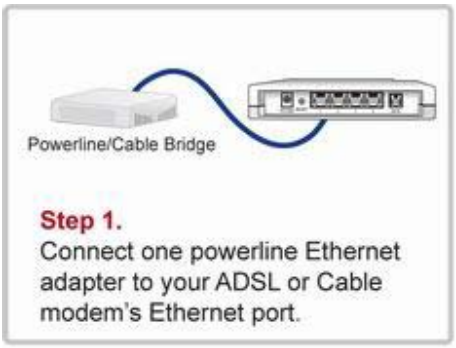
User’s Manual

(For SI/ engineer)

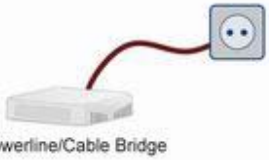
Powerline/Cable 500M Bridge

1. Powerline Networking Installation

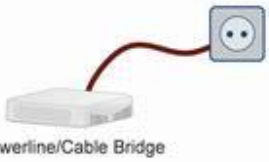
1.1 Simple step to install Powerline Networking



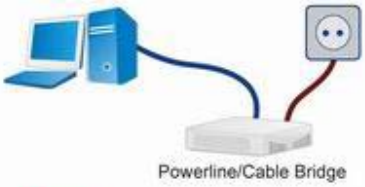
Step 1.
Connect one powerline Ethernet adapter to your ADSL or Cable modem's Ethernet port.



Step 2.
Plug it into the nearest power socket.



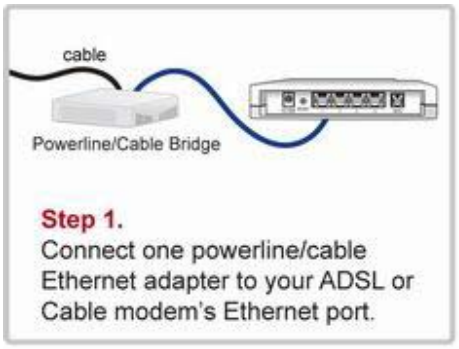
Step 3.
Plug in the second Powerline Ethernet adapter next to your PC & connect the Ethernet ports.

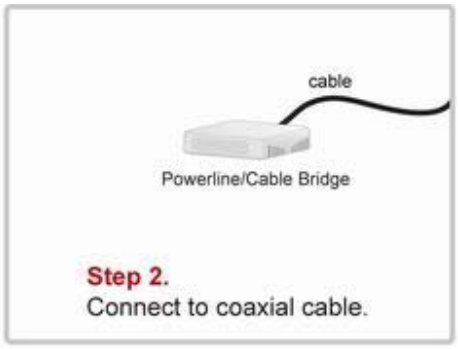


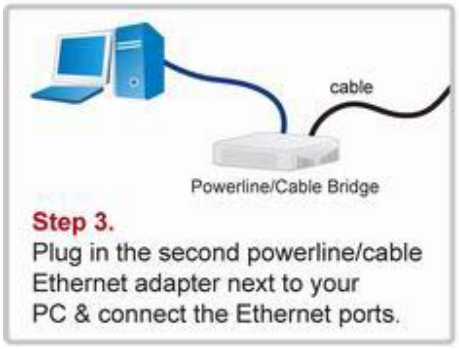
Step 4.
Internet access from any power socket in your home.

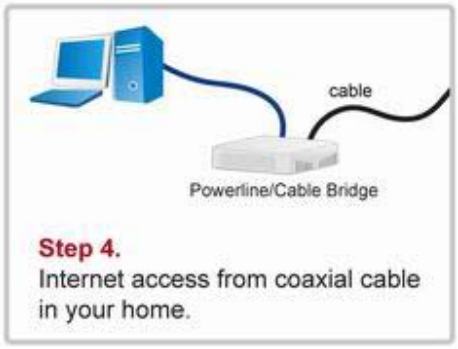
1.2 Simple step to install Powerline/Cable Networking

(User can connect to Powerline/Cable simultaneously, the device will auto select to the best performance to transfer data, be sure the switch set in PL/Cable mode)



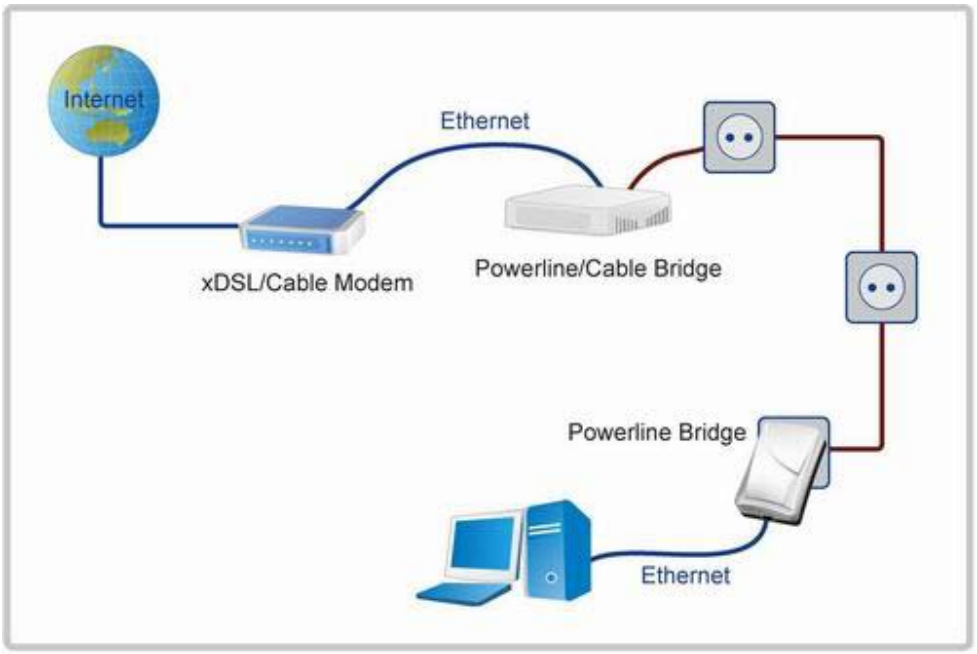




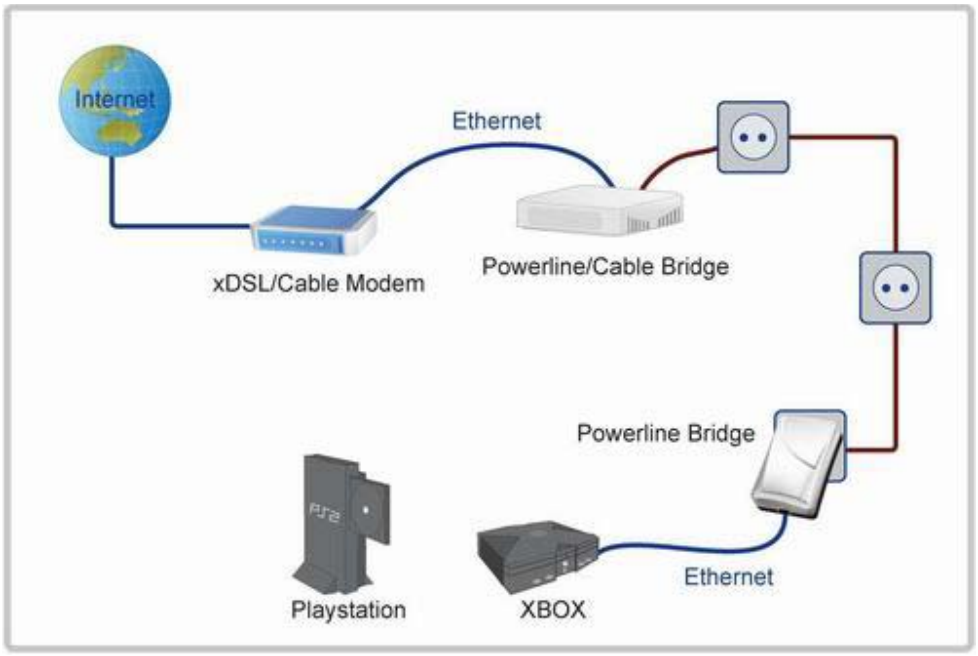


1.3 Application Block Diagram

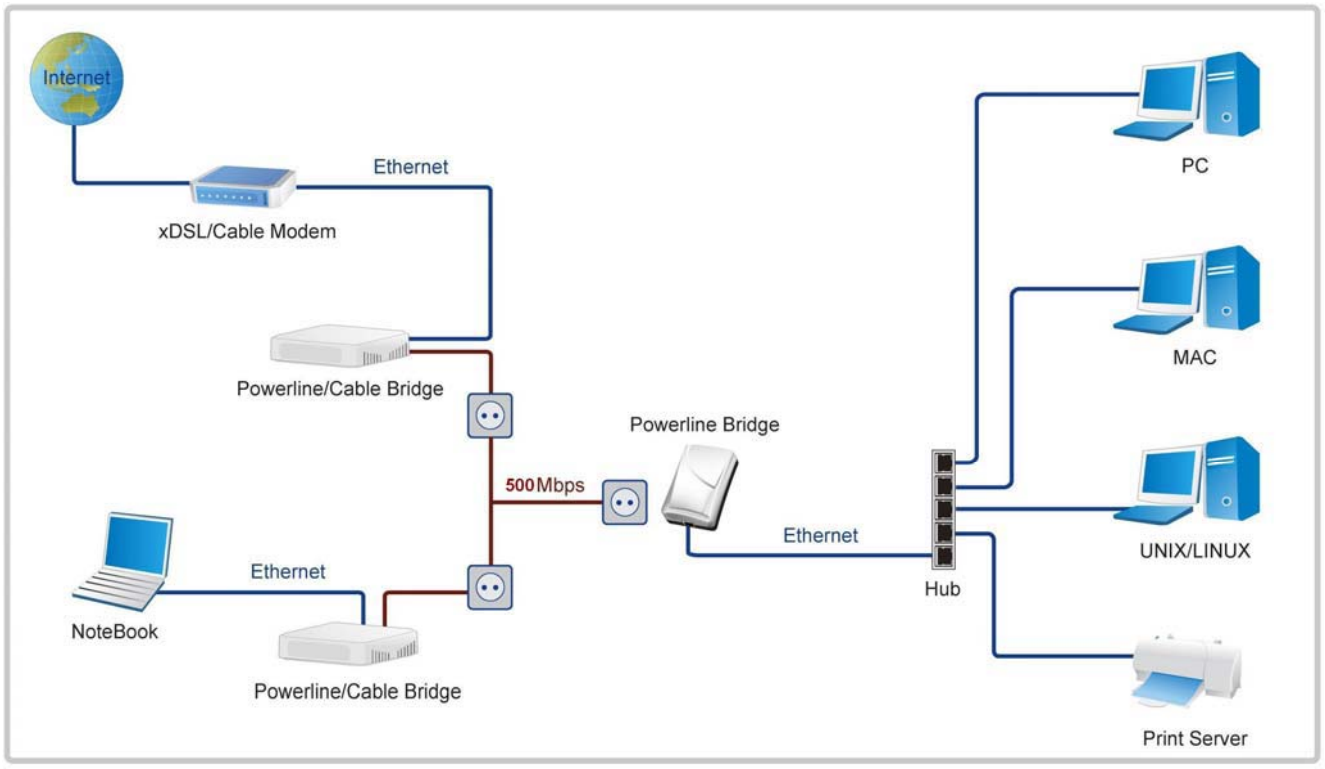
1.3.1 Internet ADSL with one computer via power outlet (Switch in PL/Cable side)



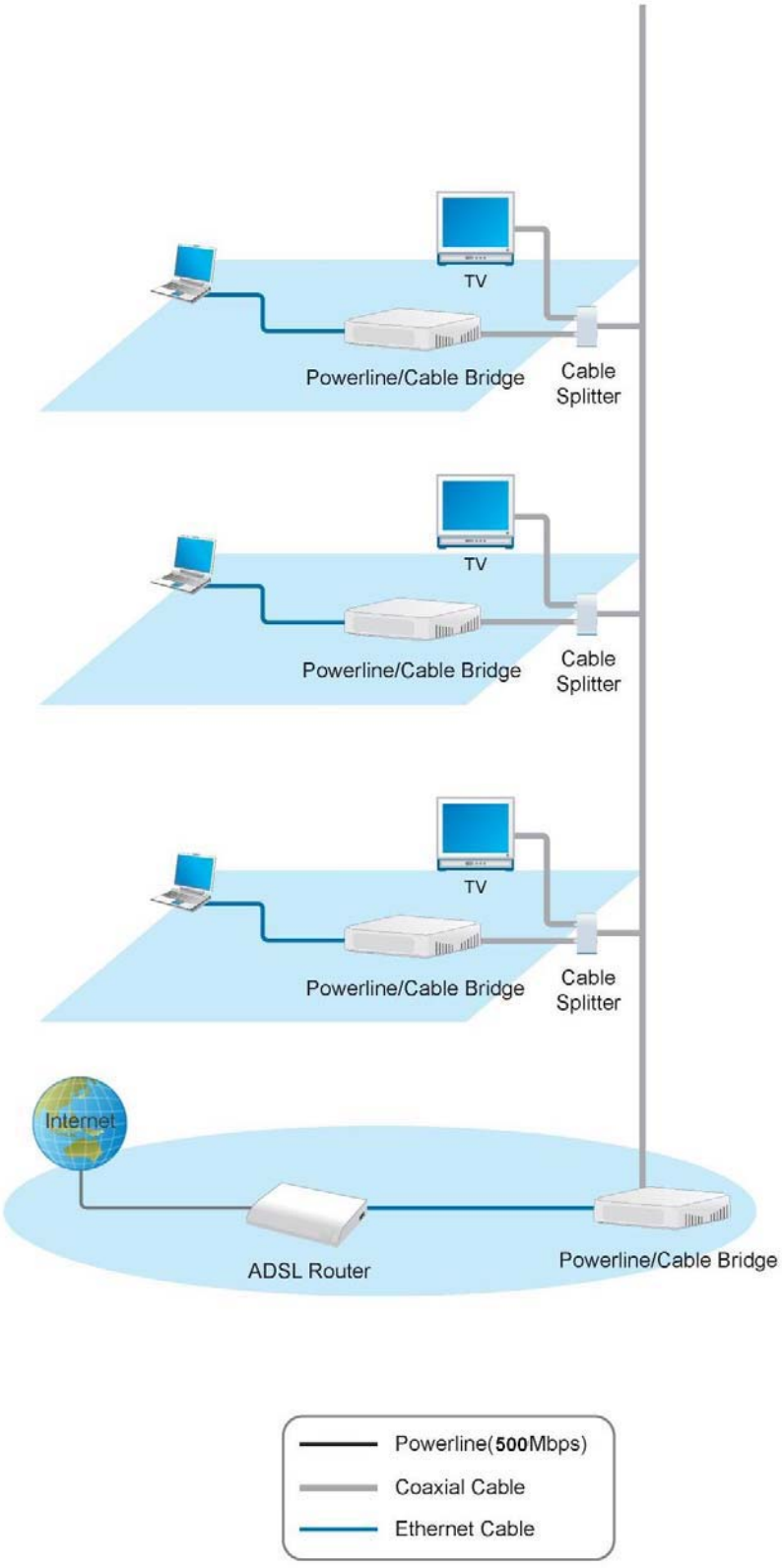
1.3.2 Online game via power outlet (Switch in PL/Cable side)



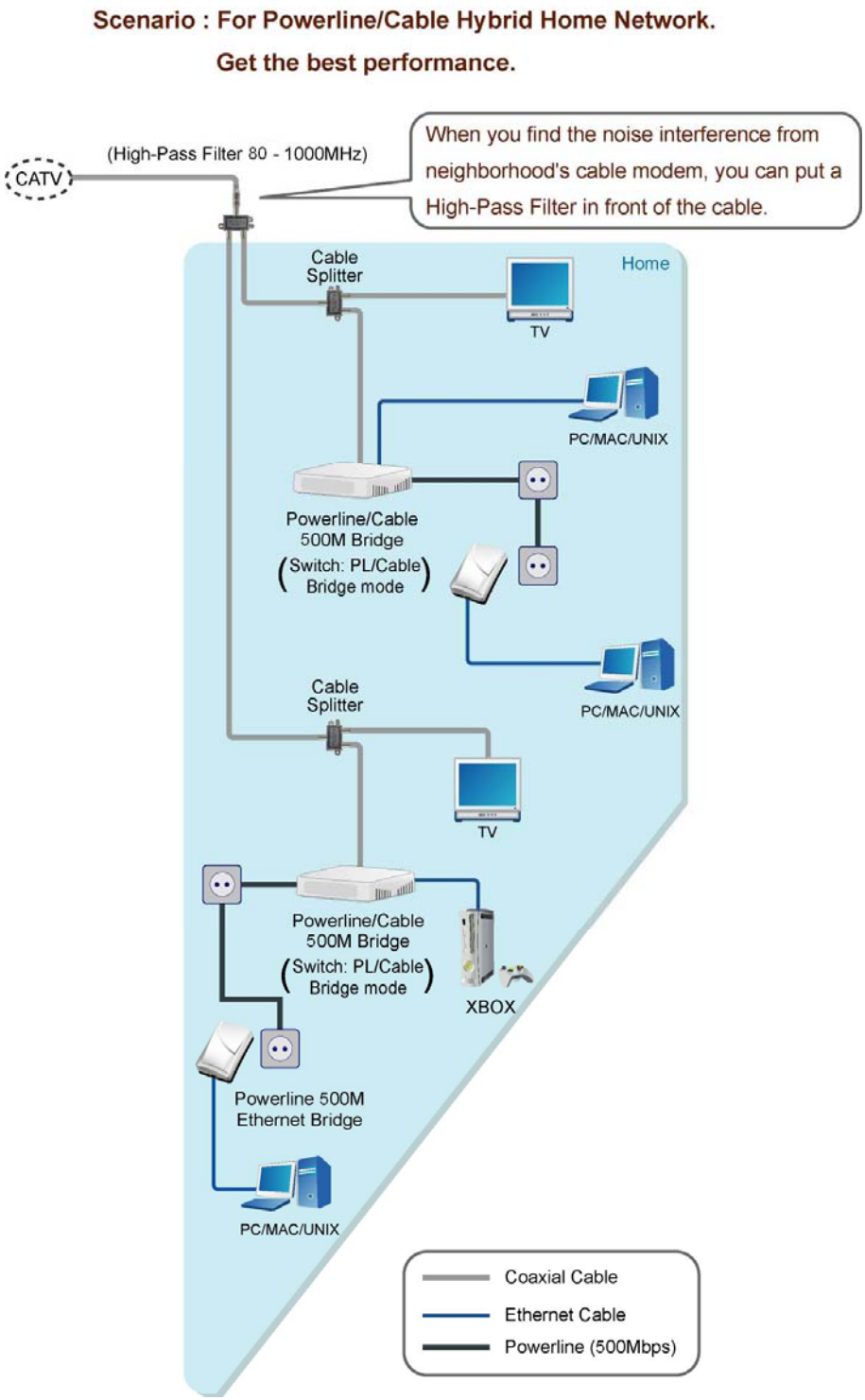
1.3.3 Internet ADSL and Home Networking via power outlet (Switch in PL/Cable side)



1.3.4 Internet ADSL and Home Networking via coaxial cable (Bridge mode) (Switch in Cable only side)



1.3.5 Internet ADSL and Home Networking for Powerline/cable device hybrid mode (Bridge mode) (Switch in PL/Cable side)



1.4 Benefits

- Data transfers at up to 500 Mbps over the household power circuit or coaxial cable
- Ranges of 200 meters
- No need new wires for Home networking
- Deliver the benefits of Ethernet without the wiring expense
- Send even large files between PCs without long waits
- High-speed Internet and DVD-quality video streaming
- Fully compliant with IEEE 802.3, IEEE 802.3u and IEEE 802.3ab
- Privacy through AES encryption

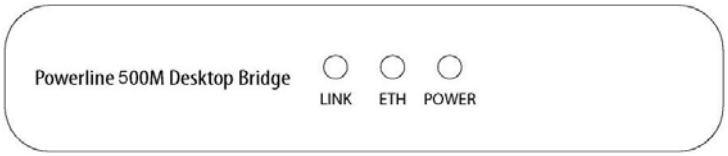
1.5 Features

- Use the home's existing Powerline or coaxial cable
- Support coexist with Powerline 85M or 14M bridges
- Easy to install
- Throughout the whole house, just use your power circuit to access the Internet or PC network
- Orthogonal Frequency Division Multiplexing for high data reliability in noisy media conditions
- Integrated Enhanced Quality of Service(QoS) features: Eight levels of prioritized random access, contention free access, and segment bursting
- Up to 500Mbps data rate on Powerline or coaxial cable
- Provide 128-bit AES Link Encryption with key management for secure Powerline communications
- Master/Slave mode support (coaxial cable link only)
- Up to 252 slaves with 1 master, 253 total devices for cable link
- Up to 4096 addressable devices including bridged devices
- Support IEEE 802.3af PoE PD. (option)

1.6 Package Contents

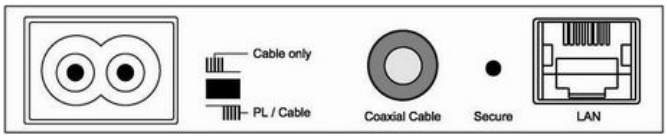
- Powerline/Cable 500M Ethernet Bridge unit
- Quick Installation Guide
- Category 5 cable

1.7 The Front LEDs



LED	State	Description
LINK	ON	Powerline network activity.
	OFF	Search or no Powerline network activity.
ETH	ON	Ethernet connection is OK.
	Flashing	Data transfer.
	OFF	No link to Ethernet.
POWER	ON	Power on.
	OFF	Powerline off or failure.

