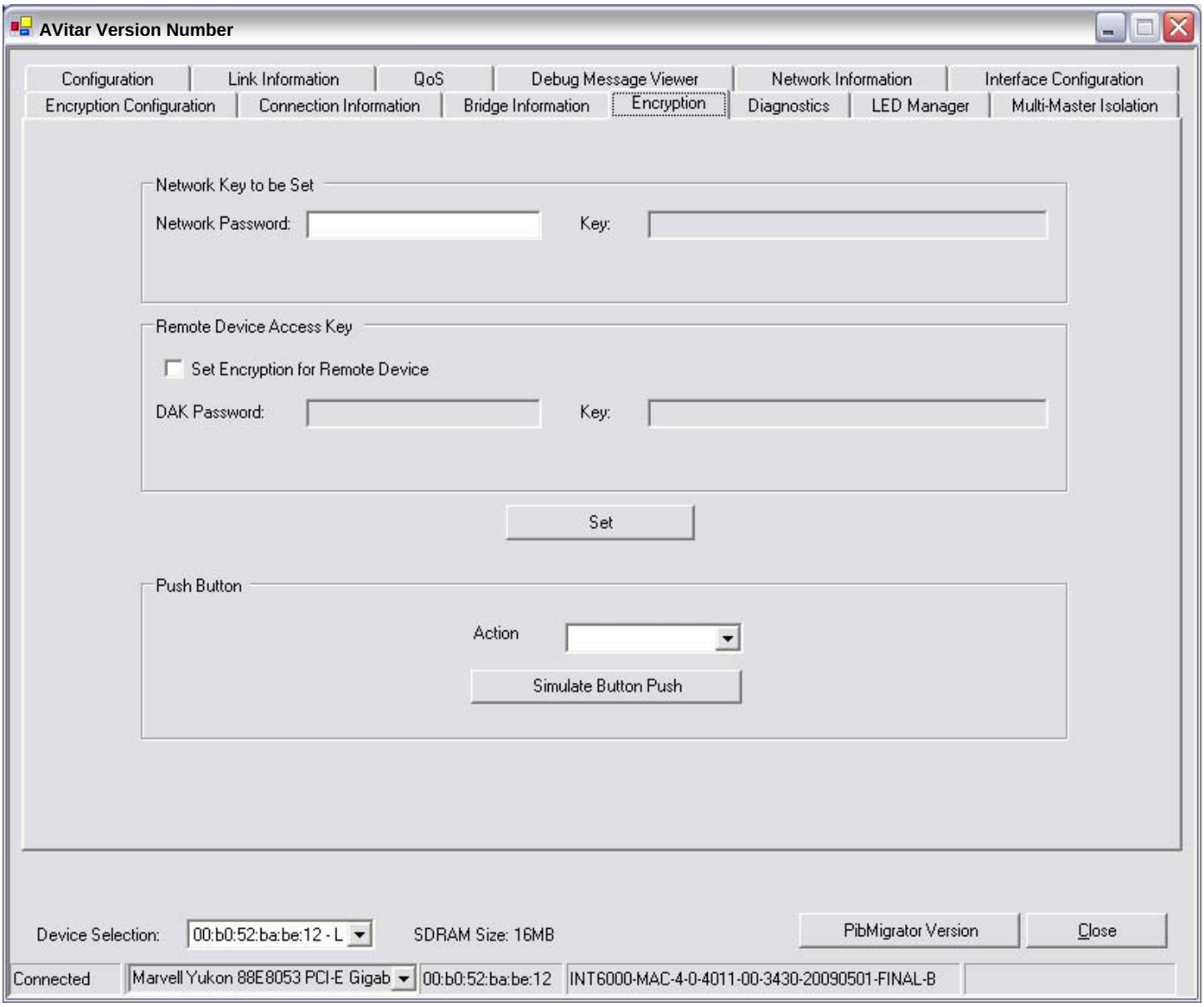



**Figure 17: Encryption Tab Window**

This Encryption window is used to set or change the network password on a remote device identified by its Device Access Key (DAK) password. Clicking the 'Set' button sets the entered passwords. If the DAK password field is left blank, then clicking the 'Set' button will set local device with the entered password. The 'Set Encryption for Remote device' checkbox should be selected to set the Network Password for the remote device.

The Key fields are the Hashed Keys of the network password or DAK password.

The Push Button controls box includes the 'Action' drop-down box that provides a choice of three actions {Simple Connect, NMK Randomize and AVLN Status} signaled to the device when the 'Simulate Button Push' button is pressed. Additionally, two configuration parameters are exposed in the 'PIB Controls' sub-group box.