1.8 The Rear Ports



Connector	Description
POWER	Connect to power cord.
Coaxial Cable	Connect to coaxial cable. Be sure, in some countries or Europe, the coaxial connector is different so user need to buy extra converter to link the device to the internal TV cable not the satellite cable.
switch	Switch to cable only mode or Powerline/Cable mode, when switch to cable only, the Powerline function will be disable. When switch to Powerline/cable, it can enable both, so just don't connect to the coaxial cable, it can use as Powerline device.
LAN	Router is successfully connected to a device through the corresponding port. If the LED is flashing, the Router is actively sending or receiving data over that port.
Secure/Reset	Button can auto secure and group the Powerline devices. Press 2 seconds to auto secure. Press 10 seconds to generate random encryption key. Press 15 seconds to restore default settings.

※ The Europe TV connector is different type, like the picture 1.8.1. So user need to have the converter(picture 1.8.2) to connect the coaxial cable to the TV cable connector on the wall, don't connect the device to the satellite connector, it will not work.

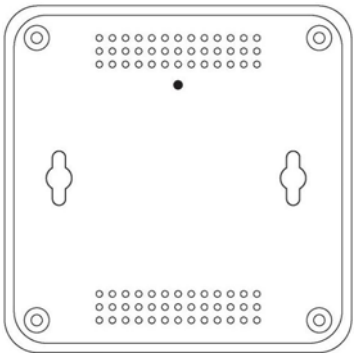
In some countries or in Europe use different TV connector for coaxial cable.

Picture 1.8.1

Use this converter to connect to the coaxial cable and then connect to the TV connector on the wall.

Picture 1.8.2

1.9 The Bottom Port



1.10 System Requirements

- Ethernet device
- AC power outlet
- Cable link
- Windows system for setup utility

2. Push Button Setting

There is a buttons in this device, it has two functions, one is Reset the other is Secure.

Reset: Push this button can reset to the factory default settings. **Be careful, when you press the reset button, please make sure unplug (remove) the Ethernet cable (RJ-45cable) first, and then press the reset button. After press the reset button (the time need > 15 sec) and then wait the PWR LED light again. Don't power off when the device is in reset process.**

Secure button can auto secure and group the Powerline devices, the follow is the scenario for secure button.

Two Push Button trigger state conditions

"Adder state" for a device providing the NMK for an existing AVLN

"Joiner state" for a device that will join an AVLN

Pushing buttons on any two devices results in one of them becoming an "adder" and the other one a "joiner"

Three possible scenarios

Unassociated device joining an existing AVLN

– Two Unassociated devices joining to form a new AVLN
– Special case: one device is a CCo, the other is a STA

Two Associated devices joining to form an AVLN with a new NMK

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 Microsoft® Windows XP©, Microsoft Vista© and Microsoft Windows7©.
3. Before installing a new version of AVitar, you must manually remove the previously installed version of AVitar using the Microsoft Windows© Add or Remove Programs application.
4. Double click on the installer.bat file and follow the installation wizard through the installation process.
5. AVitar uses the .NET Framework version 3.5. The AVitar installer will automatically install .NET framework version 3.5 if it detects that it is not installed.
6. Launch the AVitar by double clicking on avitar.exe.
7. The installation is now complete.

NOTE: If user is running AVitar v4.3.1.01, it must be manually uninstalled before installing AVitar v5.2.0. Minimum screen resolution must be 1280 x 800. For Windows7, DPI settings must be 100%.

3.2 Common Features of Tabbed Windows

3.3 About Tab

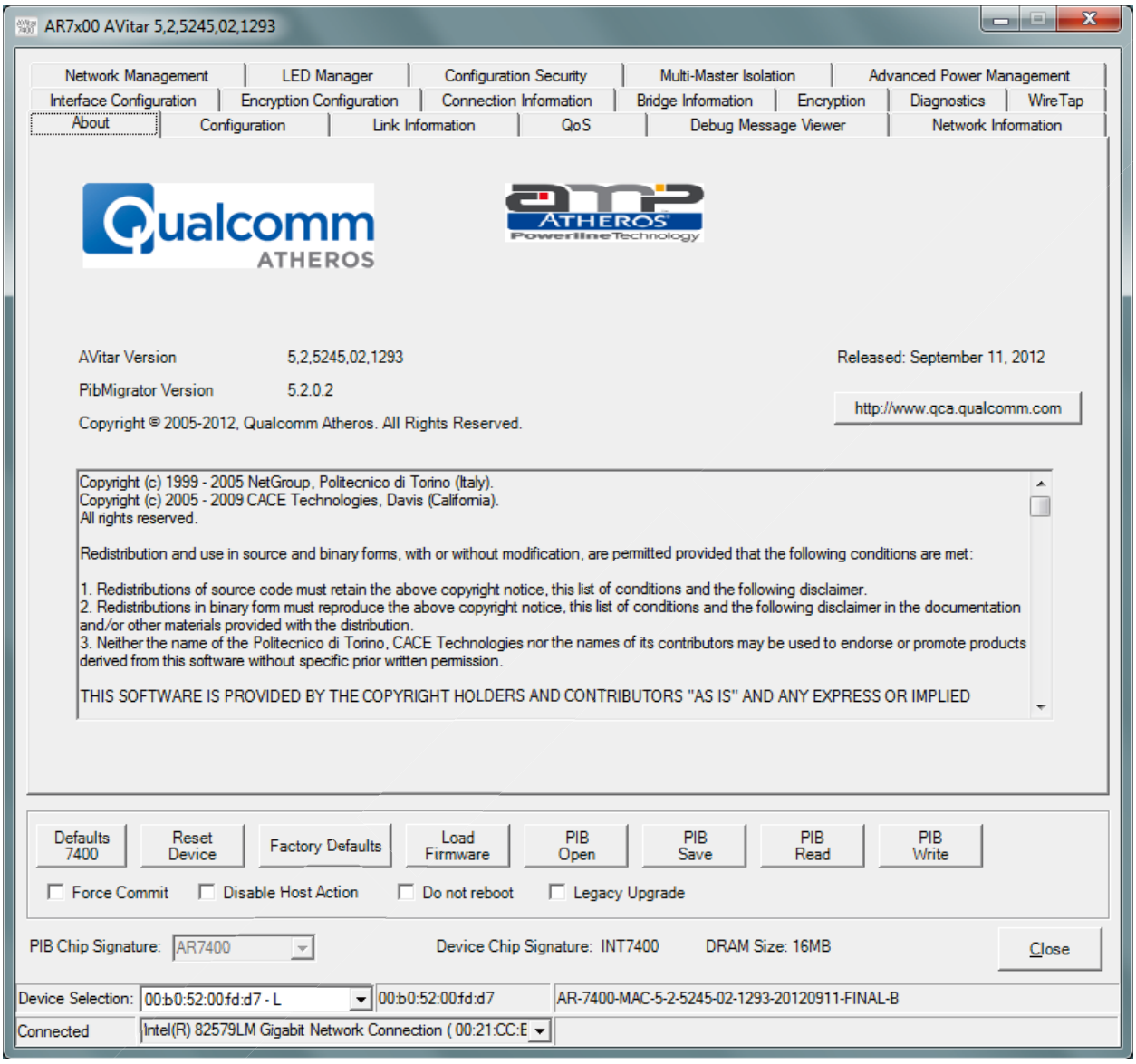


Figure 3-1: About Tab

3.4 Network Interface Cards (NIC) Selector

As shown in Figure 3-2, 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.

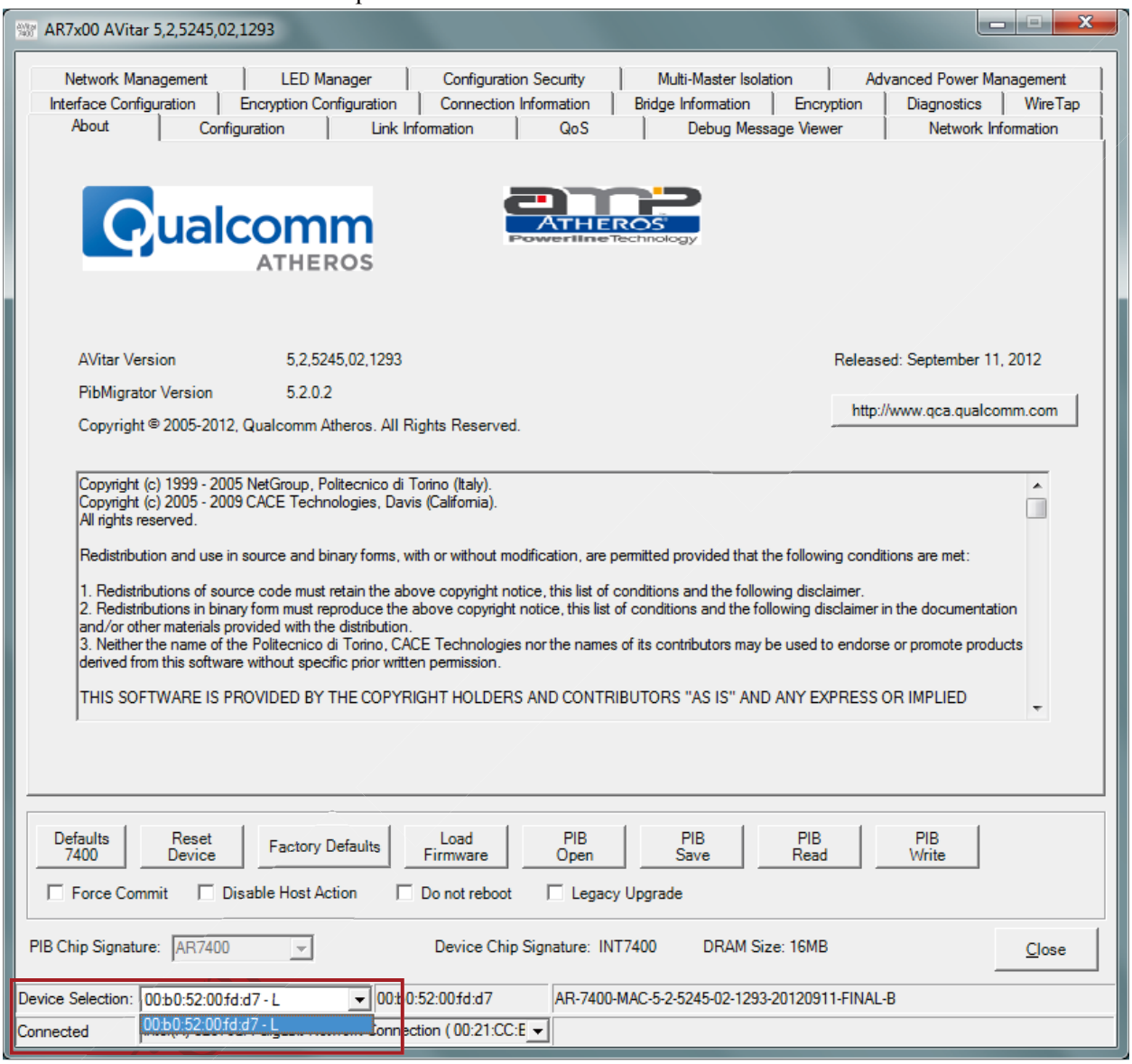


Figure 3-2: Viewing and Selecting a Network Interface Card

3.5 Configuration Tab *(Configuration Window)*

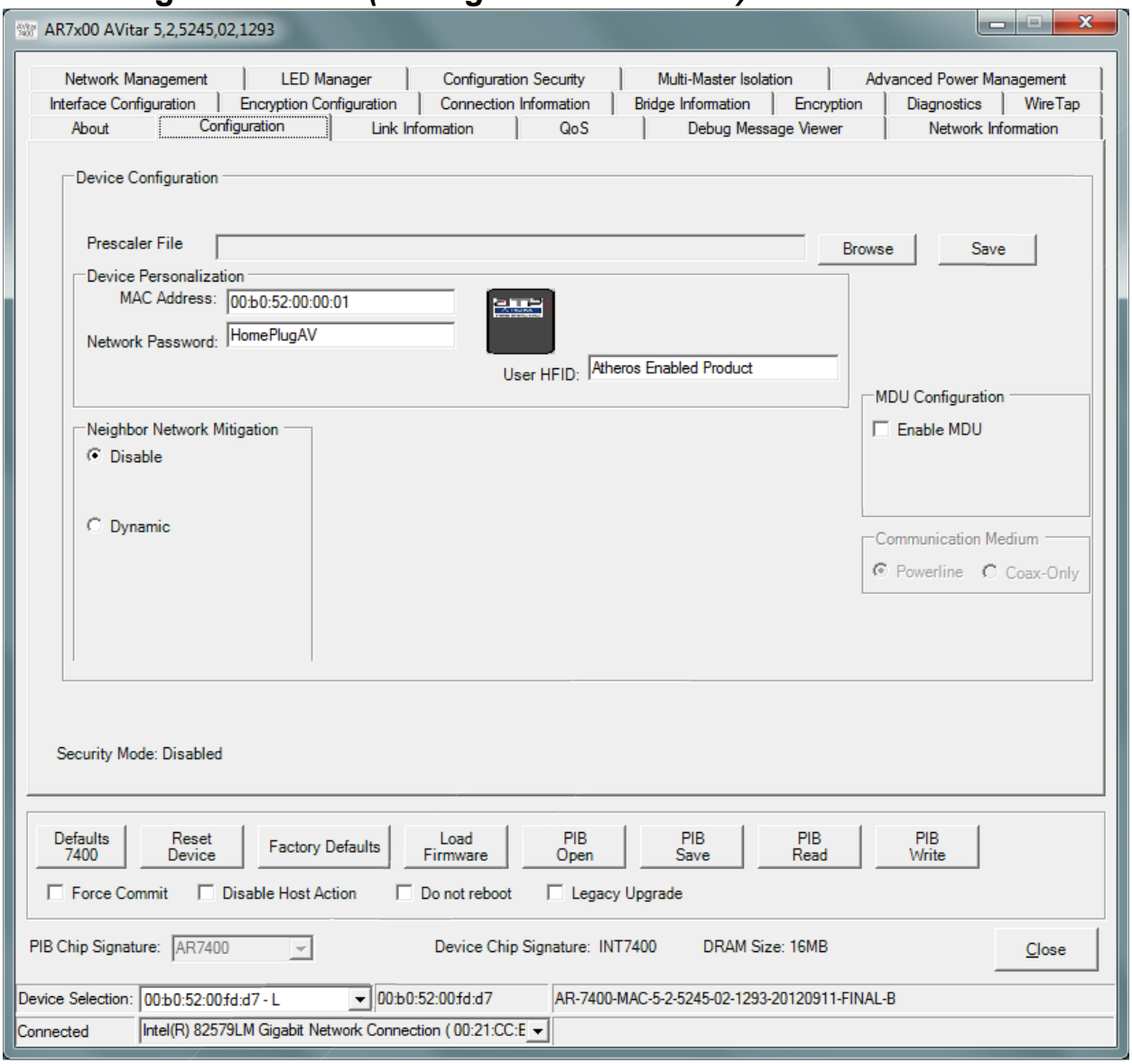


Figure 3-3: Configuration Tab Window

3.5.1 Configuration Fields

The AVitar GUI tabbed window labeled 'Configuration' is shown in Figure 3-3. 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.

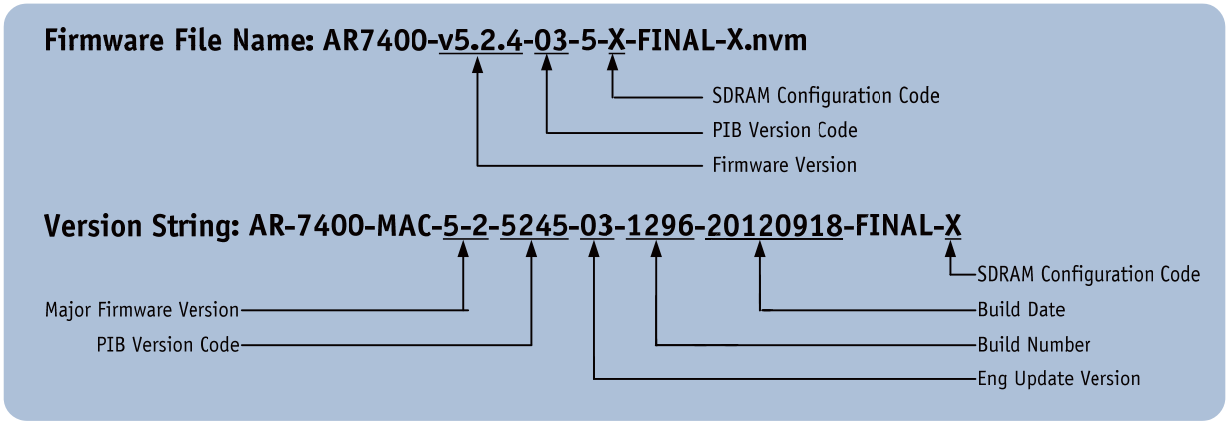


Figure 3-4: AR7400 Firmware and Version Strings

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.