## 3.13 Diagnostics Tab *(Event Log)*

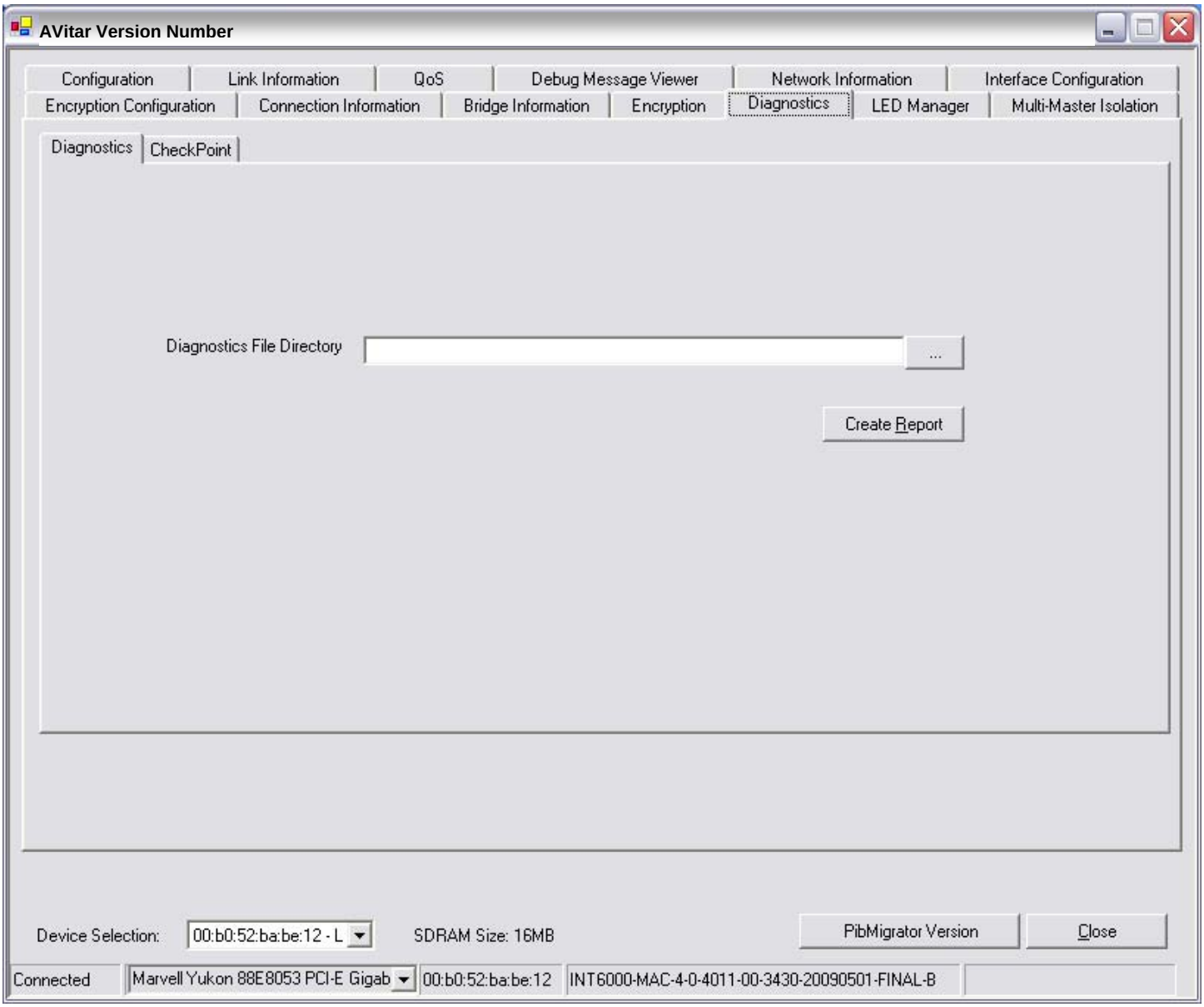



**Figure 18: Diagnostics Tab Window**

### 3.13.1 Three Sub-tabs

*Diagnostics* – This tab allows the user to select a directory to be used as a repository for retrieved reports.

*Watchdog* – This tab displays the Watchdog component of the report.

*Check Point* – This tab displays the Check Point component of the report.

**Note** – The use of the Diagnostic tabs should be used in conjunction with Intellon field application engineers.

## 3.14 LED Manager Tab *(Configuration Window)*

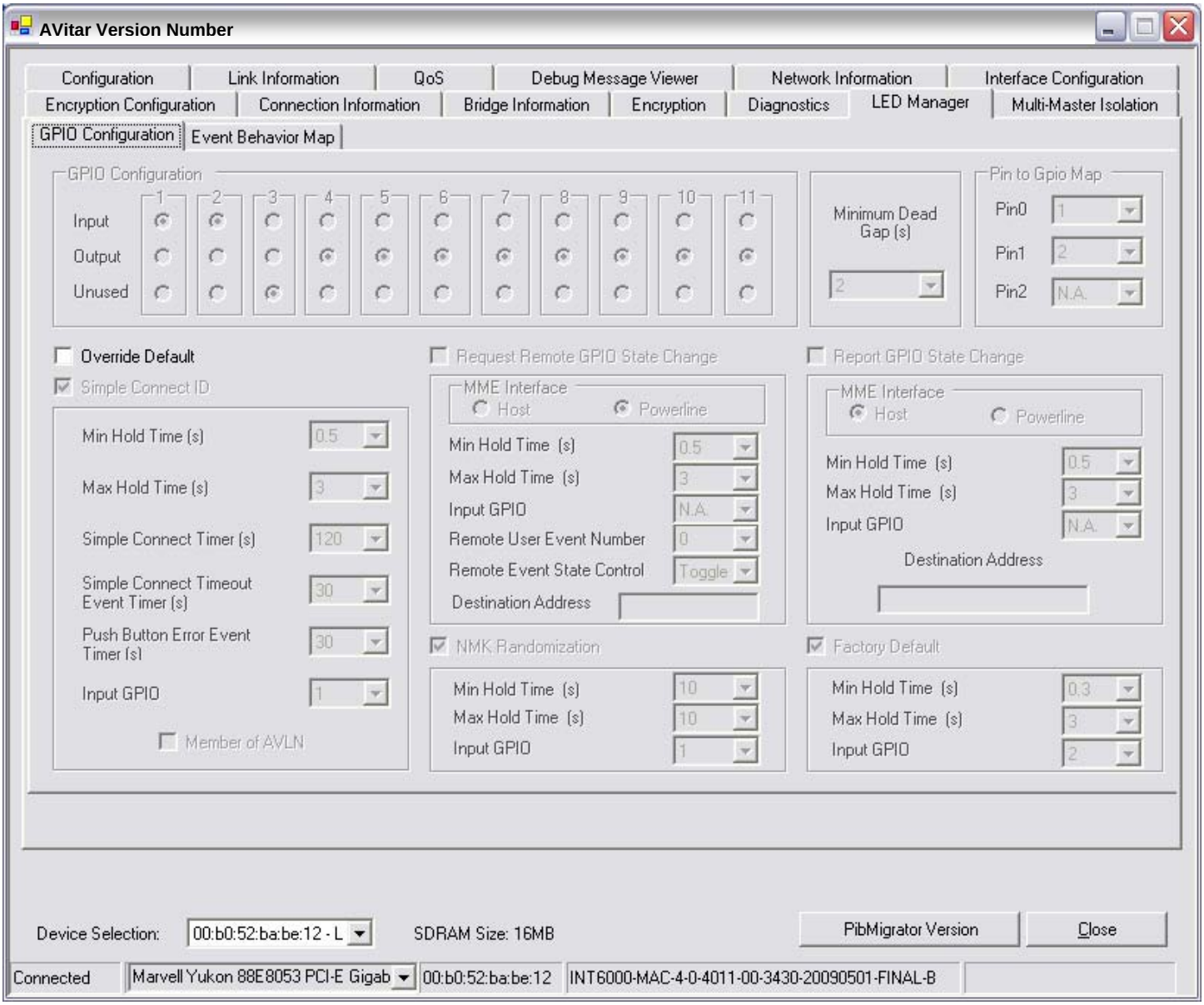



**Figure 19: LED Manager Tab Window**

The LED Manager tab allows the user to configure the LED functionality. These configuration elements are conveyed in the PIB and must be written or saved to preserve them.

### 3.14.1 GPIO Configuration

The 'GPIO Configuration' group allows the user to map GPIO signals to Input, Output, or Unused. Figure 18 show the default mapping for the Intellon INT6400 Wall Adapter.

The input GPIO configuration for Simple Connect, NMK Randomization and Factory Default functions are shown to the left of the screen displayed in Figure 19.

- **Simple Connect ID**
  Min Hold Time, Max Hold Time, Adder Failure Timeout, and Simple Connect Timeout controls can be used to customize this function.
- **NMK Randomization**
  Min Hold Time, Max Hold Time controls can be used to customize this function.

- **Factory Default**
  Min Hold Time, Max Hold Time controls can be used to customize this function.
- **Minimum Dead Gap**
  Minimum period between the maximum hold time and the minimum hold time of two button functions on the same GPIO. For example, Simple Connect has a maximum hold time of three seconds by default. Setting the Minimum Dead Gap to two seconds requires that the NMK Randomization function have a minimum hold time of five seconds.
- **Request Remote GPIO State Change**
  Enables the GPIO State Change Request MME. This is used to trigger a change in the GPIOs of another device. The trigger is a GPIO Input event (i.e. Pushbutton). See the Intellon HomePlug AV FW TRM for details on the GPIO State Change Request MME. Min Hold Time, Max Hold Time and Input GPIO controls can be used to customize this function. The fields of Remote User Event Number and Remote Event State Control are used to control the behavior of the remote device upon receipt of this MME.
- **Report GPIO State Change**
  Enable GPIO state change indicates MME. See Intellon HomePlug AV Firmware v4.0 TRM for GPIO state change MME. Min Hold Time, Max Hold Time controls can be used to customize this function.
- **MME Interface Host or Powerline**
  Interface which MME is transmitted
- **Destination Address**
  Destination Address is the destination MAC address

#### 3.14.1.1 Stand By Mode/Low Power Mode GPIO Assignment

The user can assign the Stand By Mode (or Low Power Mode) event to a specific LED (or GPIO number) by navigating to the **LED Manager** Tab → **Event Behavior Map** Tab.

The user can set the GPIO number in ***Stand By Mode*** Pane: check **Override Stand By Mode GPIO** and select from the drop down list the GPIO number.

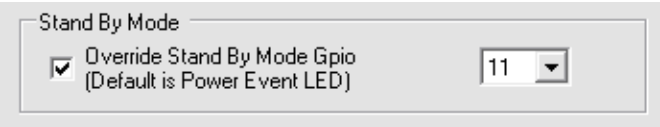



**Figure 20: Low Power Mode GPIO Assignment**

The default GPIO number assigned to Stand By Mode (or Low Power Mode) event is 11 (Power LED).

### 3.14.2 Event Behavior Map

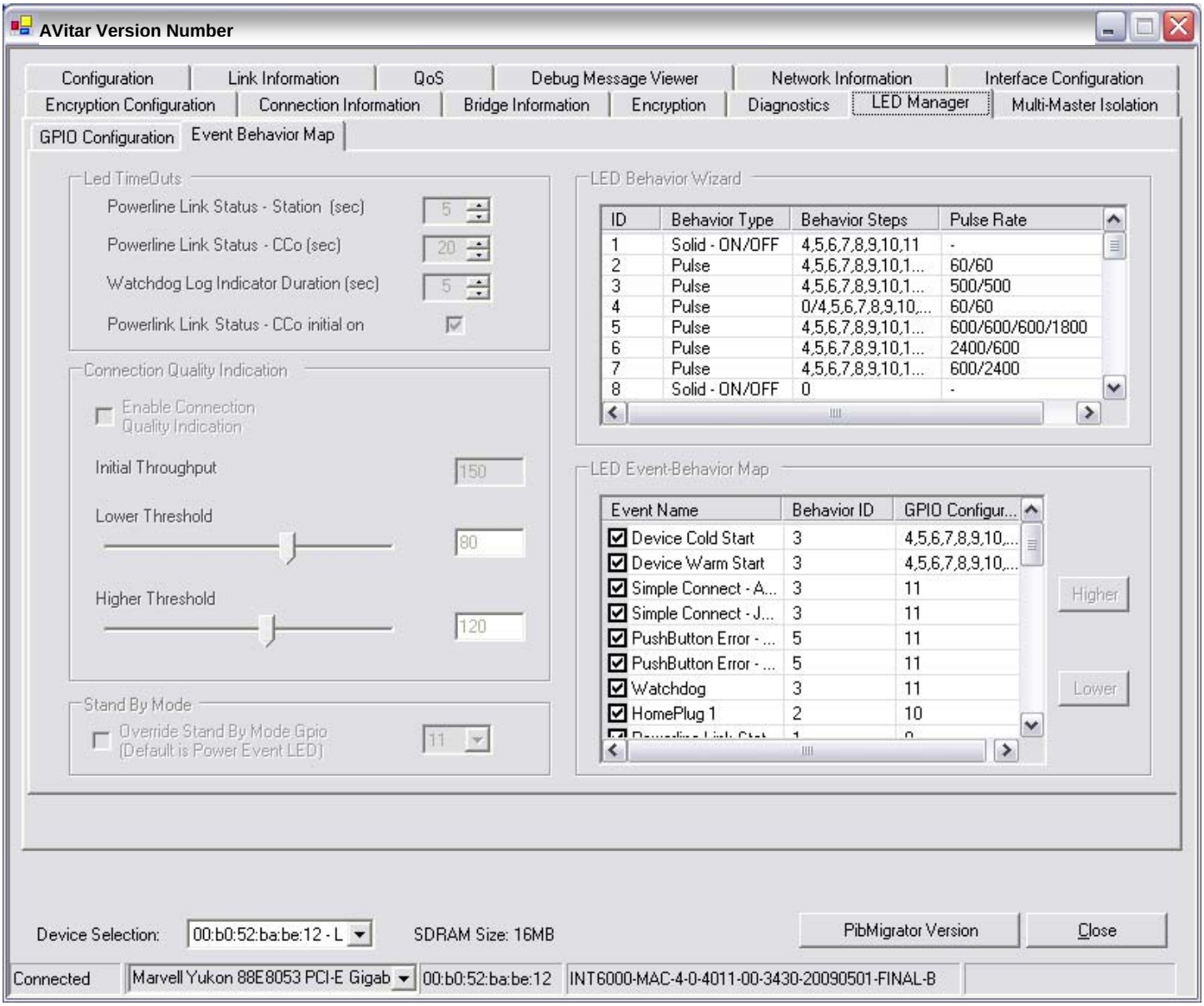



**Figure 21: Event Behavior Map Window**

The Event Behavior Map tab allows the user to configure the LED event behavior.

The Led TimeOuts Control is used to control the Powerline Link Status LED and Watchdog log indication LEDs

The Connection Quality Indication Control is used to customize the throughput events. The slider controls are used to set the lower and higher thresholds. The range of the connection quality threshold is between 10 Mbs and 150 Mbs.