3.5.2 Prescaler File Selection

Browse buttons are used to locate the Prescaler files.

3.5.3 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.

3.5.3.1 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.

3.5.4 Configuration Checkboxes

3.5.4.1 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.

3.5.4.2 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 DRAM configuration. Based on the user's selection of the DRAM size, which is chosen with the new *DRAM Size* drop-down, one of two DRAM configuration files will be downloaded to the Bootloader. This will happen automatically, evidenced by "DRAM Config updated" message in the bottom right status box. The two configuration files, each associated with 16M or 64M DRAM sizes are provided by Qualcomm Atheros 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 DRAM 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.

3.5.4.3 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.

NOTE: May take up to 3 minutes for the algorithm to converge, additionally these values are not stored to flash. Subsequent reboots will restart the algorithm.

3.5.4.4 Device Action Buttons

- **Defaults:** Loads default PIB values into AVitar's current working PIB.

NOTE: Clicking the Defaults button will load in a non-compliant set of pre-scalars. To load a compliant set of pre-scalars (e.g. North American Wall Plug) use the "Open" button in the PIB group to read in the PIB with the correct set of pre-scalar.

- **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.

3.5.4.5 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.
- **Legacy Upgrade Checkbox:** Performs FW upgrade using the legacy method of overwriting Factory Default PIB with supplied PIB, except essential parameters (Manufacturing HFID, DAK, NVAK, MAC Address, NMK, TR-069 parameters). If unchecked (default), FW upgrade will overlay Factory Default PIB on the supplied PIB.

3.5.4.6 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.

3.6 Link Information Tab *(Operation Analysis Window)*

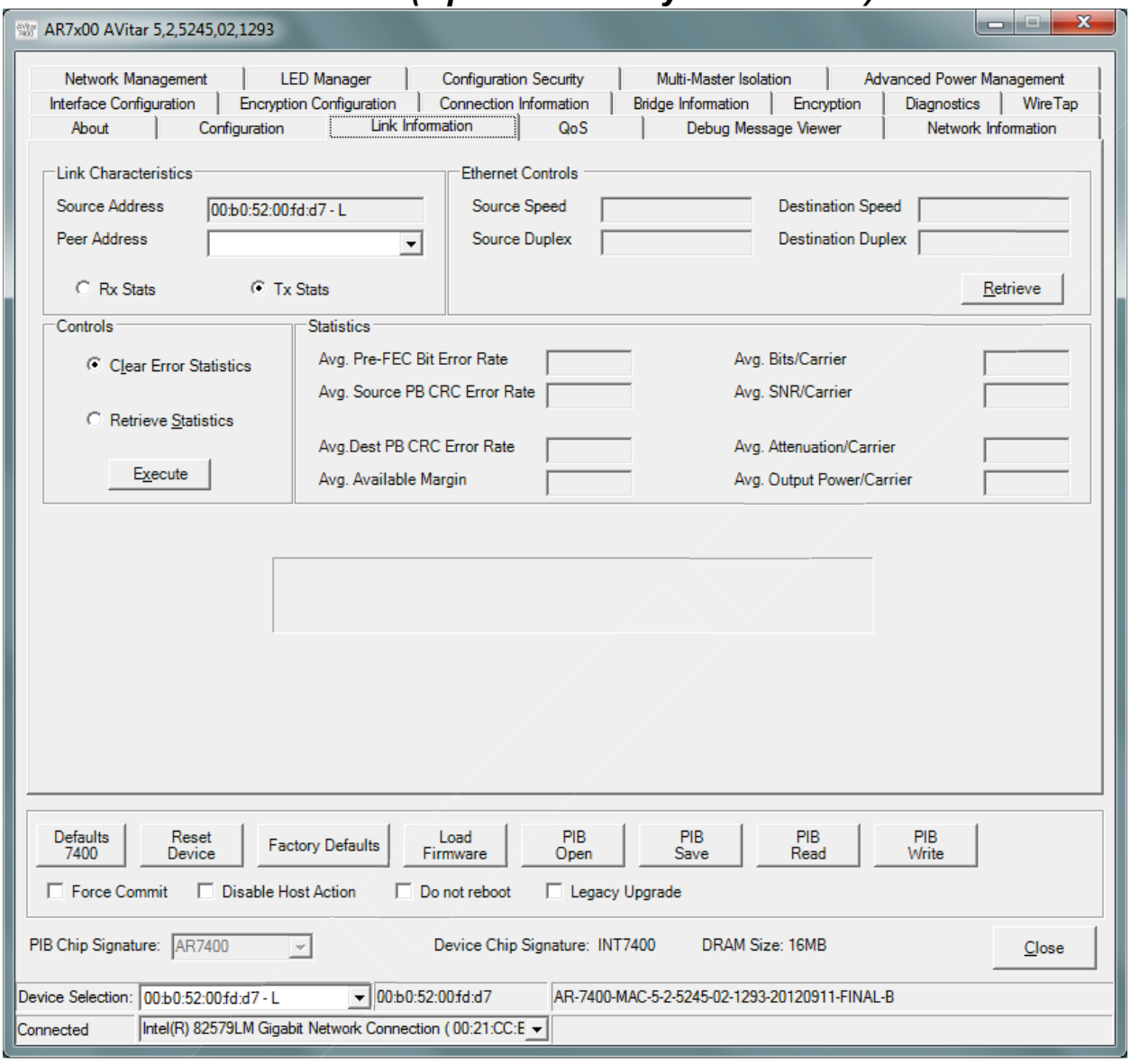


Figure 3-5: Link Information Tab Window

3.6.1 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.

3.6.2 Ethernet Controls

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

3.6.3 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.

3.7 QoS Tab *(Configuration Window)*

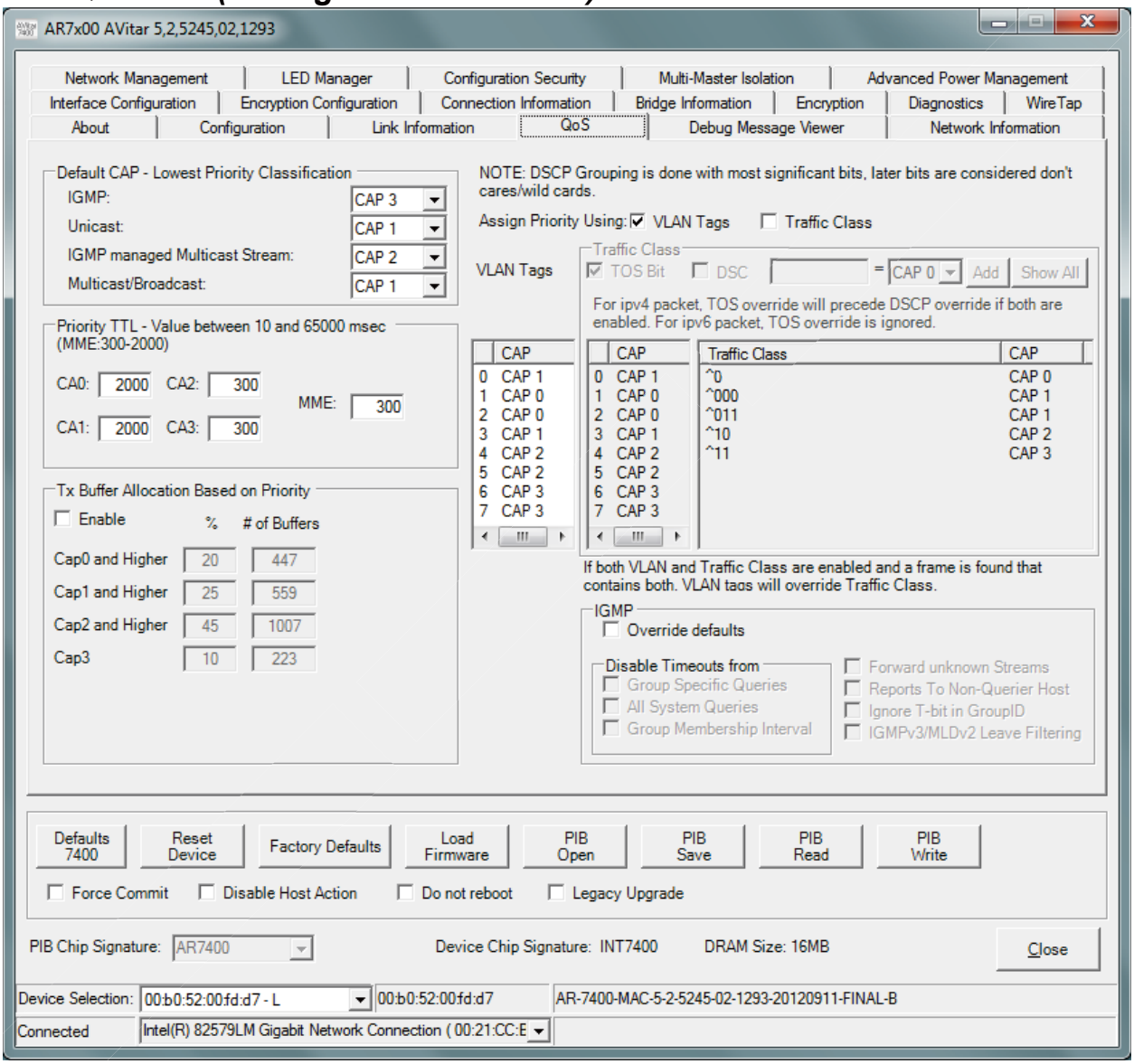


Figure 3-6: QoS Tab Window

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.

3.7.1 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.

3.7.1.1 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 3-6.

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.

3.7.1.2 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.

3.7.2 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.

3.7.3 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.

By default, all IGMPv3 Leave operations (i.e. INCLUDE with an empty source list) will send forward all leave message to the host gateway. An option has been added to the firmware to filter all leave messages from being sent to the host gateway until the last stream is shutdown. This feature is enabled by the IGMPv3/MLDv2 Leave Filtering check box.

3.7.4 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 Qualcomm Atheros Vendor Specific MMEs)

Qualcomm Atheros highly recommends that the 300 msec and 2,000 msec default settings not be changed because they are optimized for the above stated traffic. Qualcomm Atheros 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.

3.7.5 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.

3.8 Debug Message Viewer *(Operation Analysis Window)*

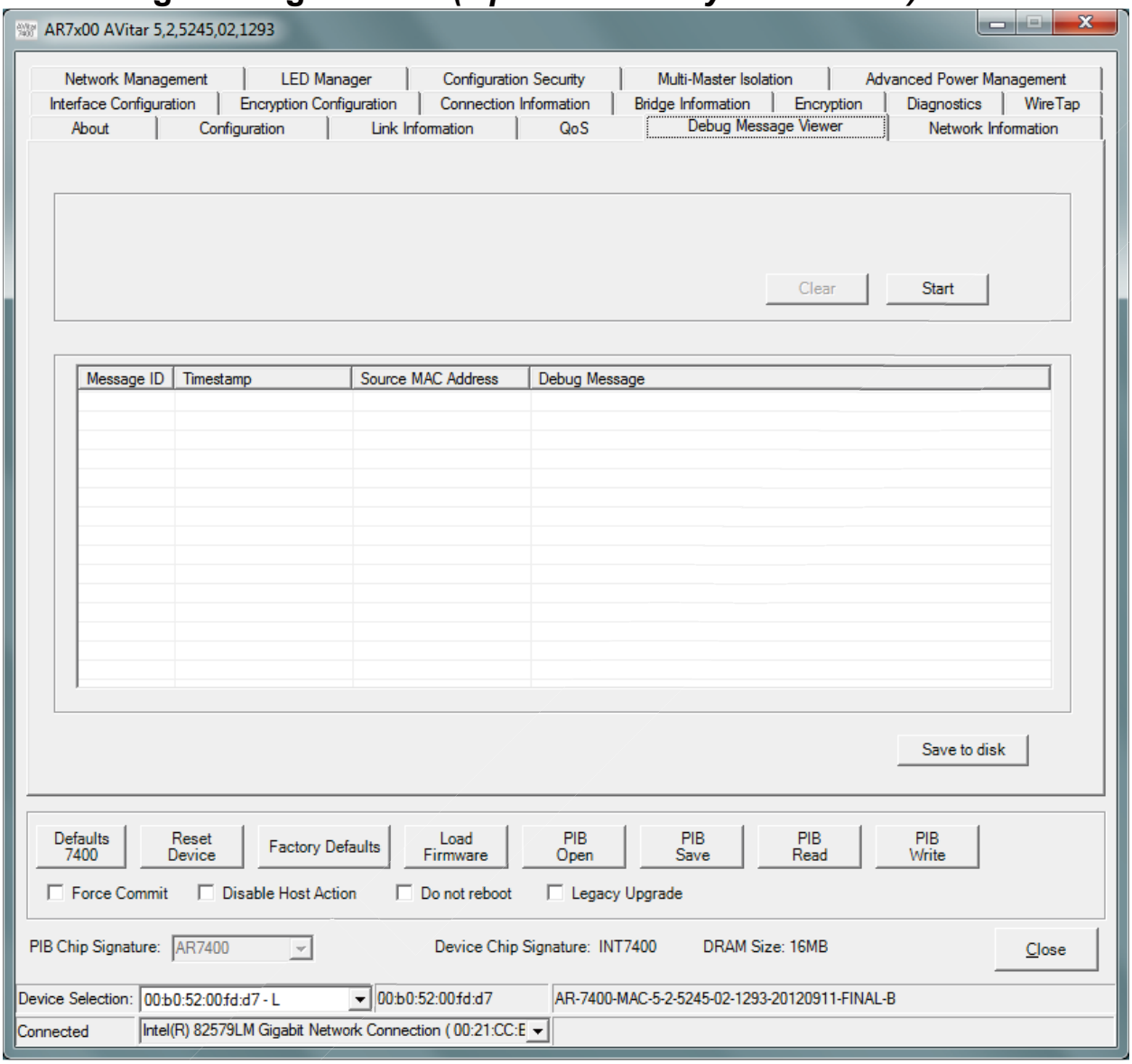


Figure 3-7: Debug Message Viewer Tab Window

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 Qualcomm Atheros 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.

3.9 Network Information Tab *(Operation Analysis Window)*

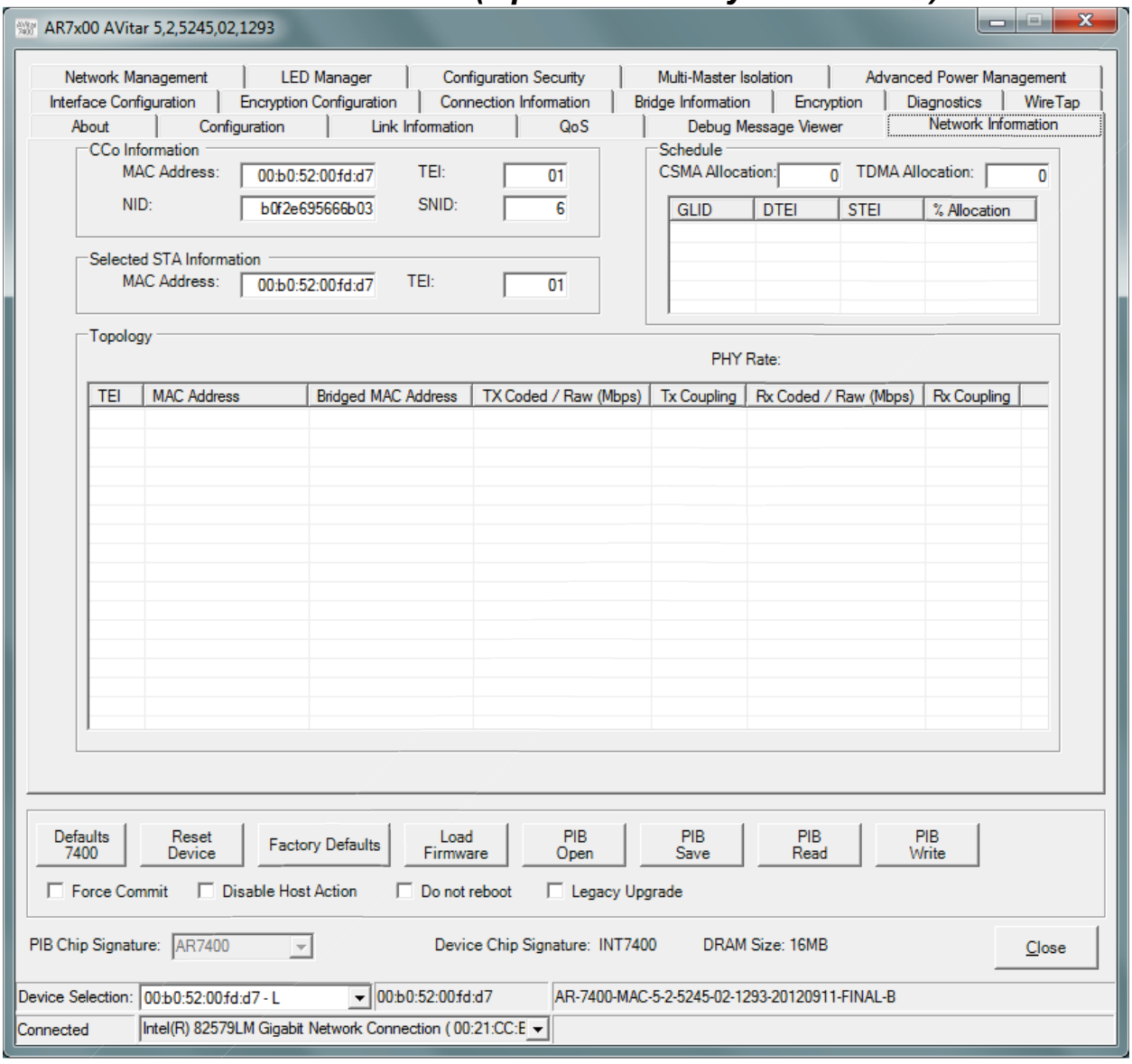


Figure 3-8: Network Information Tab Window

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

3.9.1 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.

3.9.2 Selected Station (STA) Information

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

3.9.3 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).