The Stand By Mode Control is used to assign a GPIO pin to the Stand By Mode behavior.

### 3.14.3 LED Behavior Wizard

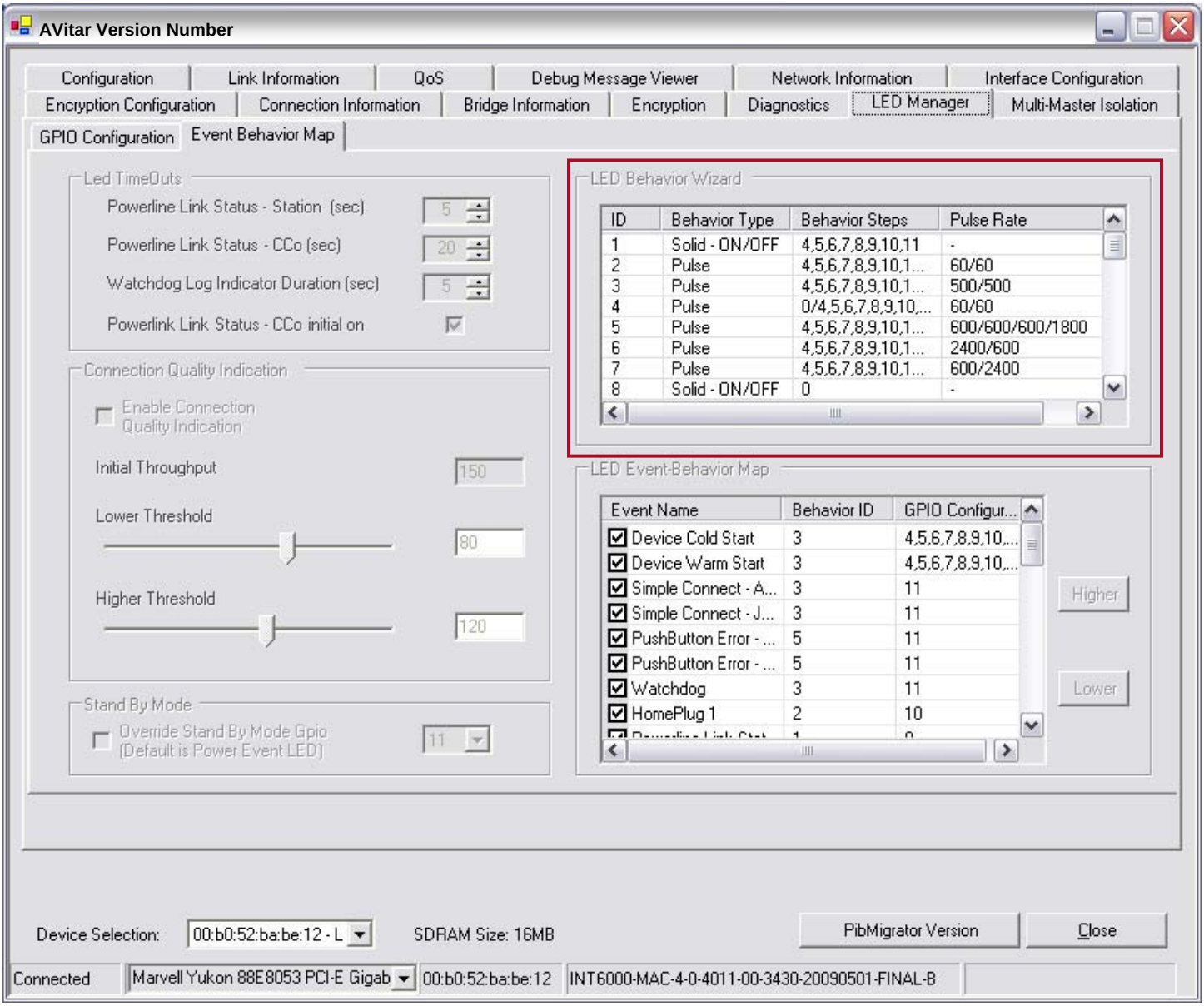



**Figure 22: LED Behavior Wizard**

The LED Behavior Wizard Control is used to define the pulse pattern for an LED behavior. The default behaviors are shown in this control. Double clicking on a behavior ID brings up the LED Event Behavior Wizard. The LED Behavior Wizard allows custom programming of a behavior.

### 3.14.4 LED Event-Behavior Map

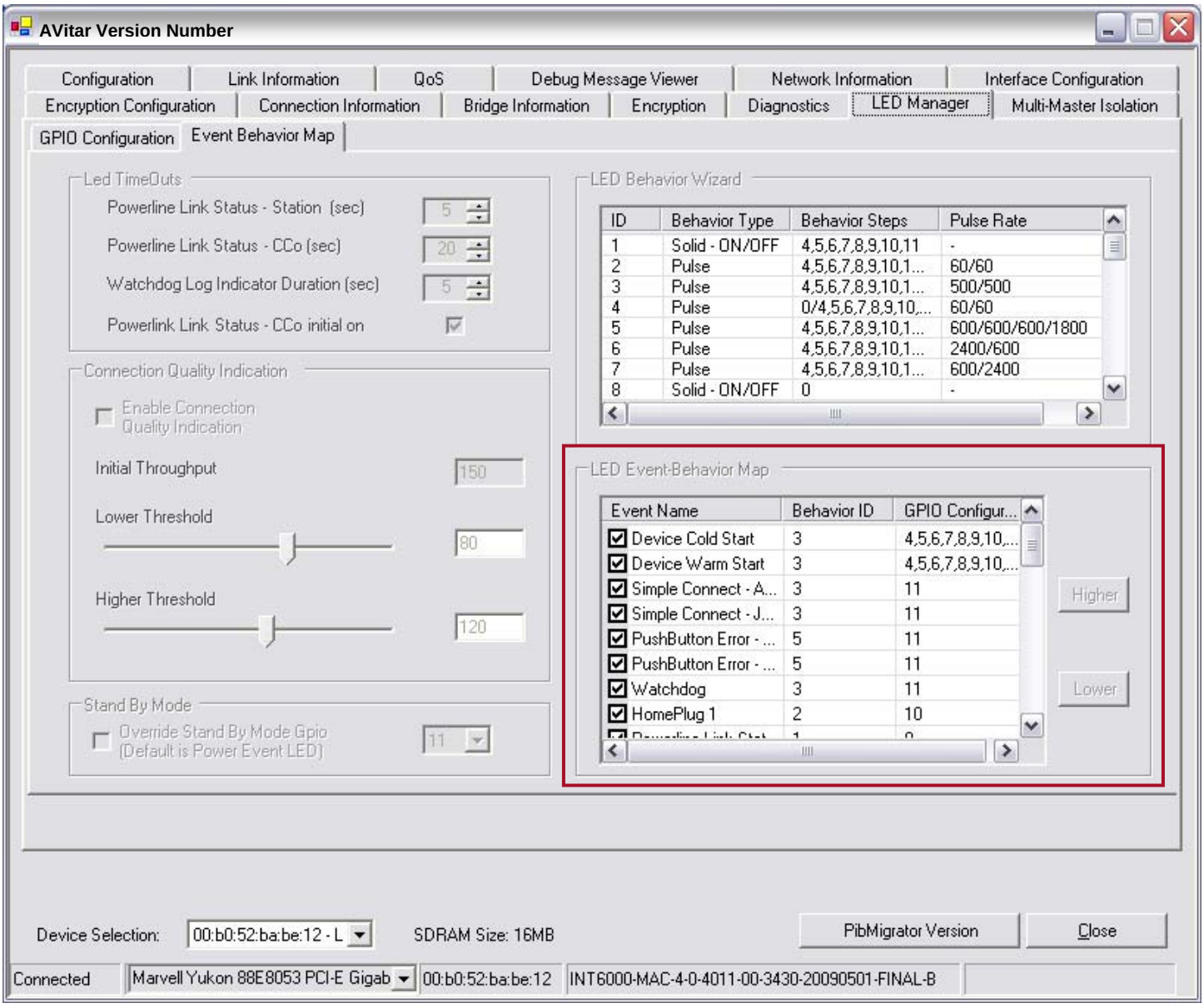



**Figure 23: LED Event-Behavior Map**

The LED Event Behavior Map is used to map a LED Event to an LED behavior ID. The default LED Events are shown in this control. Double clicking on an Event Name brings up the Event Behavior Map Wizard. The Event Behavior Map Wizard allows custom assignments for a selected event and configures a corresponding GPIO signal.

Higher/Lower buttons are used to assign priority when multiple events are mapped to the same GPIO pin.

For example the power LED can be used to indicate that the Simple Connect Function is in progress as well as indicating power on.

## 3.15 Multi-Master Isolation Tab *(Configuration Window)*

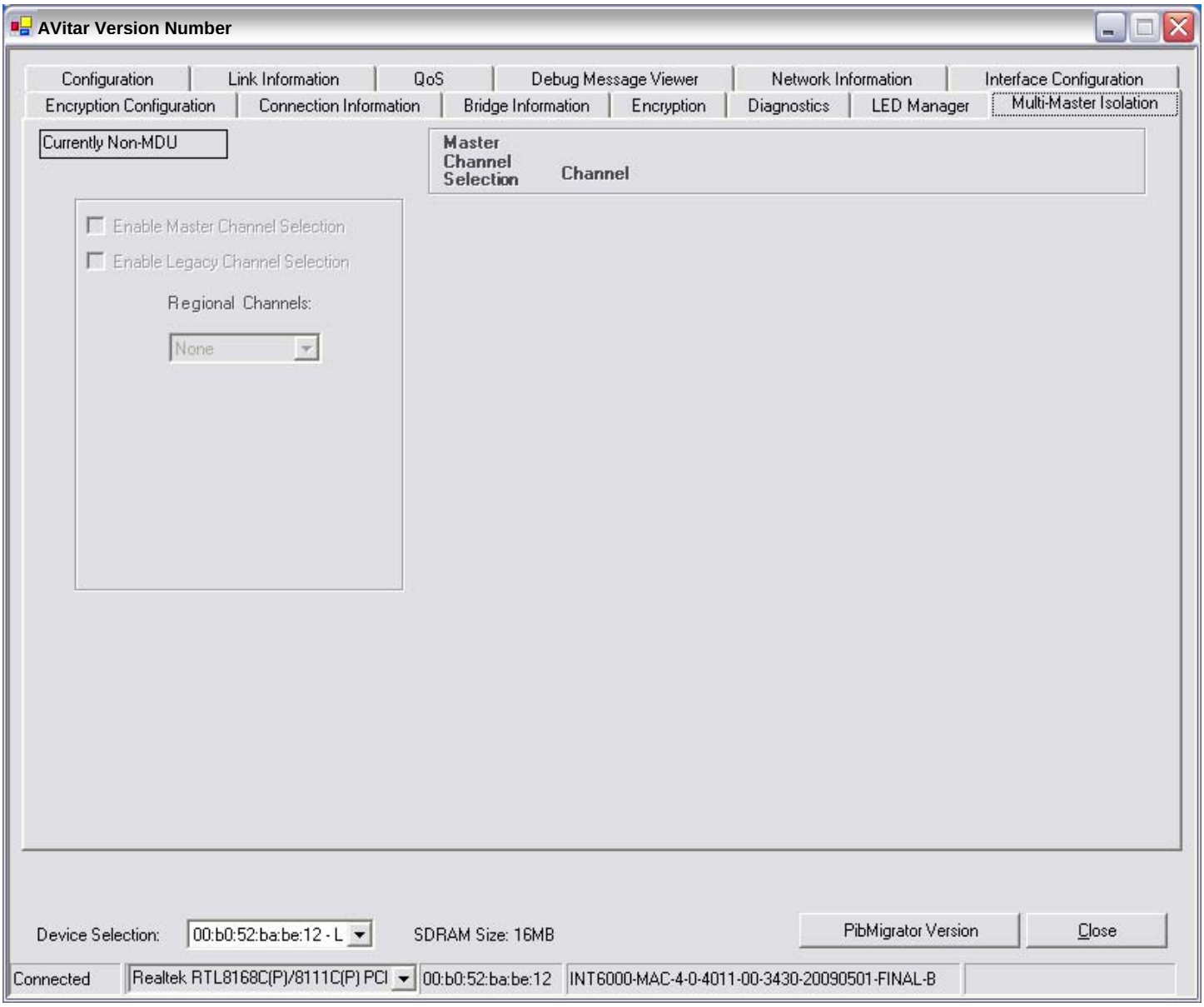



**Figure 24: Multi-Master Isolation Tab – Currently Non-MDU**

### 3.15.1 Currently Non-MDU

The 'Currently Non-MDU' indicates the current mode operation which is determined by the MDU selection on the Configuration Tab see Figure 5.

To enable Multiple Master channel selection, choose MDU selection on the configuration tab (Figure 5) and channel selections in the Multi Master Isolation tab (see Figure 25 or Figure 26).