3.10 Network Management *(Configuration Window)*

The primary purpose of the Network Management section of AVitar is to create the PIB file to be used for provisioning the device. Once the device has been provisioned with a PIB in which TR-069 is enabled, network parameters cannot be modified by writing another PIB.

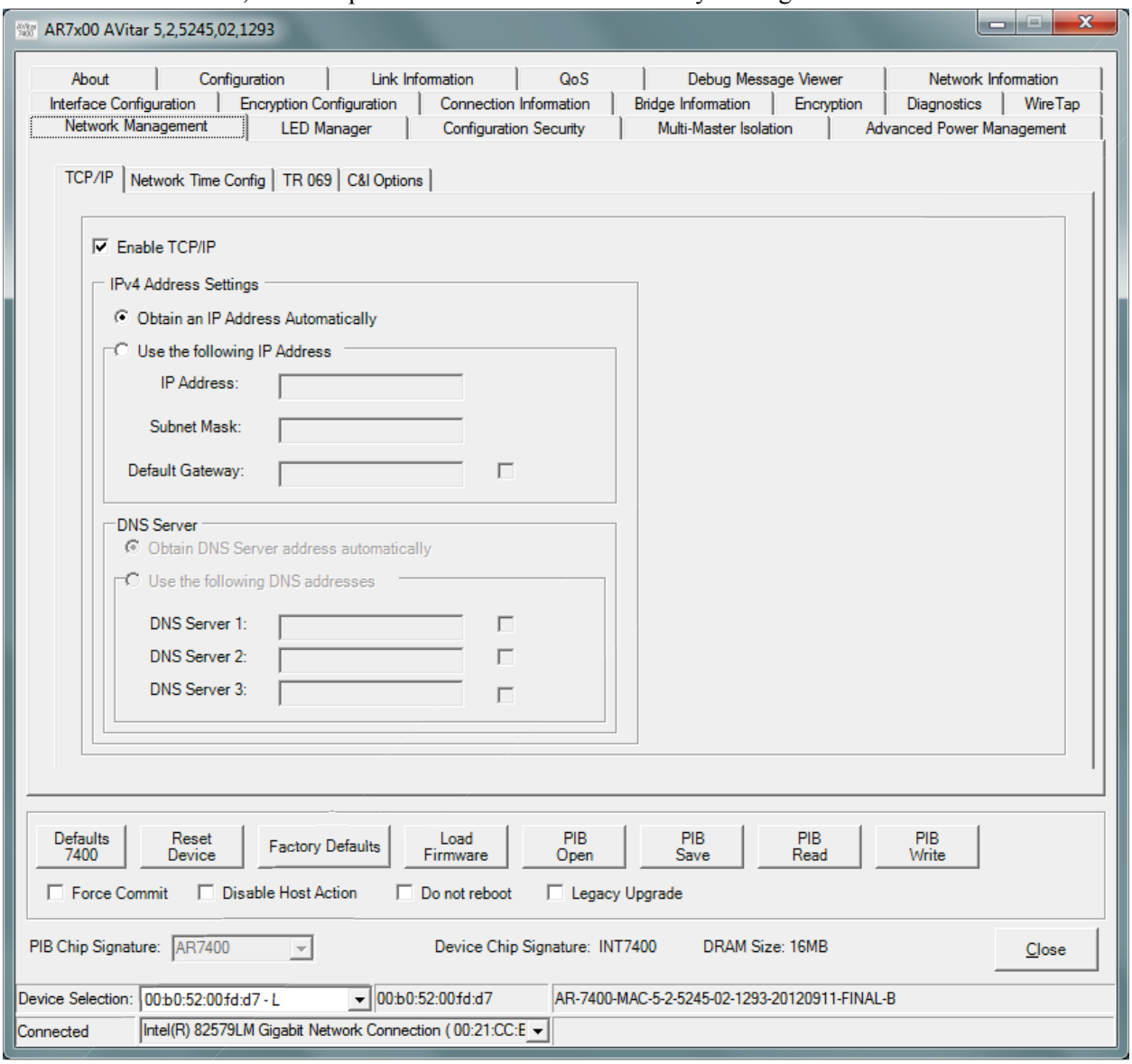


Figure 3-9: DHCP IP Configuration

The Network Management tab allows for configuration of TR-069 parameters. It includes following sub-tabs:

TCP/IP – Configuration tab for TCP/IP parameter details.

Network Time Config – Configuration tab for Network Time Protocol (NTP) server and Time Zone Parameters.

TR 069 – Configuration tab for Auto Configuration Server (ACS) parameters and SSL connection parameters.

3.10.1 TCP/IP Configuration

End users can configure the TCP/IP parameters required for the TCP/IP stack through this tab. This TCP/IP GUI supports configuration for both DHCP IP address as well as Static IP address.

3.10.1.1 Enabling DHCP IP Address

Select the "Network Management" Tab, select the "TCP/IP" sub-tab. Select the "Enable TCP/**IP**" checkbox. Then select the "Obtain an IP Address Automatically" option.

3.10.1.2 Enabling Static IP Address

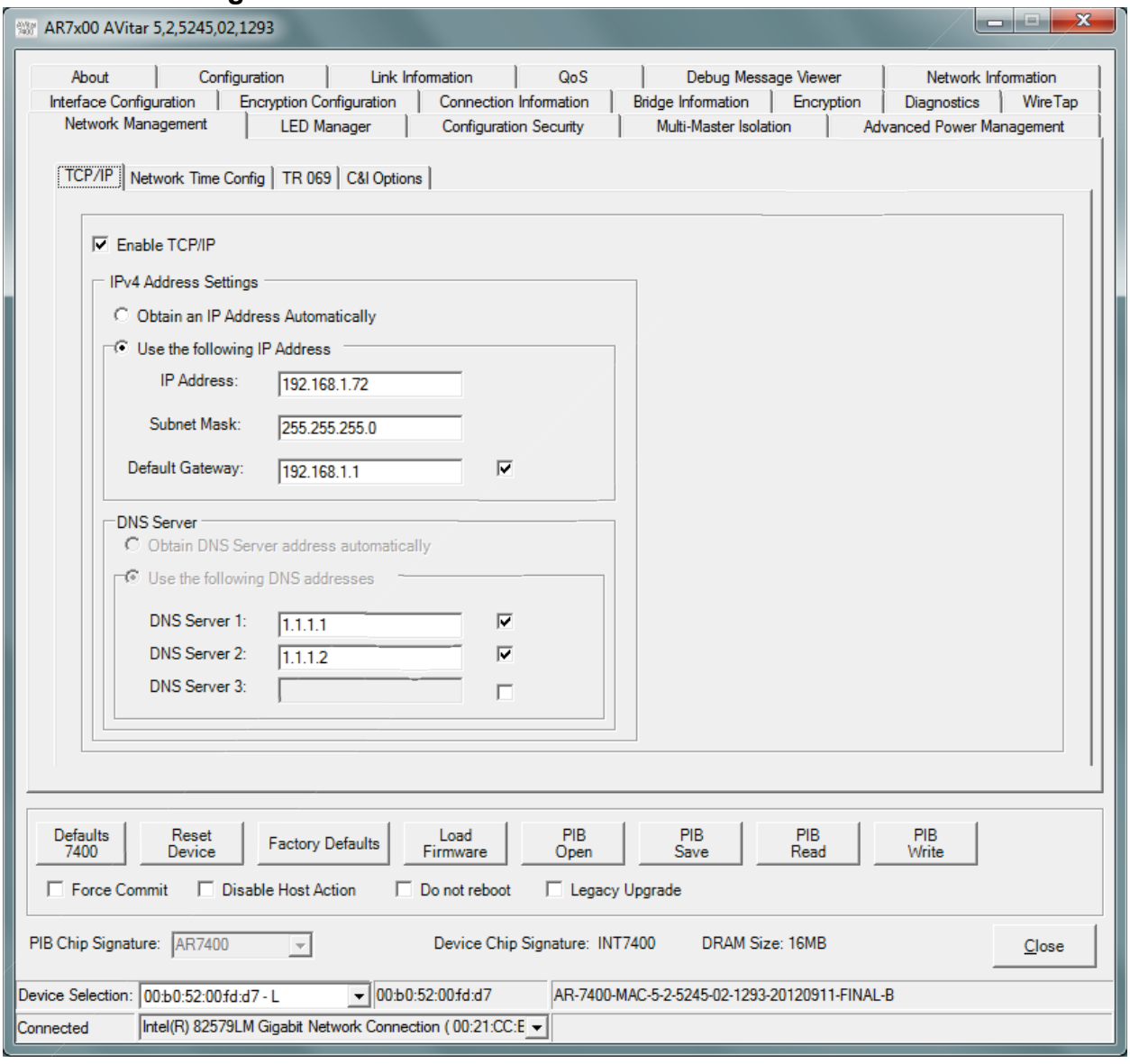


Figure 3-10: Static IP Configurations

Users can configure the Static IP by selecting the "Use the following IP Address" option from the TCP/IP sub-tab. Also, users can configure Default Gateway and DNS Server as part of a static IP configuration.

Also users can enter the "Default Gateway" and "DNS Server" address when using the static IP configuration option. The usage of these configuration addresses are controlled by the enable (checked) or disable (unchecked) checkbox.

3.10.2 Network Time Configuration

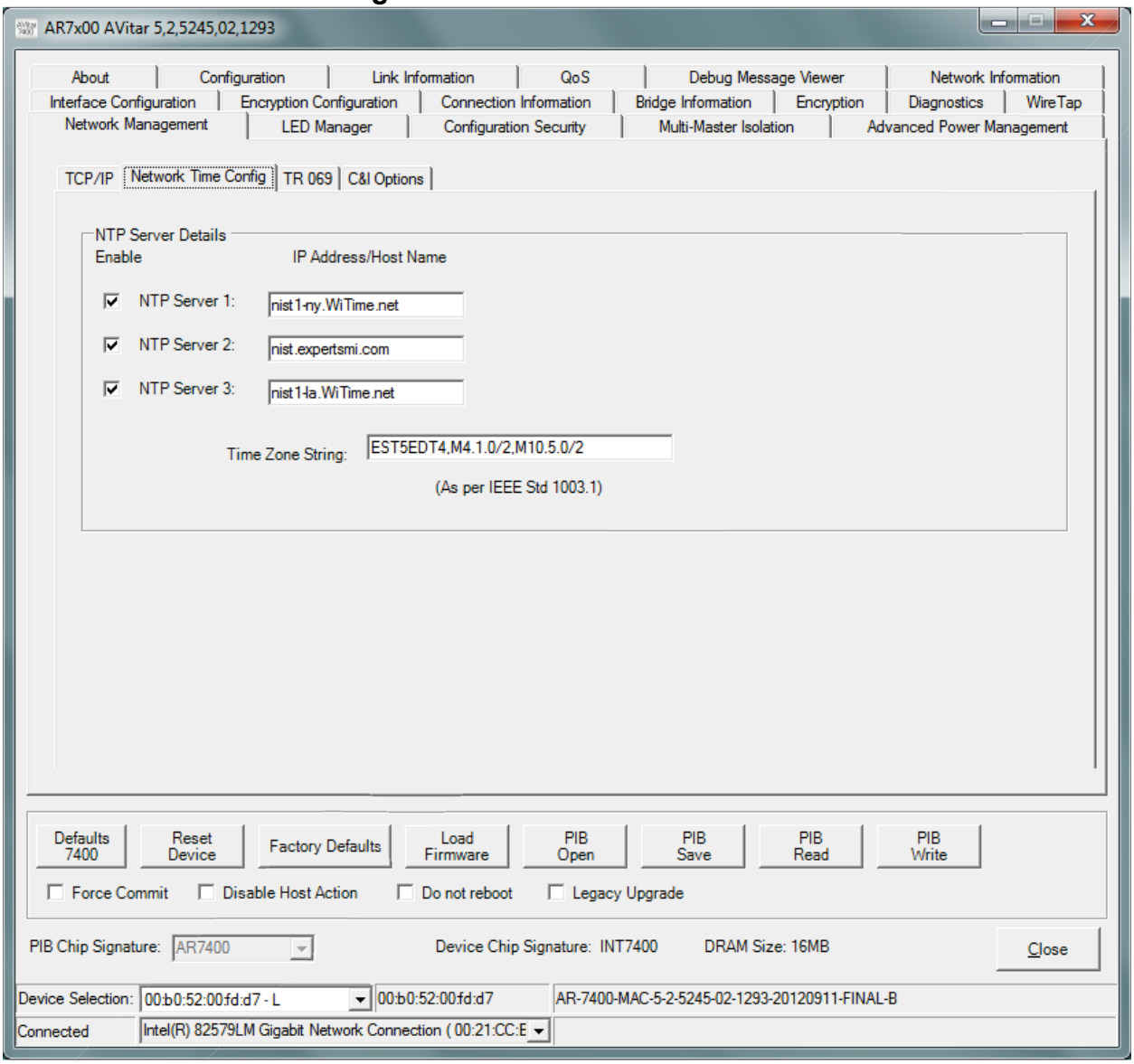


Figure 3-11: Network Time Configurations

Users can configure the Network Time Protocol (NTP) server name/address and current "Time Zone" value through "Network Time Config" sub-tab.

Enable each "NTP" server and provide the Server IP address/server host name. Users can enable/disable the particular "NTP" server through "Enable" checkbox.

Users can elect the current "Time Zone" by entering in the Time Zone String (as per IEEE Std. 1003.1). The Time Zone String content has been implemented according to the following description:

3.10.2.1 Time Zone information (IEEE Std. 1003.1, 2004 Edition)

The value of Time Zone String Stored has one of the two forms (spaces inserted for clarity):

:characters

or:

std offset dst offset, rule

If it is of the first format (that is, if the first character is a colon), the characters following the colon are handled in an implementation-defined manner.

The expanded format (for all Time Zones whose value does not have a colon as the first character) is as follows:

stdoffset[dst[offset][,start[/time],end[/time]]]

Where:

std and dst – Indicate no less than three, nor more than {TZNAME_MAX}, bytes that are the designation for the standard (std) or the alternative (dst -such as Daylight Savings Time) timezone. Only std is required; if dst is missing, then the alternative time does not apply in this locale.

Each of these fields may occur in either of two formats quoted or unquoted:

- In the quoted form, the first character shall be the less-than ('<') character and the last character shall be the greater-than ('>') character. All characters between these quoting characters shall be alphanumeric characters from the portable character set in the current locale, the plus-sign ('+') character, or the minus-sign ('-') character. The std and dst fields in this case shall not include the quoting characters.
- In the unquoted form, all characters in these fields shall be alphabetic characters from the portable character set in the current locale.

The interpretation of these fields is unspecified if either field is less than three bytes (except for the case when dst is missing), more than {TZNAME_MAX} bytes, or if they contain characters other than those specified.

offset – Indicates the value added to the local time to arrive at Coordinated Universal Time. The offset has the form:

hh[:mm[:ss]]

The minutes (mm) and seconds (ss) are optional. The hour (hh) shall be required and may be a single digit. The offset following std shall be required. If no offset follows dst, the alternative time is assumed to be one hour ahead of standard time. One or more digits may be used; the value is always interpreted as a decimal number. The hour shall be between zero and 24, and the minutes (and seconds)-if present-between zero and 59.

The result of using values outside of this range is unspecified. If preceded by a '-', the timezone shall be east of the Prime Meridian; otherwise, it shall be west (which may be indicated by an optional preceding '+').

rule – Indicates when to change to and back from the alternative time. The rule has the form:

date[/time],date[/time]

where the first date describes when the change from standard to alternative time occurs and the second date describes when the change back happens. Each time field describes when, in current local time, the change to the other time is made.

The format of date is one of the following:

Jn – The Julian day n (1 <= n <= 365). Leap days shall not be counted. That is, in all years-including leap years-February 28 is day 59 and March 1 is day 60. It is impossible to refer explicitly to the occasional February 29.

n – The zero-based Julian day (0 <= n <= 365). Leap days shall be counted, and it is possible to refer to February 29.

Mm.n.d – The d'th day (0 <= d <= 6) of week n of month m of the year (1 <= n <= 5, 1 <= **m** <= 12, where week 5 means "the last d day in month m" which may occur in either the fou**rth or the** fifth week). Week 1 is the first week in which the d'th day occurs. Day zero is Sund**ay.**

The time has the same format as offset except that no leading sign ('-' or '+') is **allowed**. **Th**e default, if time is not given, shall be 02:00:00.

Here are some example strings:

"NZST-12NZDT-13,M10.5.0/2,M3.1.0/3",
"EST-10EST-11,M10.5.0/2,M3.1.0/3",
"JST-9",
"HKT-8",
"EET-3EET_DST-4,M3.5.0/1,M9.5.0/1"
"EET-2EET_DST-3,M3.5.0/3,M9.5.0/3",
"MET-1MET_DST-2,M3.5.0/2,M9.5.0/2",
"GMT0BST-1,M3.5.0/1,M10.5.0/1",
"FST2FDT1",
"EST3EDT2,M10.4.6/2,M2.2.6/2",
"AST4ADT3,M4.1.0/2,M10.5.0/2",
"EST5EDT4,M4.1.0/2,M10.5.0/2",
"CST6CDT5,M4.1.0/2,M10.5.0/2",
"MST7MDT6,M4.1.0/2,M10.5.0/2",
"PST8PDT7,M4.1.0/2,M10.5.0/2",
"YST9YDT8,M4.1.0/2,M10.5.0/2",
"HAST10HAST9,M4.1.0/2,M10.5.0/2",
"SST11"

3.10.3 TR-069 ACS Server Configuration

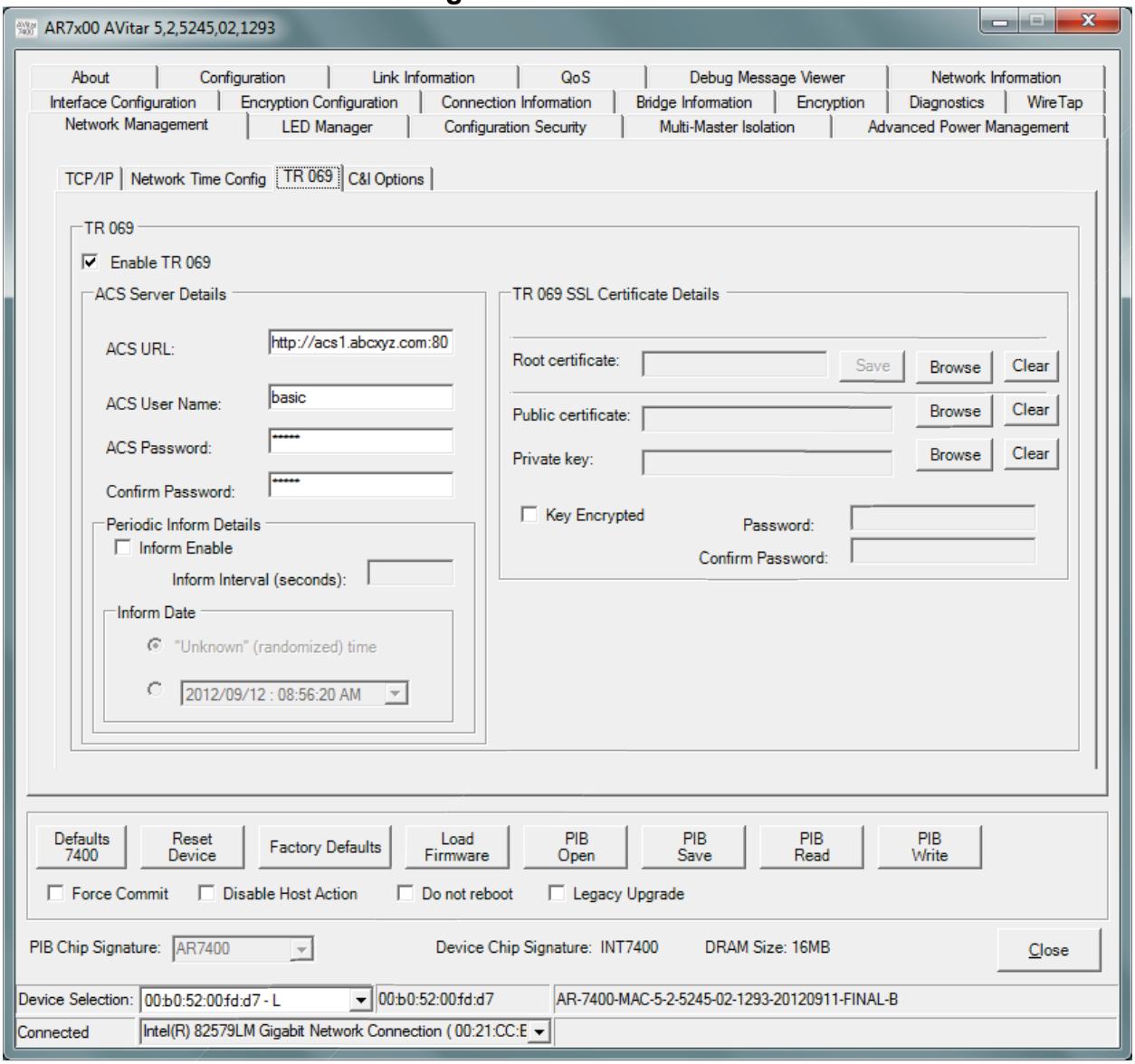


Figure 3-12: TR 069 ACS Configurations

Users can configure TR-069 Auto Configuration Server (ACS) parameters through "TR-069" sub-tab. This sub-tab allows for configuration of ACS URL, Username, Password, enabling or disabling of ACS Periodic Inform, Periodic Inform Interval value and Inform Date.