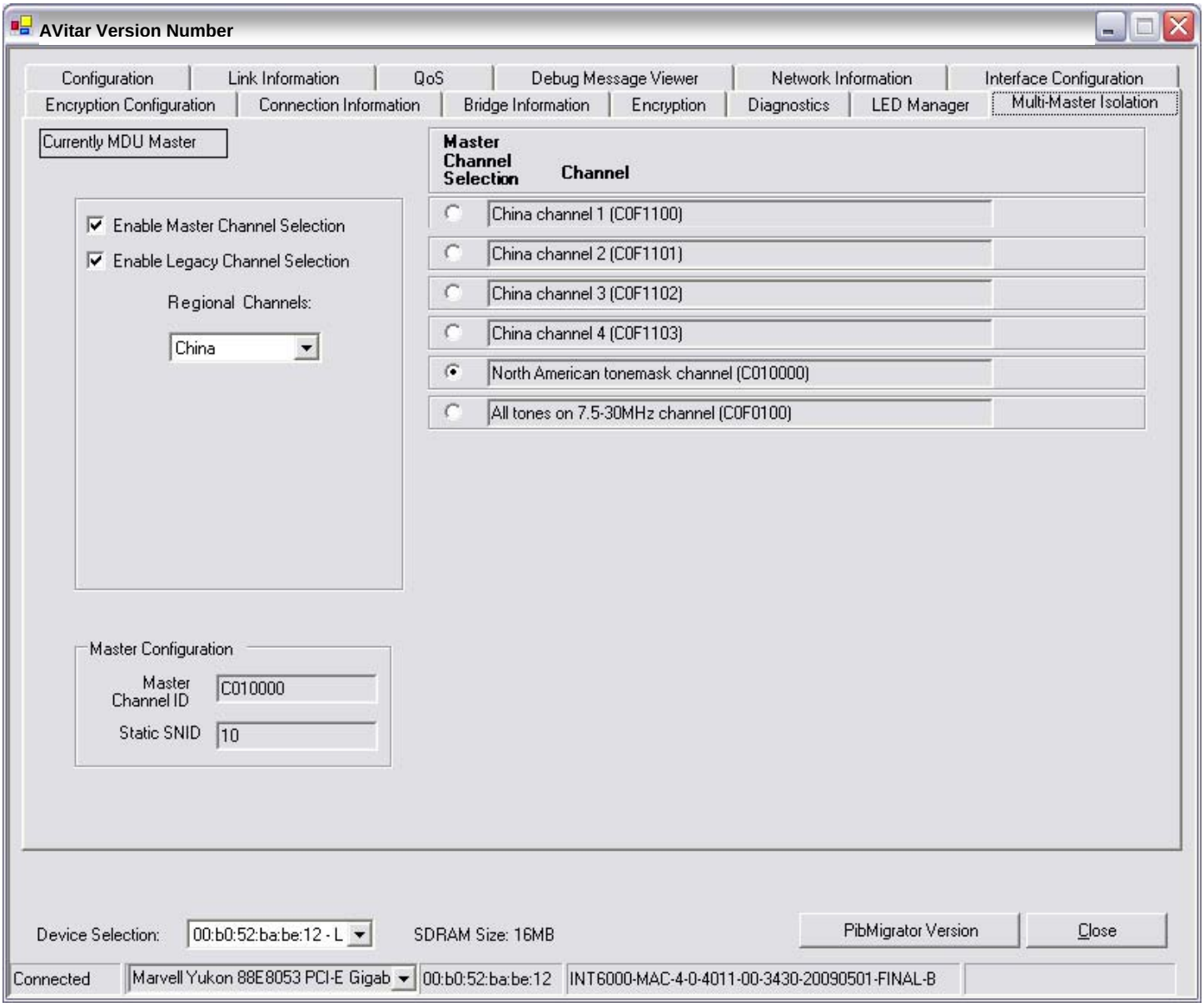



**Figure 25: Multi-Master Isolation Tab – Master Configuration**

### 3.15.2 Currently MDU Master

The 'Currently MDU Master' indicates the current mode operation 'Master' which is determined by the MDU selection on the Configuration Tab see Figure 5.

#### 3.15.2.1 Enable Master Channel Selection

The 'Enable Master Channel Selection' will enable Legacy Channel Selection checkbox and Regional Channels dropdown. China selection will enable Master Channel Selection radial buttons and display channel ID on the right panel.

#### 3.15.2.2 Enable Legacy Channel Selection

The 'Enable Legacy Channel Selection' will display channel ID for 'North America' and 'All tones on'. This option is only available if the Enable Legacy Channel Selection checkbox is selected.

### 3.15.2.3 Master Configuration

The 'Master Configuration' this is *read only*, the Static SNID number is extracted from the Configuration Tab see Figure 5. The Master Channel ID is displayed as a result from the 'Master Channel Selection' radial button selected on the right panel.