The Inform Date can be provided as either "Unknown" time, as defined in TR-069 specification, or can be entered as a reference point in time to be used to calculate next actual Inform time (as per TR069 specification).

To configure ACS Server parameters, please follow these steps:

1. Select the "Enable TR 069" checkbox.
2. Configure all the required parameters.
3. Write the configuration into the PIB.

3.10.3.1 TR-069 SSL Certificate Configurations

TR-069 CPE device and ACS server may communicate through Secure Socket Layer (SSL) protocol. For configuring SSL in CPE device there are 3 certificate types available:

1. SSL Root Certificate (CA Certificate)
2. SSL Public Certificate
3. SSL Private Key and Decryption password.

- **SSL Root Certificate (Certificate Authority)**
  SSL Root Certificate (CA) is an entity that issues digital certificate for other parties. CA issues digital certificates that contain the public key and identity owner.
- **SSL Public Certificate**
  A public key certificate also known as identity certificate which uses a digital signature to bind together a public key with an identity.
- **SSL Private Key**
  SSL private key is used to decrypt the data passed over SSL connection. End users can configure the SSL connection in TR-069 CPE device through AVitar SSL configuration setup.

  For configuring the SSL connection, please follow the steps:

  1. If required browse for the files containing SSL Root Certificate
  2. If required browse for the files containing SSL Public Certificate
  3. If required browse for the files containing SSL Private key.
  4. Select "Key Encrypted" flag to notify the decryption password.
  5. Write the above configurations into the PIB block.

3.10.3.2 C&I Option

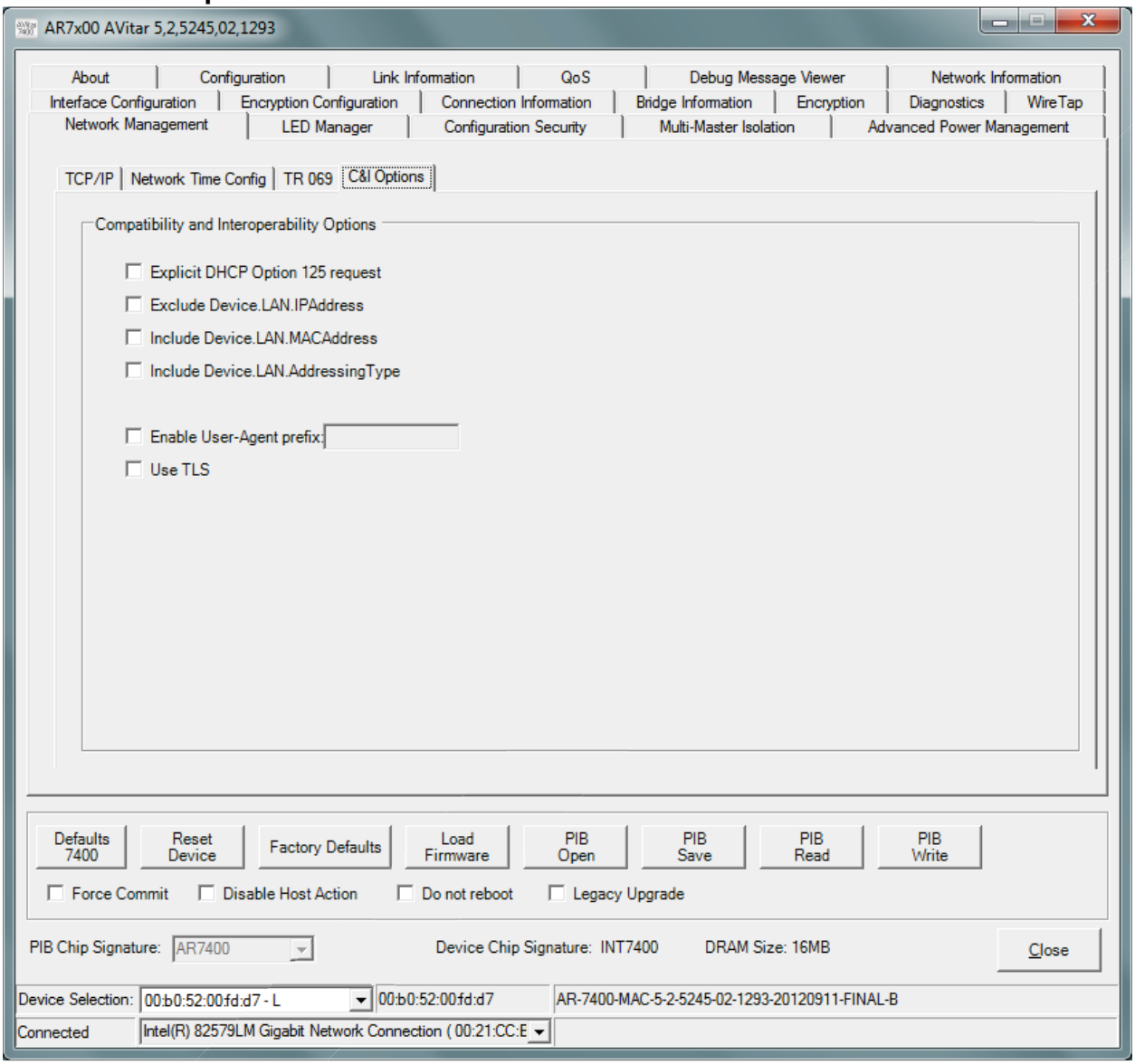


Figure 3-13: C&I Compatibility and Interoperability Options

The Compatibility and Interoperability (C&I) Options tab allows the customer to enable/disable specific CPE configuration options in order to operate properly with certain ACS servers, DHCP servers, or LAN gateway devices. All of these options should normally be left disabled and should only be used if a particular compatibility or interoperability issue has been identified.

The available CPE configuration options include the following:

- Explicit DHCP Option 125 request
  - Enable/Disable explicitly including the Vendor-Specific Information request (option number 125) in DHCPDISCOVER, DHCPREQUEST, and DHCPINFORM messages from the CPE.
  - Certain LAN gateway devices may not return their gateway identity information as required by the TR-111 specification unless this option is also enabled.

- Exclude Device.LAN.IPAddress
  - Enable/Disable the removal of the legacy TR-181 Issue 1 Device.LAN.IPAddress parameter from each INFORM message.
  - Some ACS servers may not work properly if the Device.LAN.IPAddress parameter is present in the INFORM message.
- Include Device.LAN.MACAddress
  - Enable/Disable the insertion of the legacy TR-181 Issue 1 Device.LAN.MACAddress parameter into each INFORM message.
  - Some ACS servers may not work properly if the Device.LAN.MACAddress parameter is not present in the INFORM message.
- Include Device.LAN.AddressingType
  - Enable/Disable the insertion of the legacy TR-181 Issue 1 Device.LAN.AddressingType parameter into the CPE's data model.
  - Some ACS servers may not work properly if the Device.LAN.AddressingType parameter is not present in the CPE's data model.

    NOTE: This parameter is read-only and will return either "DHCP" or "Static".
- Enable User-Agent prefix
  - Enables a customer-specific prefix string to be prepended to the normal "TR069 Client 1.0" user agent string (with a single blank character in between).
  - The maximum length of the User-Agent prefix is 7 characters.
  - This user agent string appears immediately following the "User-Agent:" parameter in all HTTP GET and POST messages that are generated by the CPE.
- Use TLS
  - Enables the CPE to negotiate a TLS v1 encrypted connection to the ACS.
  - Normally, an SSL v3 encrypted connection is used if the ACS URL begins with "https".

3.11 LED Manager Tab *(Configuration Window)*

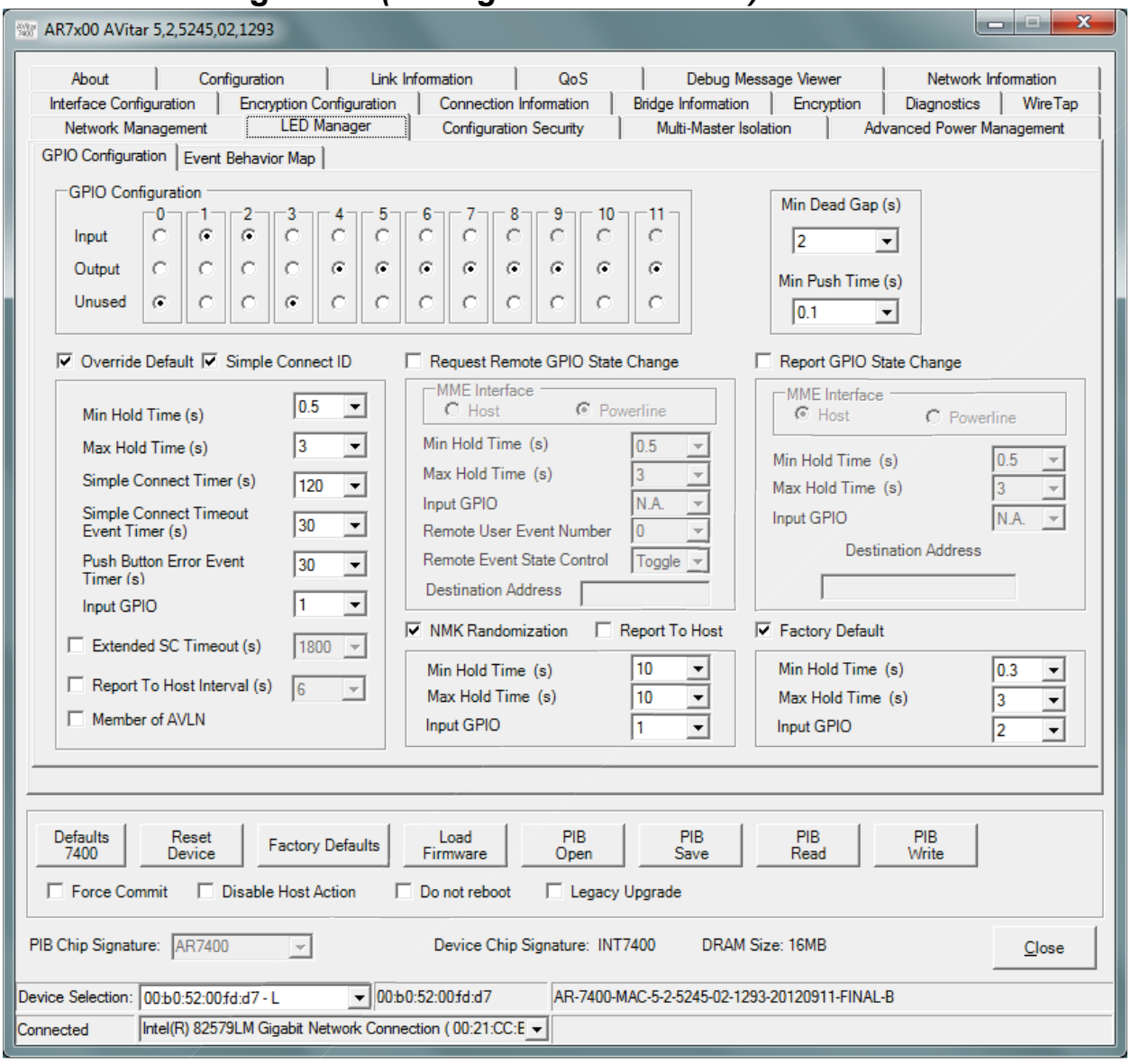


Figure 3-14: LED Manager Tab Window

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.

3.11.1 GPIO Configuration

The 'GPIO Configuration' group allows the user to map GPIO signals to Input, Output, or Unused. Figure 3-14 show the default mapping for the Qualcomm Atheros AR7400 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 3-14.

- **Simple Connect ID**
  Min Hold Time, Max Hold Time, Adder Failure Timeout, and Simple Connect Timeout controls can be used to customize this function.
  - **Extended SC Timeout**: when enabled, this feature overrides the "Simple Connect Timeout Event Timer" and "Push Button Error Event Timer", and allows an "Extended SC Timeout" from 20 seconds to 30 minutes to be specified. If a Simple Connect Error or Timeout occurs, the device will remain in the Error or Timeout state for a duration of "Extended SC Timeout".
- **Report To Host Interval**: Frequency of Host Update if 'Report to Host' functionality is enabled (valid values are from 1 to 10 seconds in steps of 1 sec, default value is 6 seconds).
- **NMK Randomization**
  Min Hold Time, Max Hold Time controls can be used to customize this function.
- **Report To Host:** If enabled, reports to Host (via GPIO State Change Indicate MME) Simple Connect, NMK Randomization or Reset to Factory Defaults Event.
- **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 Qualcomm Atheros HomePlug AV v5.2.x 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 Remote User Event Number field and the Remote Event State Control field are used to control the behavior of a remote device which has been identified in the destination address field.
- **Report GPIO State Change**
  Enable GPIO state change indicates MME. See Qualcomm Atheros 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

3.11.2 Event Behavior Map

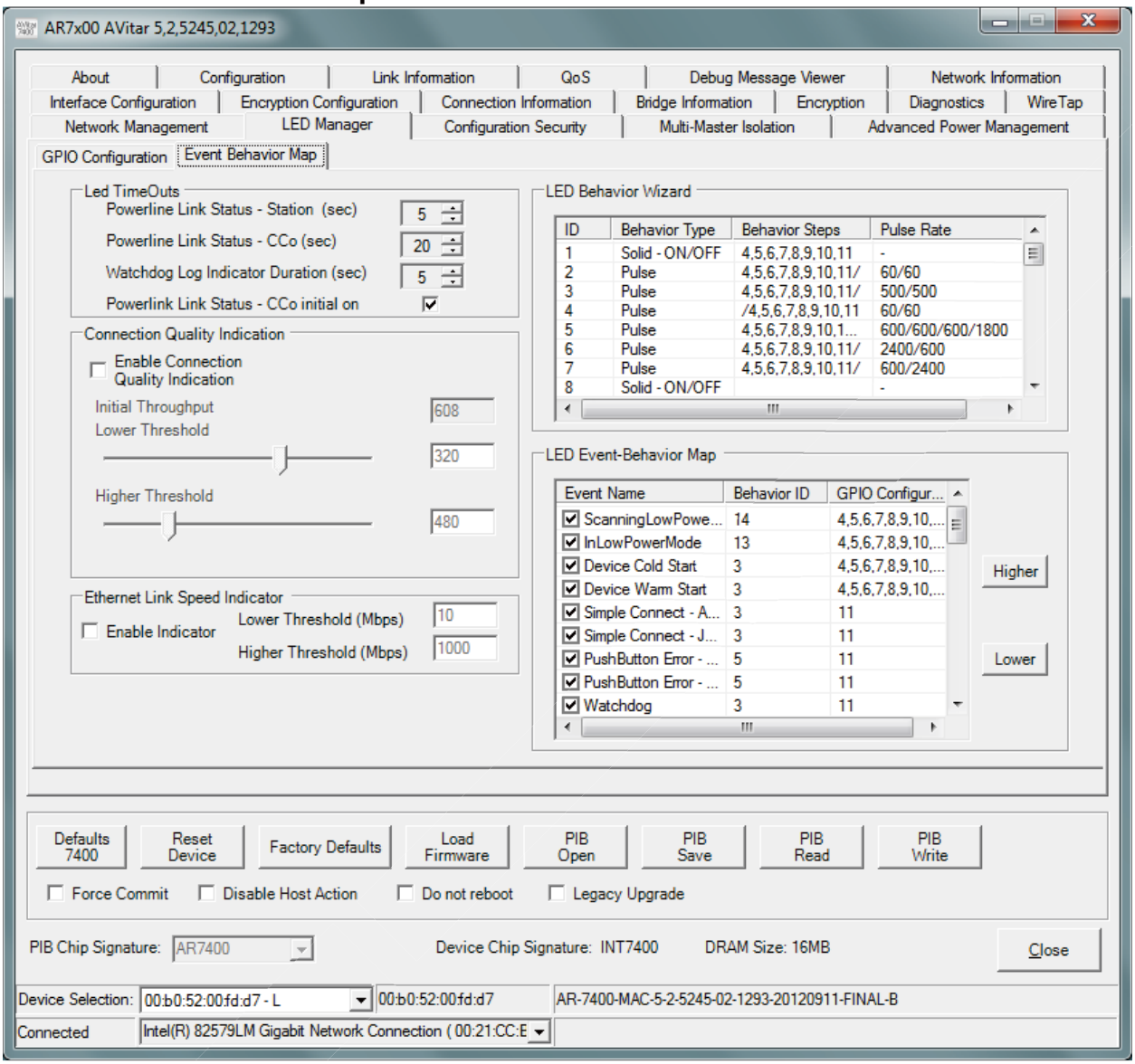


Figure 3-15: Event Behavior Map Window

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

The user can update the default ***Led TimeOuts*** and ***Connection Quality Indication*** by navigating to the LED Manager Tab → GPIO Configuration Tab, ☑ Override Default checkbox which enables the Led TimeOuts and Connection Quality Indication Controls.

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.

NOTE: The Threshold values are quantized to 4 Mbps increments.

3.11.3 LED Behavior Wizard

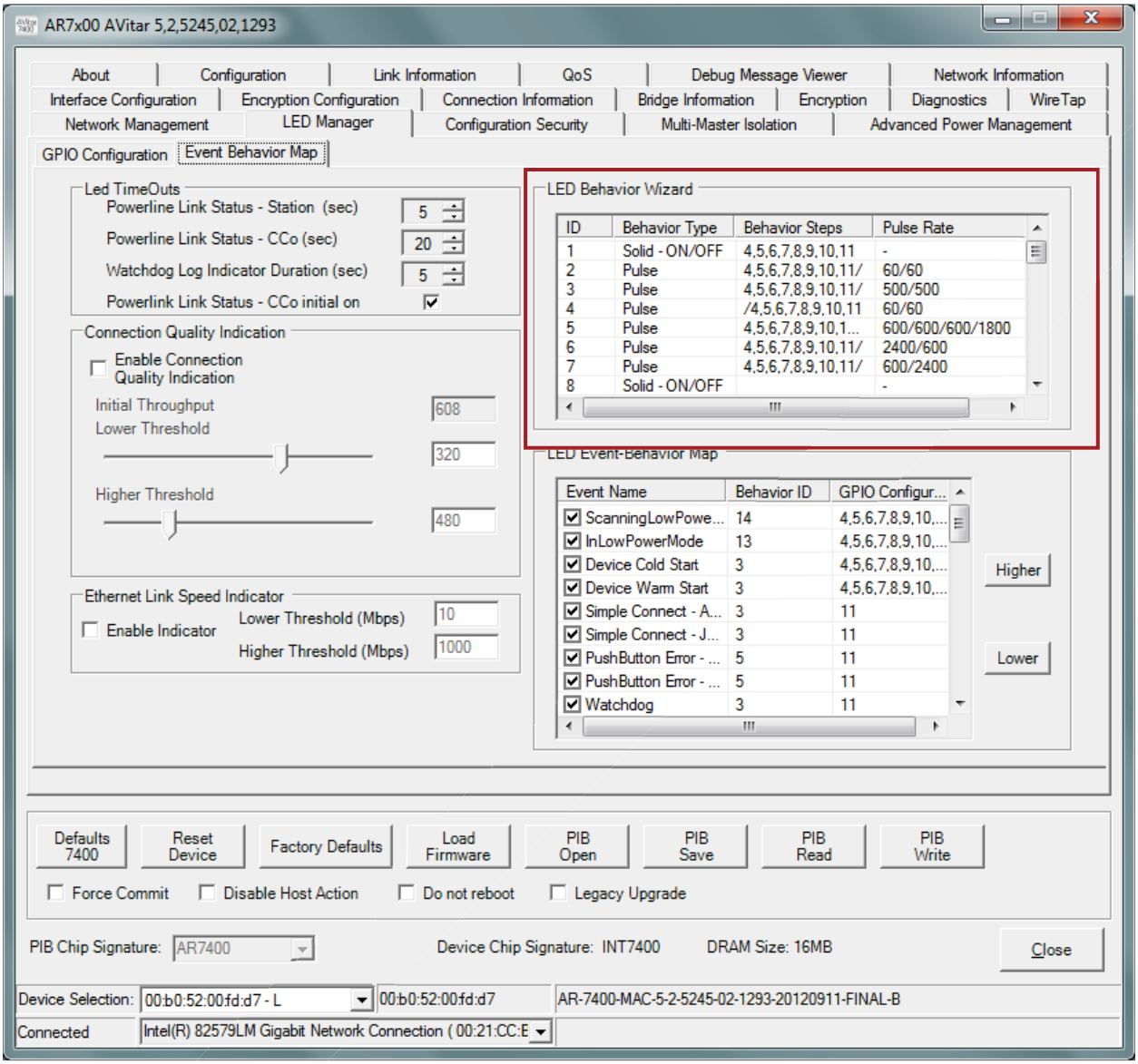


Figure 3-16: LED Behavior Wizard

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. Refer to the Firmware Technical Reference Manual for details on the LED Behavior Event.

3.11.4 LED Event-Behavior Map

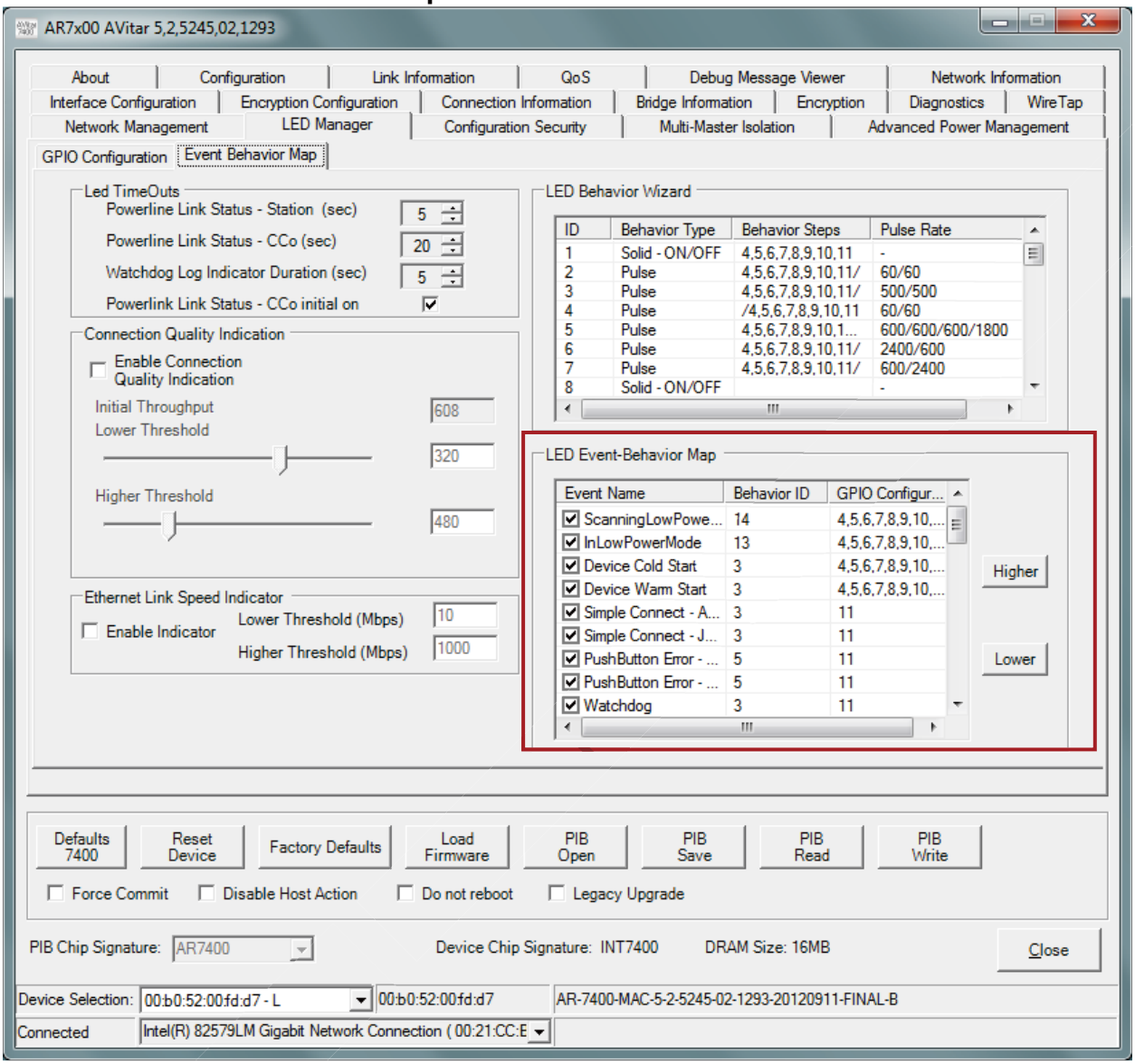
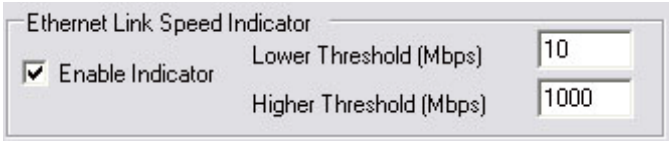


Figure 3-17: LED Event-Behavior Map

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.

LED Events Ethernet Link Rx, Ethernet Link Tx and Ethernet Link can be used to indicate the speed of the MII connection between the AR7400 and the Ethernet PHY chip. This provides a link speed indication on adapters to illustrate when the Ethernet port is running at either 10 Mbps or 100 Mbps. This indication can be used to provide user friendly diagnostics for potential problems with the deployment in the field. This feature is enabled by the Enable Indicator check box:

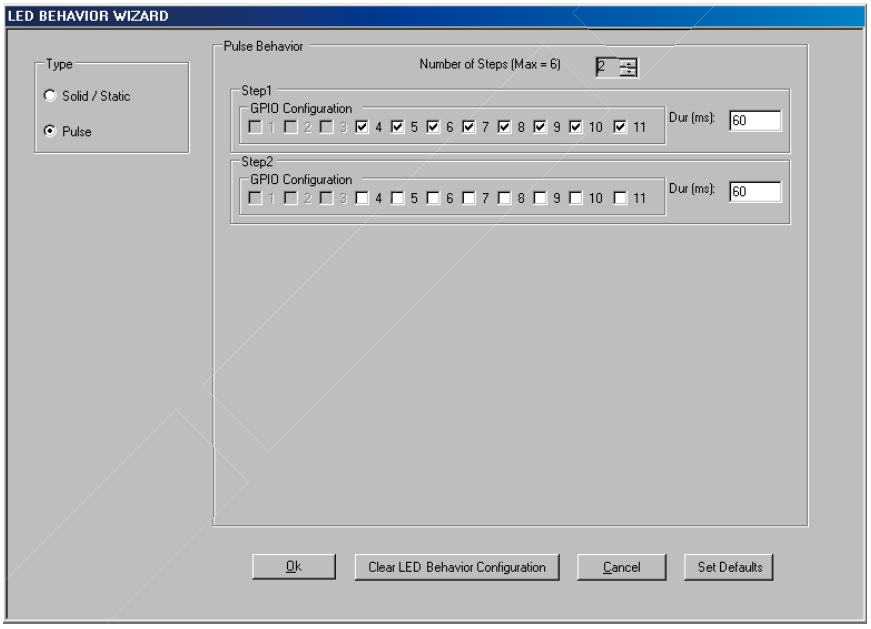


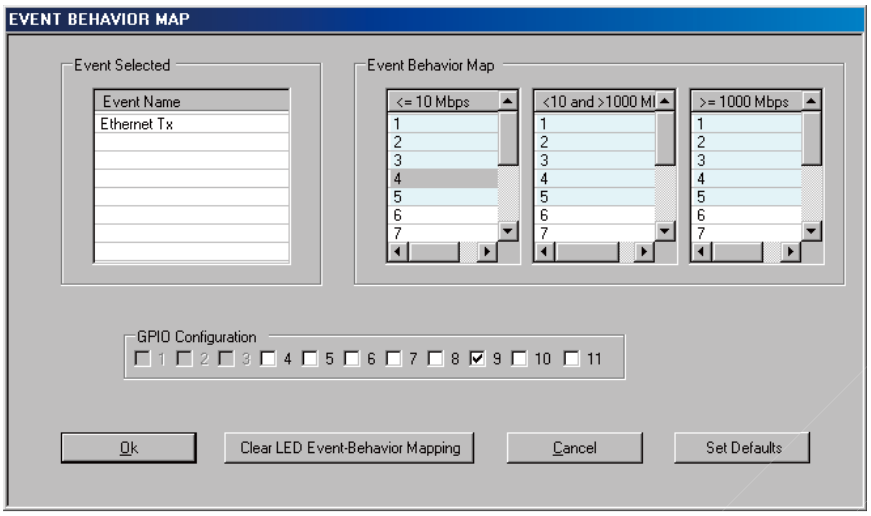
Ethernet link/TX/RX can be represents with a 2 color LED in place of the single color LED such that the end user can tell the Ethernet link speed is either 10Mbps or 100Mbps. This operation can also be extended to support 1000Mbps.

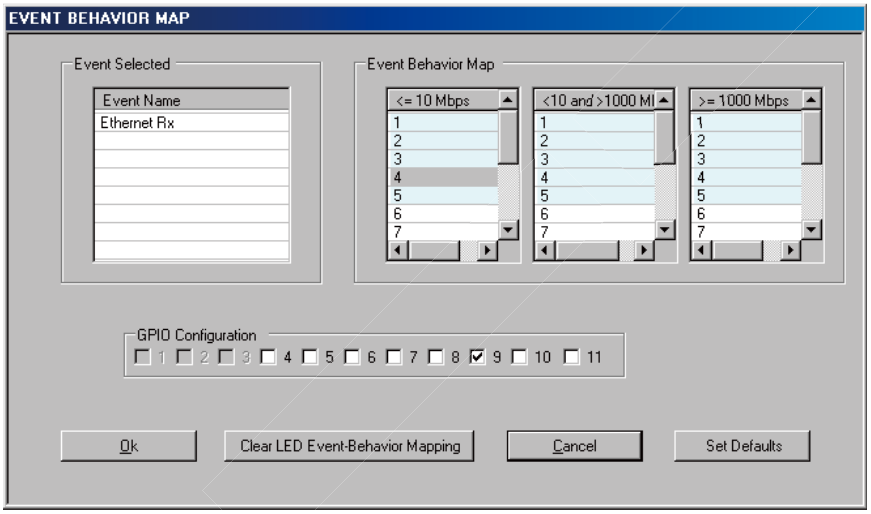
The adapter can be configured to display four Ethernet link "speeds":

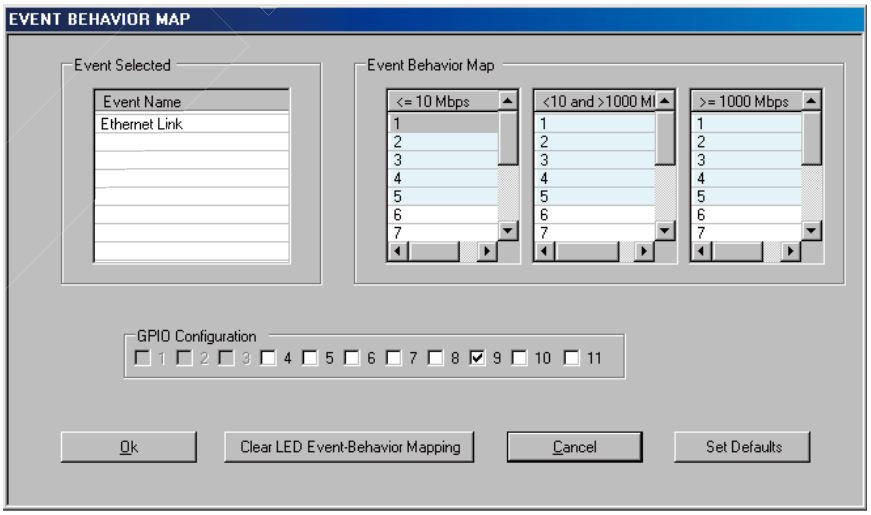
Ethernet Link Speed	Behavior
No Link	Display behavior according to No Link
<=10 Mbps	Display behavior according to Low Speed
>10 Mbps and <1000 Mbps	Display behavior according to Mid Speed
>=1000 Mbps	Display behavior according to High Speed

The event can be mapped to any behavior (i.e. Solid On/Off or Pulsed) and to a certain GPIO. This can allow the design to create a two color Ethernet speed indicator that is Off for no link, red for 10 Mbps, amber for 100 Mbps and green for 1000 Mbps.