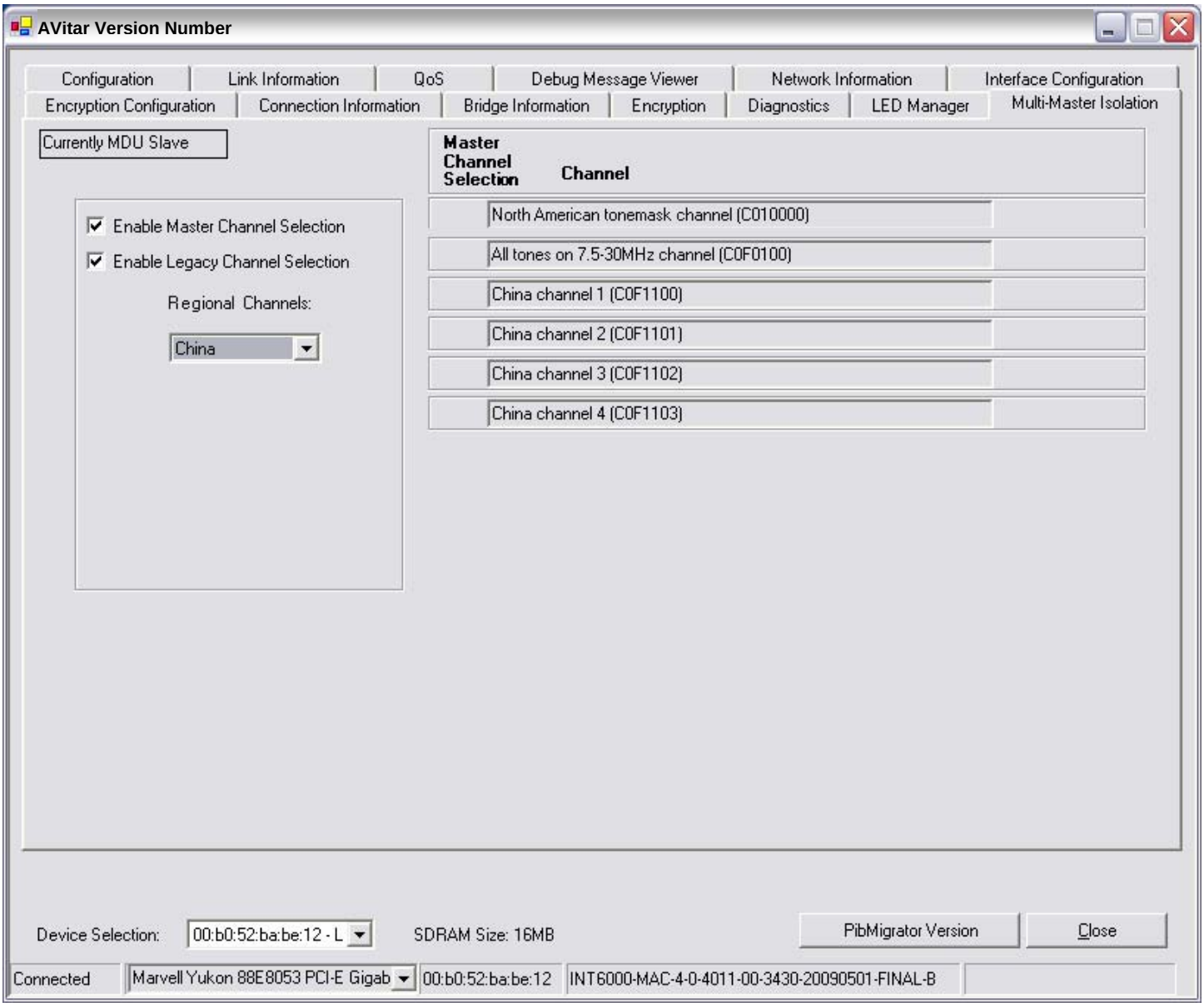



**Figure 26: Multi-Master Isolation Tab – Slave Configuration**

### 3.15.3 Currently MDU Slave

The 'Currently MDU Slave' indicates the current mode 'Slave' which is determined by the MDU selection on the Configuration Tab see Figure 5. For detailed description see Enable Master Channel Selection.

#### 3.15.3.1 Master Channel Selection

The 'Master Channel Selection' buttons are disabled for MDU Slave.

# 4. Revision History

**Table 1: Revision History**

| Revision | Modifications |
|---|---|
| 1 | Original Issue |
| 2 | Updated for v4.1 Beta Release |
| 3 | Updated for v4.1 GA Release |

# Appendix A: INT6X00 Amplitude Map Modification

Windowed OFDM is used in the PHY layer as the analog medium interface. The HomePlug AV occupied spectrum extends from approximately 1.8 MHz to 30 MHz and is divided into 1155 separately modulated carriers (tones). Not all carriers are used. The active number of carriers is fixed at 917 according to the HomePlug AV specification.

The amplitude of each active carrier is established through hexadecimal values listed in a document named **'prescaler.txt'**. This file is referred to as the 'Amplitude Map' and contains two columns of numbers.

**Tone Index Column**
The first (left-hand) column is the tone index, a list of all 1155 tones in decimal numerical order. The actual frequency of any tone can be determined as follows:

**Frequency (MHz) = (Tone Index + 74) / 40.96**

**Examples:** Tone Index = 0 and frequency = 1.806MHz, Tone Index = 1154 and frequency = 29.98MHz

**Prescale Value Column**
The second column is the assigned amplitude, or prescale, value expressed in hexadecimal. The amplitude of a carrier (tone) is set, or changed, by entering an hexadecimal prescale value next to the tone index number, with one space separation. The hexadecimal value is derived from the desired amplitude level in decibels according to this formula:

**Decibels = 20 log(prescale value/256)**

Resolve this formula for the 'prescale value':

**Prescale value = 256 [ Inverse log ( Decibels/20 ) ]**

The prescale value obtained from the above formula is in decimal form and must be converted to hexadecimal before it is entered into the prescaler.txt file.

Note that the prescale value is a numerical value that represents the tone's amplitude relative to 256. For example: a prescale value of 128 (decimal) indicates that the amplitude is 128/256 = a multiplication factor of 0.5, which means the tone's power level is half of the reference level, or -6 dB (6 dB below the reference level). The maximum decimal range for the prescale value is from 0 to 511 (H1FF).

***Caution***
Any modification to the tone amplitude map (the prescaler.txt file) must be done with caution. The default values in the prescaler.txt file have been established to optimize the performance of the Intellon corded Ethernet adapter (RD6000-ETH Reference Design). Tones in the default Amplitude Map that have a prescaler value of 00000000 are HomePlug AV masked tones – these values must not be changed or the file will not be read by the Device Manager. Additional tones can be shut off by entering 00000000 next to the desired tone index in the prescaler.txt file. However, other than turning off additional tones, it is not advisable to experimentally change the amplitudes of tones from their default values.