EVENT BEHAVIOR MAP
Event Selected
Event Name
Ethernet Tx
Event Behavior Map
<= 10 Mbps
<10 and >1000 Mbps
>= 1000 Mbps
GPIO Configuration
1 2 3 4 5 6 7 8 9 10 11
Ok
Clear LED Event-Behavior Mapping
Cancel
Set Defaults


EVENT BEHAVIOR MAP
Event Selected
Event Name
Ethernet Rx
Event Behavior Map
<= 10 Mbps
<10 and >1000 Mbps
>= 1000 Mbps
GPIO Configuration
1 2 3 4 5 6 7 8 9 10 11
Ok
Clear LED Event-Behavior Mapping
Cancel
Set Defaults


EVENT BEHAVIOR MAP
Event Selected
Event Name
Ethernet Link
Event Behavior Map
<= 10 Mbps
<10 and >1000 Mbps
>= 1000 Mbps
GPIO Configuration
1 2 3 4 5 6 7 8 9 10 11
Ok
Clear LED Event-Behavior Mapping
Cancel
Set Defaults

3.12 Configuration Security Tab *(Configuration Window)*

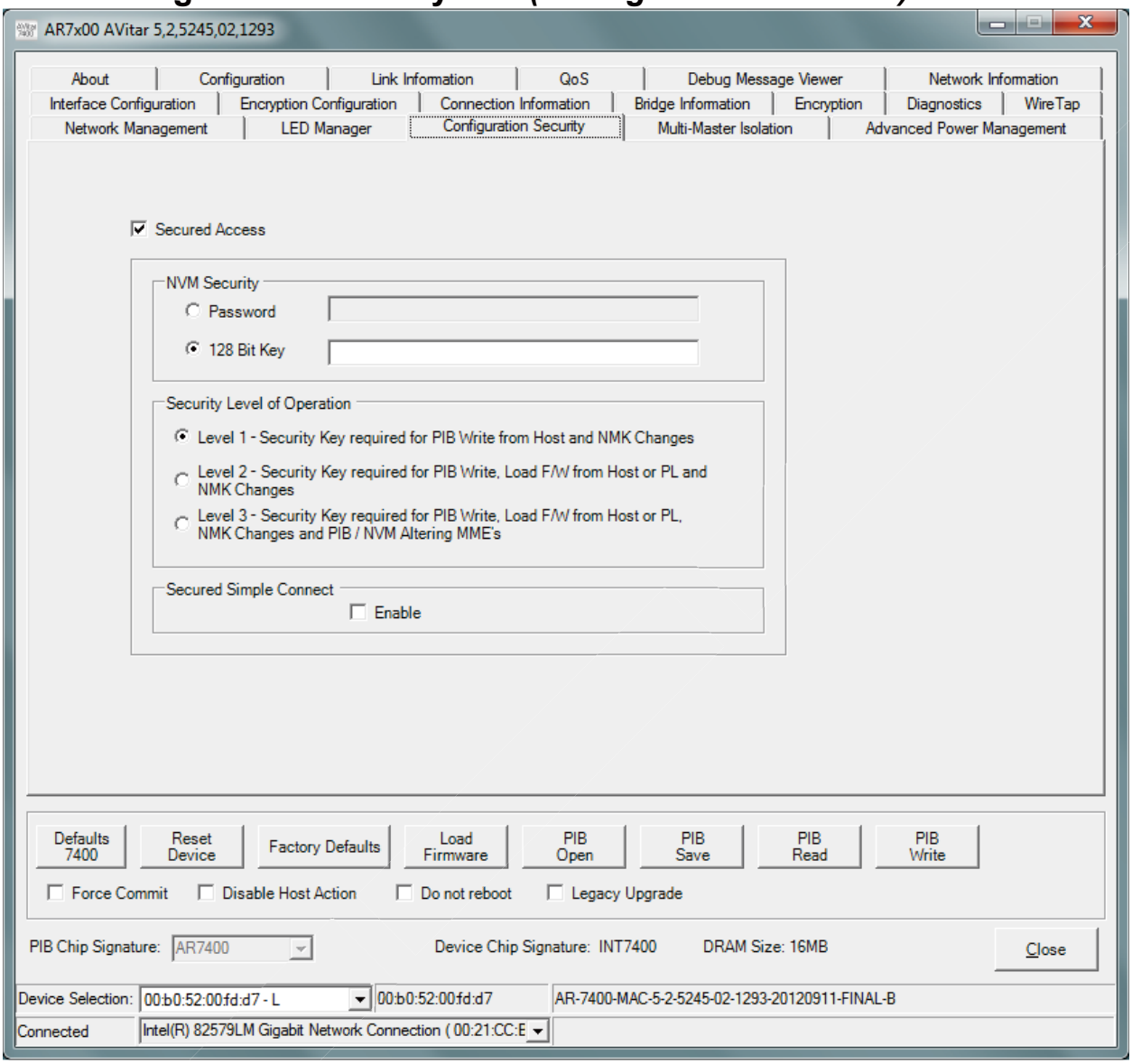


Figure 3-18: Configuration Security Tab

3.12.1.1 Secured Access

Setting the 'Secured Access' checkbox (☑) enables the capability to configure the device's security level options. Clearing the 'Secured Access' checkbox (☐) disables the devices security level. The AVitar application can only create a Parameter Information Block (PIB) file that enables the 'Secured Access' mode of operation. To write a 'Secured Access' enabled PIB into a device's Non-Volatile Memory (NVM) requires the Production Test System (PTS) or a custom developed application capable of 128 bit AES encryption and de-encryption.

3.12.1.2 NVM Security

The 'NVM Security' section permits the entry of a security key that is used protect the device against unauthorized changes to the device's configuration settings stored in its Non-Volatile Memory (NVM). This is known as the NVM Authorization Key (NVAK). There are two NVAK entry methods that can be used; a 'Password' method or a '128 bit Key' method. When using the 'Password' key entry method, a string of alphanumeric characters can be used (except for the space character). For maximum security strength, the 'password' should be at least 24 characters long. When using the '128 bit' key entry method, a string of characters consisting of any of the following values can be used; 0-9, a,A,b,B,c,C,d,D,e, E, f,F. For maximum security strength, the 128 bit key should be the maximum length of 32 characters.

3.12.1.3 Security Level of Operation

There are 3 available security levels that can be chosen which controls the types of NVM configuration changes that require authorization based upon the 'Security Key'. Level 1 is lowest authorization level and level 3 is the highest level.

Level 1 – Authorization is required for PIB writes via the host interface and for NMK changes.

Level 2 – Authorization is required for PIB writes and Load Firmware requests from either the host or powerline interfaces. NMK changes also require authorization.

Level 3 – Authorization is required for PIB writes and Load Firmware requests from either the host or powerline interfaces. NMK changes and MME's which alter the PIB, also require authorization.

3.12.1.4 Secured Simple Connect

By default, the push button 'Simple Connect' function is allowed for all Authorized Update levels of Operation. Setting the 'Secured Simple Connect' checkbox (☑) restricts the 'Simple Connect' function to be authorized only between devices which share the same NVM Authorization 'Security Key'. Disabling 'Simple Connect' functionality can be achieved by clearing (☐) the 'Simple Connect ID' checkbox on the LED Manager Tab. Disabling or restricting 'Simple Connect' functionality may be considered being a non-compliant HomePlug AV method of operation.

3.13 Multi-Master Isolation Tab *(Configuration Window)*

3.13.1 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 3-3.

To enable Multiple Master channel selection, choose MDU selection on the configuration tab (Figure 3-3) and channel selections in the Multi Master Isolation tab (see Figure 3-20 or Figure 3-21).

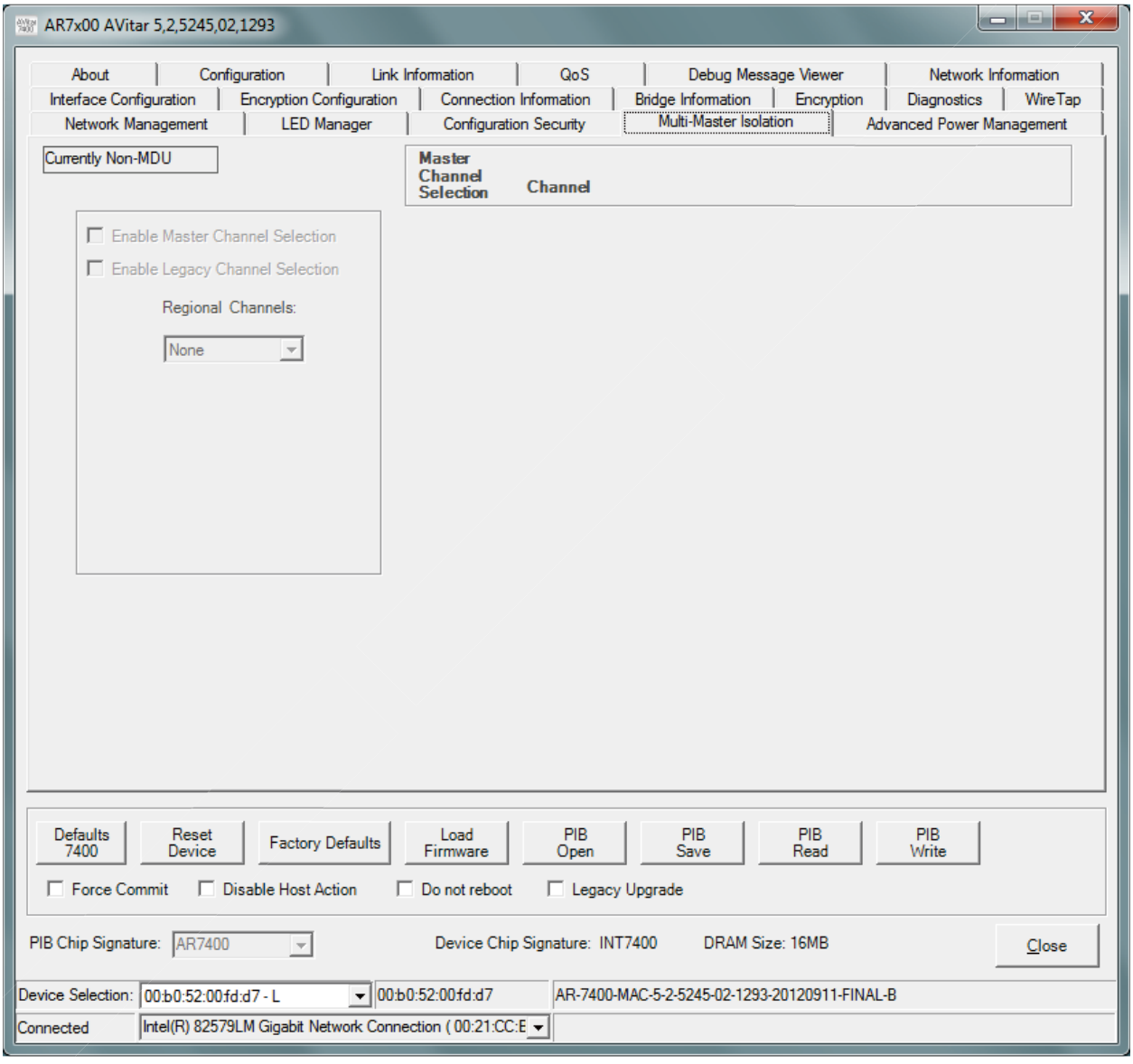


Figure 3-19: Multi-Master Isolation Tab – Currently Non-MDU

3.13.2 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 3-3.

3.13.2.1 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.

3.13.2.2 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.

3.13.2.3 Master Configuration

The 'Master Configuration' this is *read only*, the Static SNID number is extracted from the Configuration Tab see Figure 3-3. The Master Channel ID is displayed as a result from the 'Master Channel Selection' radial button selected on the right panel.

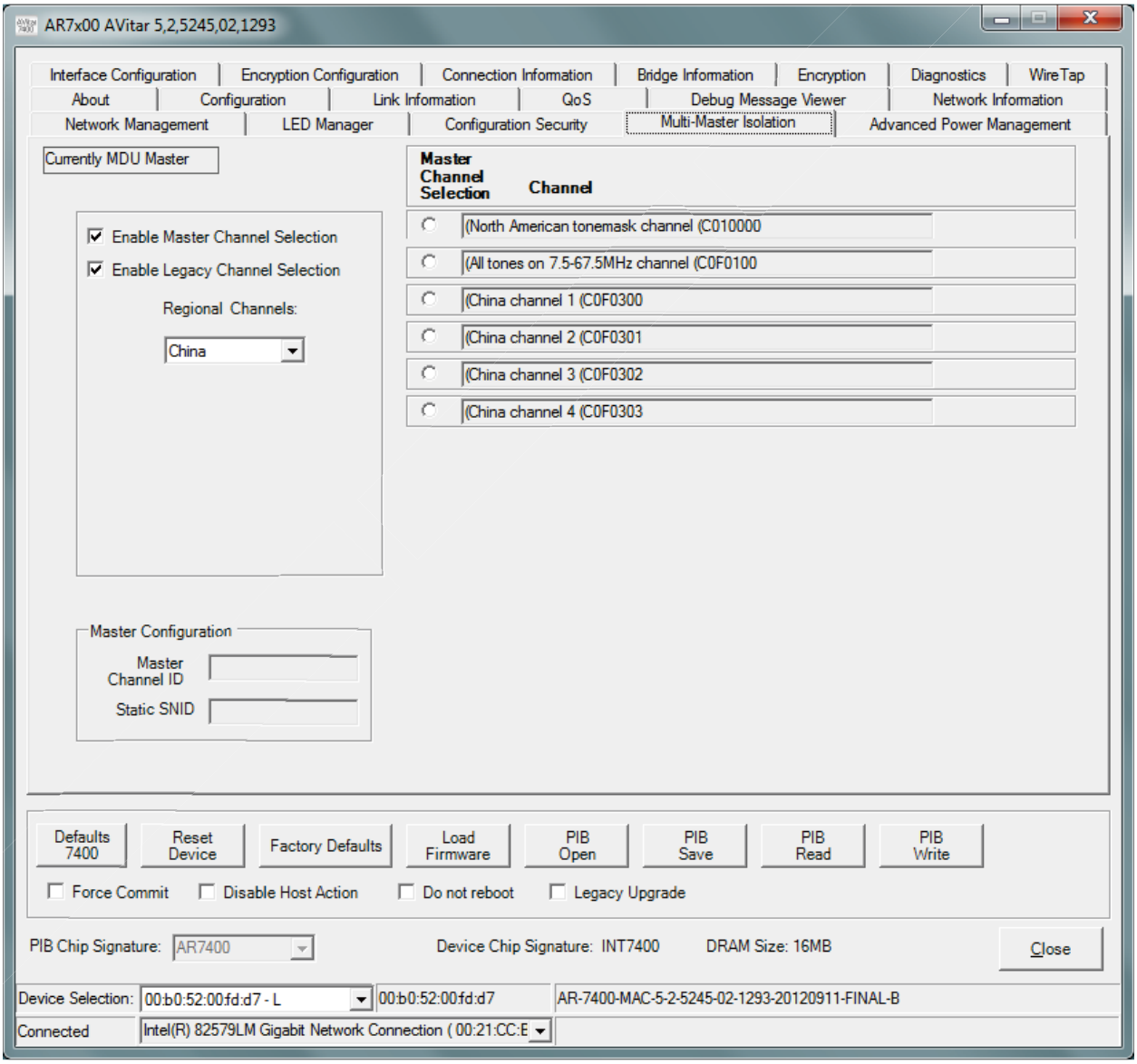


Figure 3-20: Multi-Master Isolation Tab – Master Configuration

3.13.3 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 3-3. For detailed description see Enable Master Channel Selection.

3.13.3.1 Master Channel Selection

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

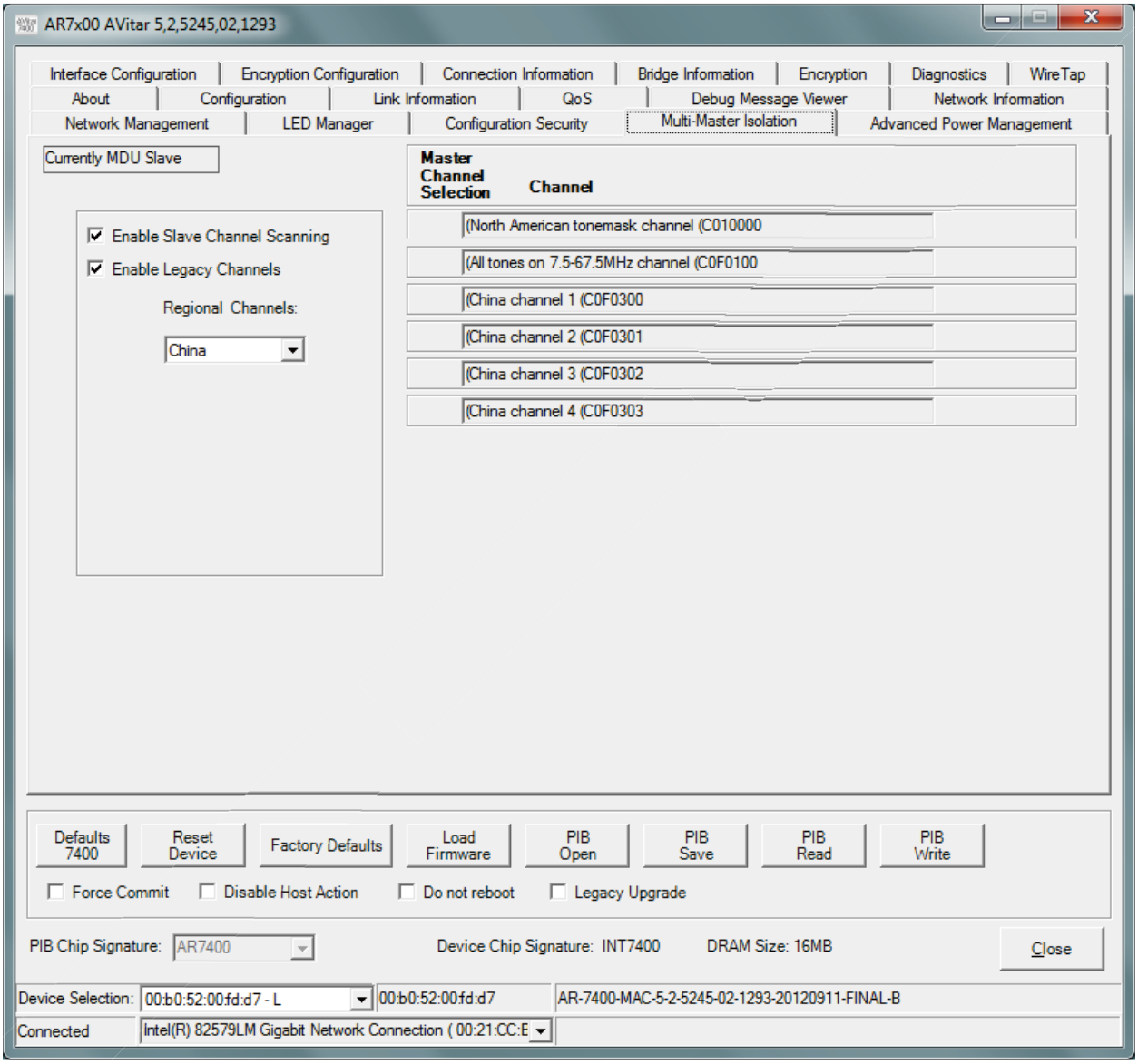


Figure 3-21: Multi-Master Isolation Tab – Slave Configuration

3.14 Advanced Power Management Tab *(Configuration Window)*

By default Low Power Management is disabled in AR7400 devices. To enable Power Management select 'Uncoordinated Sleep' from the Standby Mode dropdown.