**Examples Table**

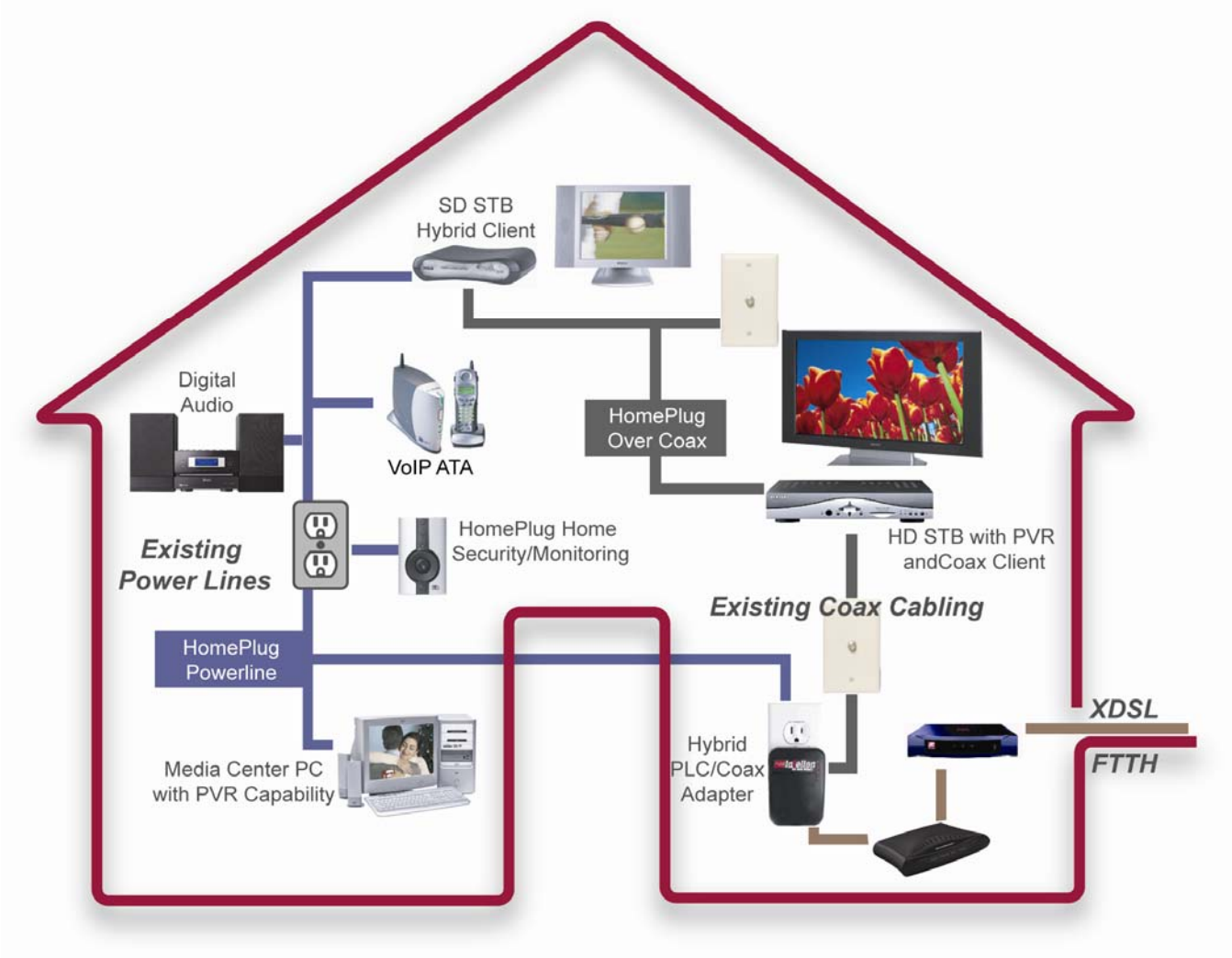
| Prescale Value (Decimal) | Hexadecimal | Relative Amplitude PV/256 | dB |
|---|---|---|---|
| 511 | 000001FF | 2 | +6 |
| 308 | 00000134 | 1.2 | +1.6 |
| 256 | 00000100 | 1 | 0 |
| 64 | 00000040 | 0.25 | -12 |
| 26 | 0000001A | 0.1 | -20 |
| 1 | 00000001 | 0.004 | -48 |
| 0 | 00000000 | 0 | *Off (-30 dB Notch) |

*A value of 0 turns the tone off with a maximum notch depth of -30 dB due to adjacent tones and noise floor.

The default tone amplitude map is contained in the PIB. Changes to the amplitude map in the prescaler.txt file are read and loaded into the PIB by the AVitar.

# Appendix B: Acronyms and Abbreviations

| | |
|---|---|
| **API** | Application Programming Interface |
| **AVLN** | HomePlug AV Logical Network |
| **CAP** | Channel Access Priority |
| **CCo** | Central Coordinator |
| **CSMA/CA** | Carrier Sense Multiple Access / Collision Avoidance |
| **DSCP** | Differentiated Services Code Point |
| **GUI** | Graphical User Interface |
| **HLE** | Higher Layer Entity |
| **IGMP** | Internet Group Management Protocol |
| **MAC** | Medium Access Controller |
| **MII** | Media Independent Interface |
| **MME** | Management Message Entry |
| **NEK** | Network Encryption Key |
| **NID** | Network ID (Identification) |
| **NMK** | Network Management Key |
| **NVRAM** | Non-Volatile Random Access Memory |
| **PCI** | Peripheral Component Interconnect |
| **PHY** | Physical |
| **PIB** | Parameter Information Block |
| **SDK** | Software Development Kit |
| **STA** | Station |
| **TDMA** | Time Division Multiple Access |
| **TEI** | Terminal Equipment Identifier |
| **TOS** | Type Of Service |
| **TTL** | Time To Live |
| **VLAN** | Virtual Local Area Network |




InTellon® NO NEW WIRES.
HOMEPLUG POWERLINE ALLIANCE
Founding Member

**Corporate Headquarters**
5955 T.G. Lee Blvd.
Suite 600
Orlando, FL 32822
(407) 428-2800
(407) 428-2850 (Fax)

**Ocala Office**
5100 West Silver Springs Blvd.
Ocala, FL 34482
(352) 237-7416
(352) 237-7616 (Fax)

**San Jose Office**
1731 Technology Drive
Suite 560
San Jose, CA 95110
(408) 501-0320
(408) 501-0323 (Fax)

**Toronto Office**
144 Front Street West,
Suite 385
Toronto, Ontario M5J 2L7
(416) 217-0451
(416) 217-0459 (Fax)

© 2009 Intellon Corporation. The information contained in this document is provided "AS IS". Intellon reserves the right to make changes to this document and to any products without notice. INTELLON MAKES NO WARRANTY, REPRESENTATION OR GUARANTEE OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING REGARDING THE CAPABILITY, PERFORMANCE OR SUITABILITY OF ITS PRODUCTS FOR ANY PARTICULAR PURPOSE. INTELLON ASSUMES NO RESPONSIBILITY OR LIABILITY ARISING OUT OF THE APPLICATION, THE USE OF ANY PRODUCT, THE USE OF ANY INFORMATION CONTAINED IN THIS DOCUMENT, OR FOR ANY INFRINGEMENT OF PATENTS OR OTHER INTELLECTUAL PROPERTY RIGHTS OWNED BY THIRD PARTIES. INTELLON SPECIFICALLY DISCLAIMS ANY AND ALL LIABILITY, INCLUDING WITHOUT LIMITATION, CONSEQUENTIAL OR INCIDENTAL DAMAGES. CERTAIN APPLICATIONS OR EQUIPMENT MAY BE SUBJECT TO REGULATORY REQUIREMENTS. INTELLON DISCLAIMS AND MAKES NO GUARANTEE OR WARRANTY, EXPRESS OR IMPLIED, THAT A PRODUCT WILL COMPLY WITH ANY SUCH REGULATORY REQUIREMENTS. All products are sold and services provided subject to Intellon's standard terms and conditions of sale, which are available on request.

Intellon and No New Wires are registered trademarks of Intellon Corporation. HomePlug is a registered trademark of the HomePlug Power line Alliance. All other trademarks are the property of their respective owners.