3.14.1 Options

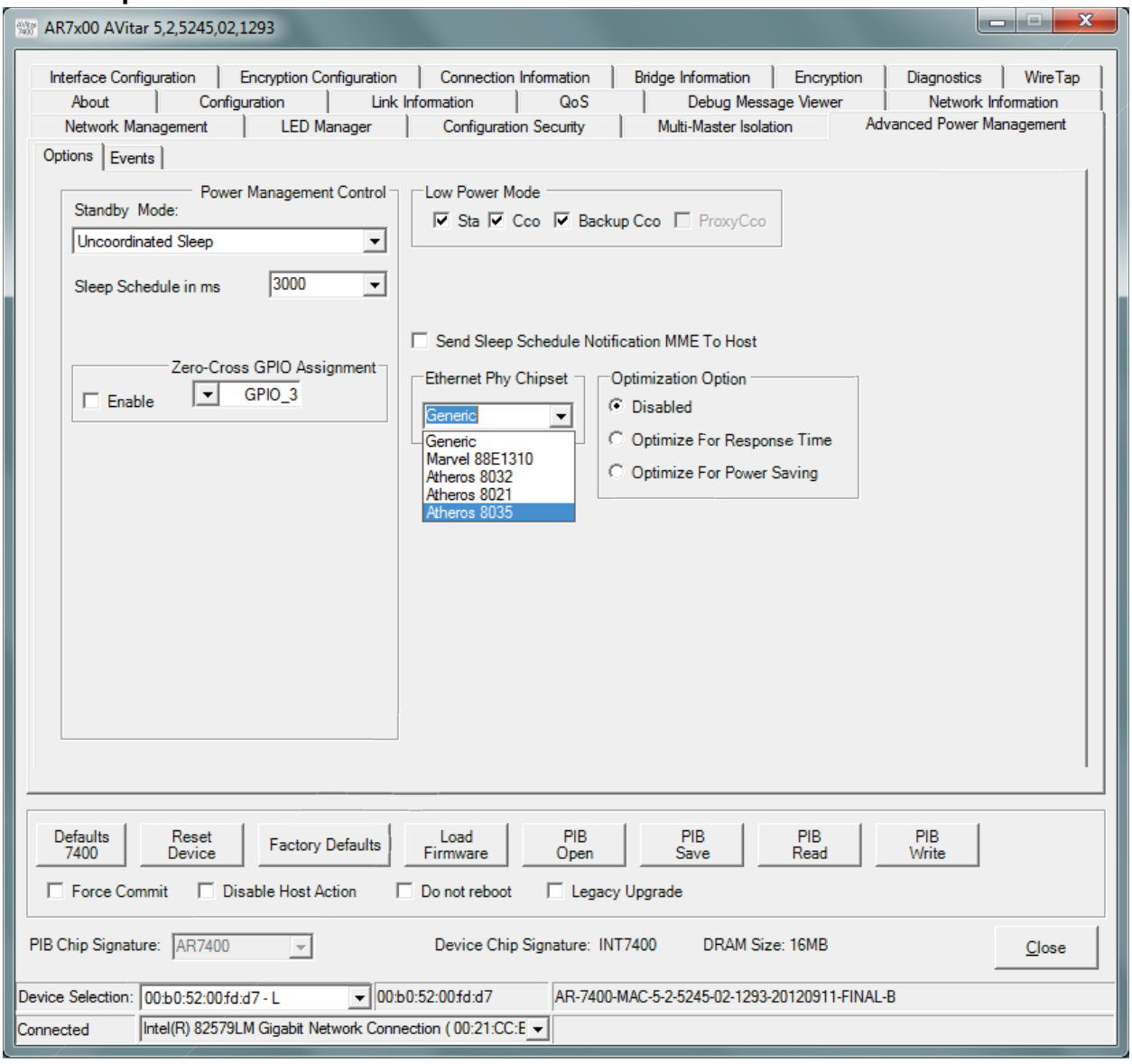


Figure 3-22: Advanced Power Management Options Tab – Options Selection

3.14.1.1 Uncoordinated Sleep Selection Option

- **Sleep Schedule in ms**: the length of time the device is in the standby state and unresponsive to a wake event (response time). Note: The longer the sleep schedule duration the lower the device's energy consumption. However, a longer sleep schedule also means the device will be slower to respond to a wake event.

- **Zero Cross:** Additional power savings can be achieved by turning off the zero cross hardware when the device is in low power mode. Select ☑ the checkbox if you want to enable this capability.
- **Zero Cross GPIO Assignment:** Specify the GPIO number used by the Zero Cross hardware.

3.14.1.2 Ethernet PHY Chipset

Improved power savings can be realized if the device hardware has been configured with one of the Qualcomm Atheros Reference Design Ethernet Chipsets. Select the appropriate chipset instead of default, "generic".

- **Optimize for Response Time or Optimize for Power Savings**: There is a user experience trade-off between device response time and power savings. Device response time refers to the device responsiveness to a "wake event" (see Section 0 for a description of events) while the device is in the standby state. If one desires that the device achieves the lowest possible power consumption while in the standby state, select the "Optimize for Power Savings" option. If one desires the device to be more responsive to a wake event, at the expense of slightly higher power consumption in the standby state, select the "Optimize for Response Time" option.

NOTE: Devices have been optimized to achieve lower power consumption in the standby state if either the Eth Link Down Sleep Event / Eth Link Up Wake Event Set has been configured OR the GPIO Sleep Event / GPIO Wake Event Set has been configured.

3.14.2 Events

There are also several system events available for triggering when a device enters and exits the low power state. The following wake and sleep event triggers can be configured for the Standby and Shutdown power management modes:

a) GPIO

b) MME

c) Ethernet Activity

d) Timer (wake only)

e) Ethernet Link

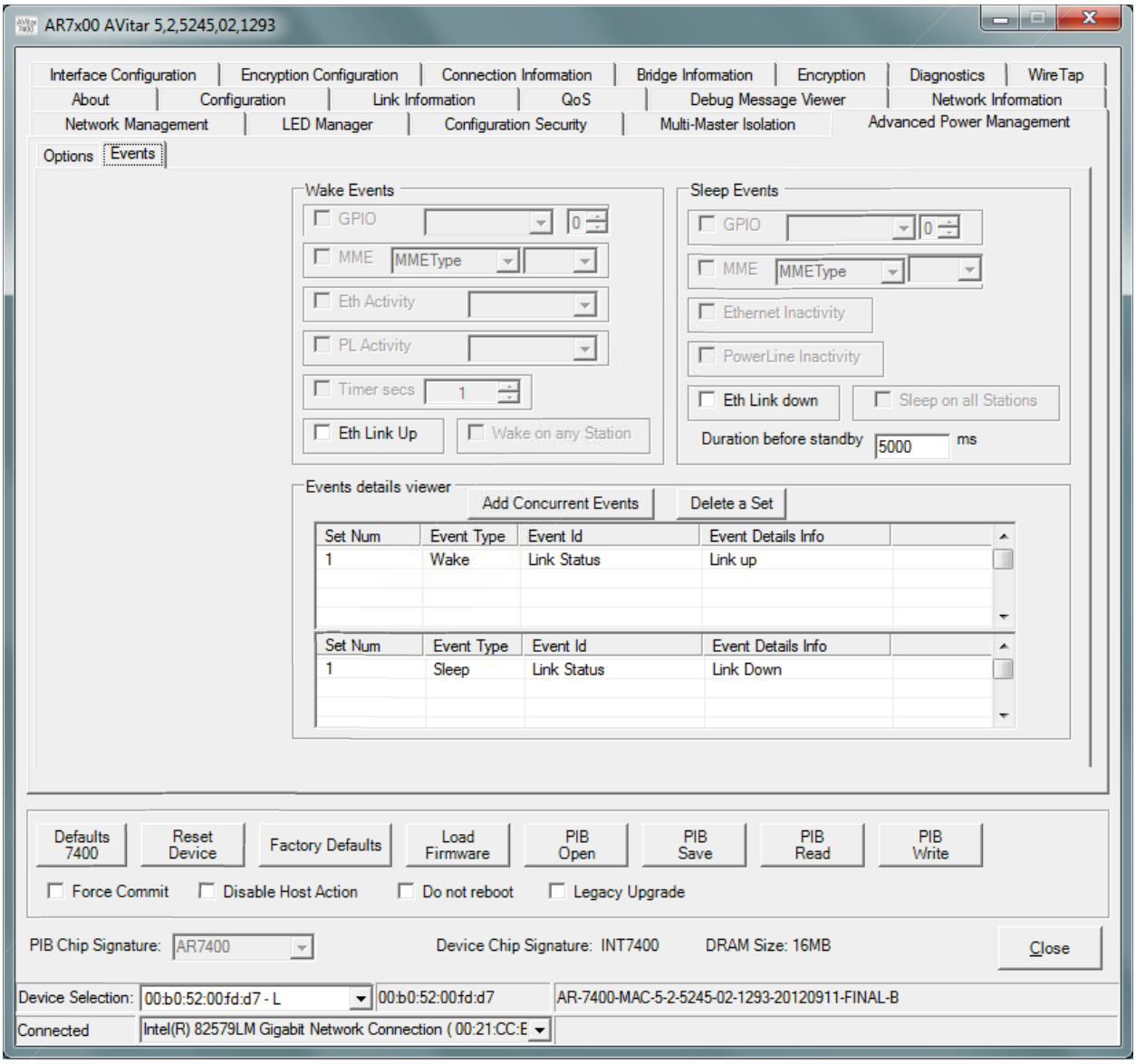


Figure 3-23: Advanced Power Management Options Tab – Events Selection

This tab is used to define the sleep and wake events that controls when a device will the low power state and exit the low power state respectively. One to three wake events can be selected, to be used in combination, to create a wake "Set" of triggers. All events within the same wake

"set" must all occur during the same 1.9 ms default scan period to generate the wake trigger. One to three sleep events can be selected, to be used in combination, to create a sleep "Set" of triggers. All events within the same sleep "set" must all occur during the same **Duration before Standby** period to generate the sleep trigger. A wake and/or sleep set are created by selecting the desired events and then press the "**Add Concurrent Event**" button. The "**Duration before Standby**" specifies the time in milliseconds that the device will wait before entering the low power state.

Multiple "wake" and "sleep" sets can be created by selecting another set of event triggers after the "**Add Concurrent Event**" button is pressed. Each set is displayed with a unique "**Set Num**" identifier in the **"Events detail viewer"** list box. The upper list box contains the "wake" events. The lower list box contains the "sleep" events. When multiple event sets are created, each set is an "OR" condition. For example, if one requires the device to enter the low power state when the Ethernet link is down OR when an MME of a specific MType is received, the event must be specified in separate "sleep" event sets. An event set can be deleted by highlighting the desire "**Set Num**" and pressing the "**Delete a Set**" button.

Table 3-1: Wake Event Triggers

Wake Event	Description	Notes
GPIO	A GPIO number can be specified along with GPIO state; high (1) or low (0).	GPIO need to properly isolated to ensure they generate false signals
MME	A MME with a specified MTYPE can be specified.	
Ethernet Activity	The device will generate a wake event when any Ethernet traffic to the device is detected	
Timer	After entering the low power state, the device will generate a wake event after the specified number of seconds.	
Eth Link Up	The device will generate a wake event when an Ethernet Link is detected	

Table 3-2: Sleep Event Triggers

Sleep Event	Description	Notes
GPIO	A GPIO number can be specified along with GPIO state; high (1) or low (0).	GPIO need to properly isolated to ensure they generate false signals
MME	A MME with a specified MTYPE can be specified.	
Ethernet Inactivity	The device trigger the sleep event if no Ethernet traffic to the device is detected	
Eth Link Down	The device will generate a sleep event when an Ethernet Link is not detected	

3.14.2.1 Power Management Support for a Managed Switch

When configured to go into low power mode using the Ethernet link trigger, this feature allows the device to enter/exit low power mode based on link status of the configured ports. A multiport switch device must be configured for MAC mode operation.

This feature accesses each port behind a multi-port switch to determine "link status." If all "link status" fields indicate "no link status," activate low power mode operations, if enabled. Following low power mode operations, continue to check "link status" fields and if any one of the ports becomes active, resume normal operations. The Access Multi-Port Link Status MME is used to configure the device to monitor the switch IC's ports.

The Access Multi-Port Link Status MME is used to configure a powerline device for accessing each port behind a multi-port switch to determine link status. If all link status fields indicate "no link status", activate low power mode operations. For details on the Multi-Port Link Status MME, refer to the Qualcomm Atheros HomePlug AV FW TRM.

3.15 Interface Configuration Tab *(Configuration Window)*

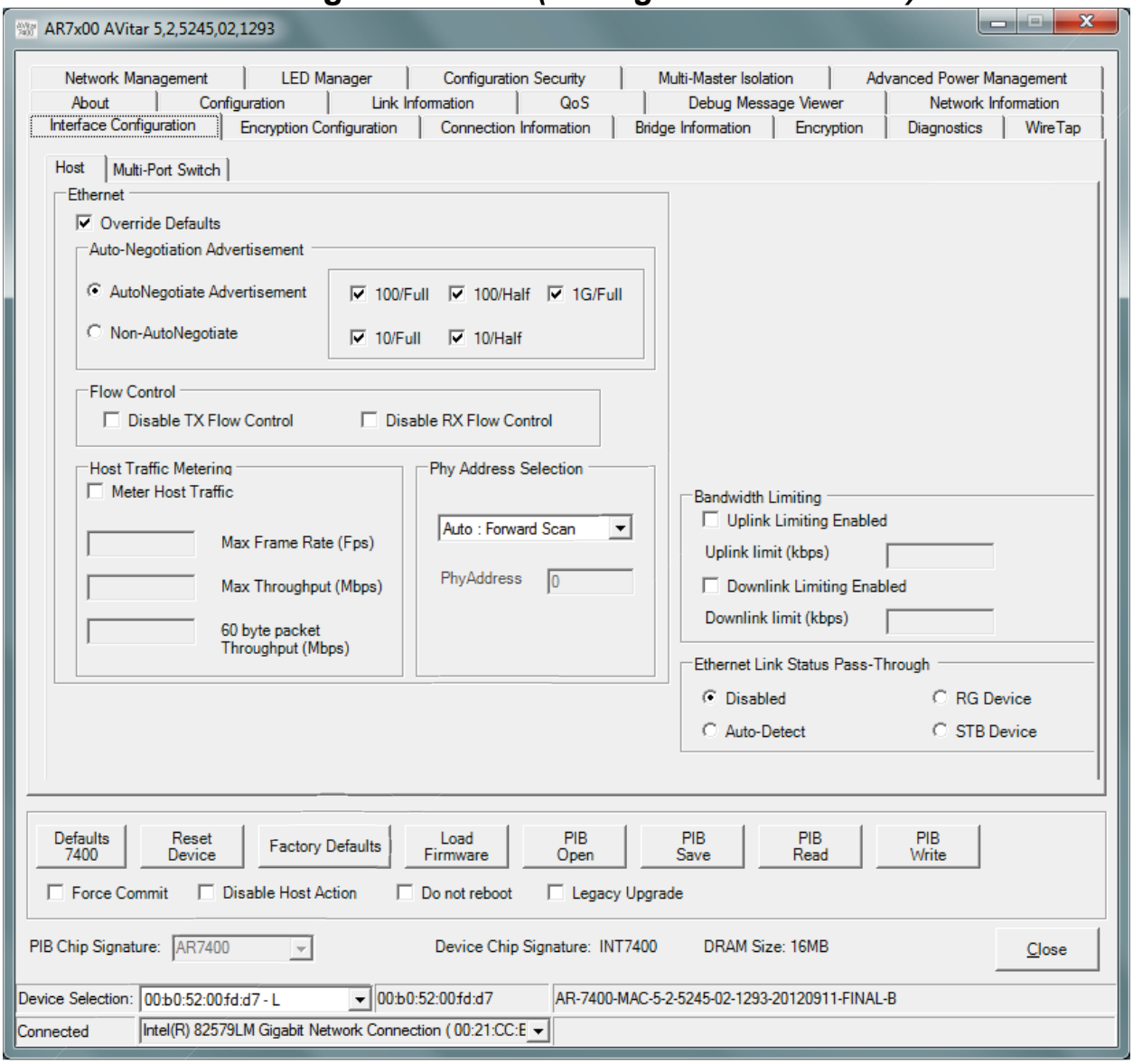


Figure 3-24: Interface Configuration Tab Window

3.15.1 Override Defaults Checkbox

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

3.15.2 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.

3.15.3 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.

3.15.4 PHY Address Selection

If the AR7400 is connected to a managed switch via MII this selects the default management PHY address.

3.15.5 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.

3.15.6 Multi-Port Switch

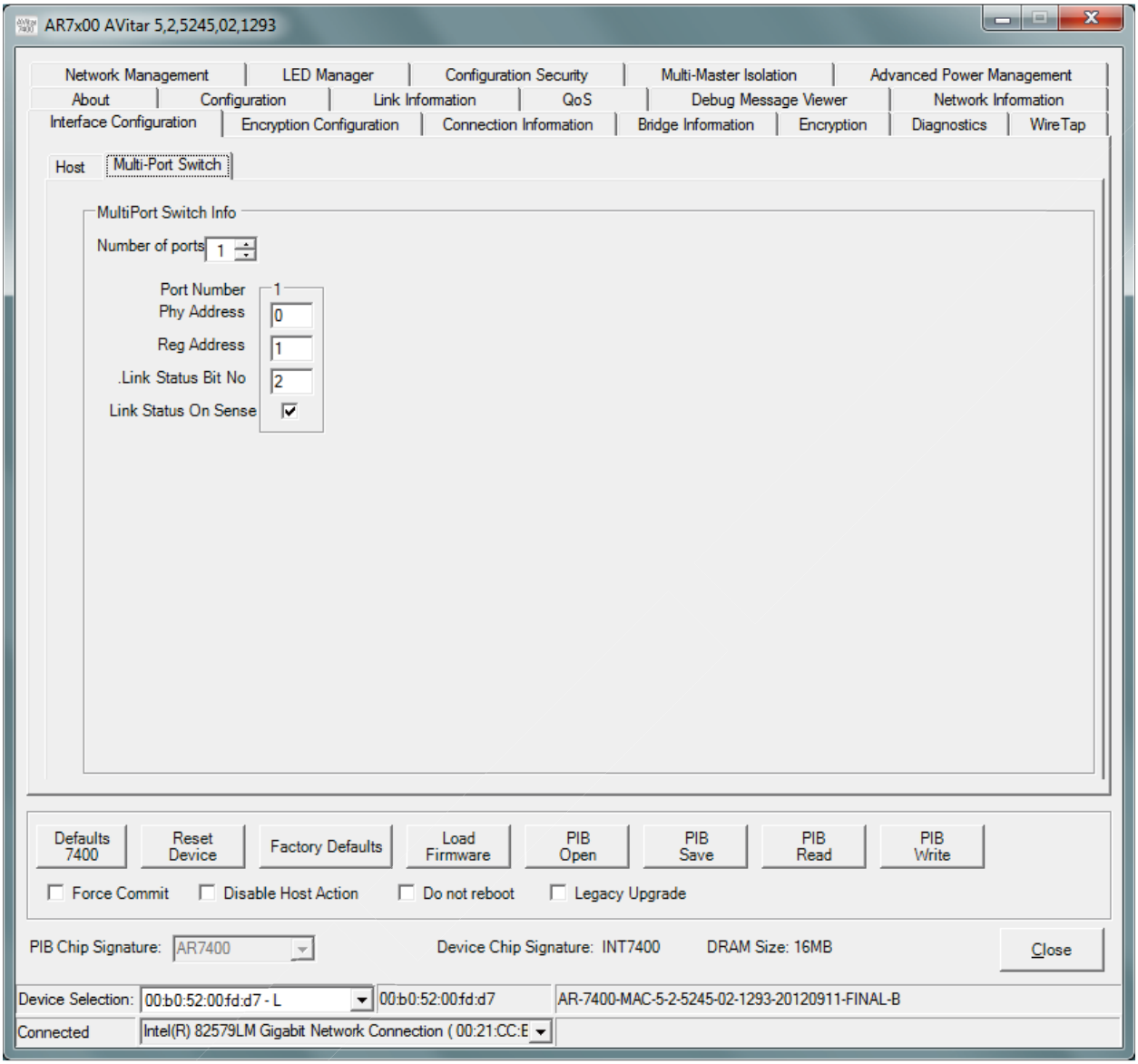


Figure 3-25: Multi-Port Switch Tab Showing Single Port Application

3.15.6.1 Number of Ports

Specifies the physical number of Ethernet PHY ports present on the multi-port PHY device

3.15.6.2 PHY Address

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

3.15.6.3 Reg Address

Specifies hardware register address used by the switch chip that corresponds to Port Number

3.15.6.4 Link Status bit

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

3.15.6.5 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.

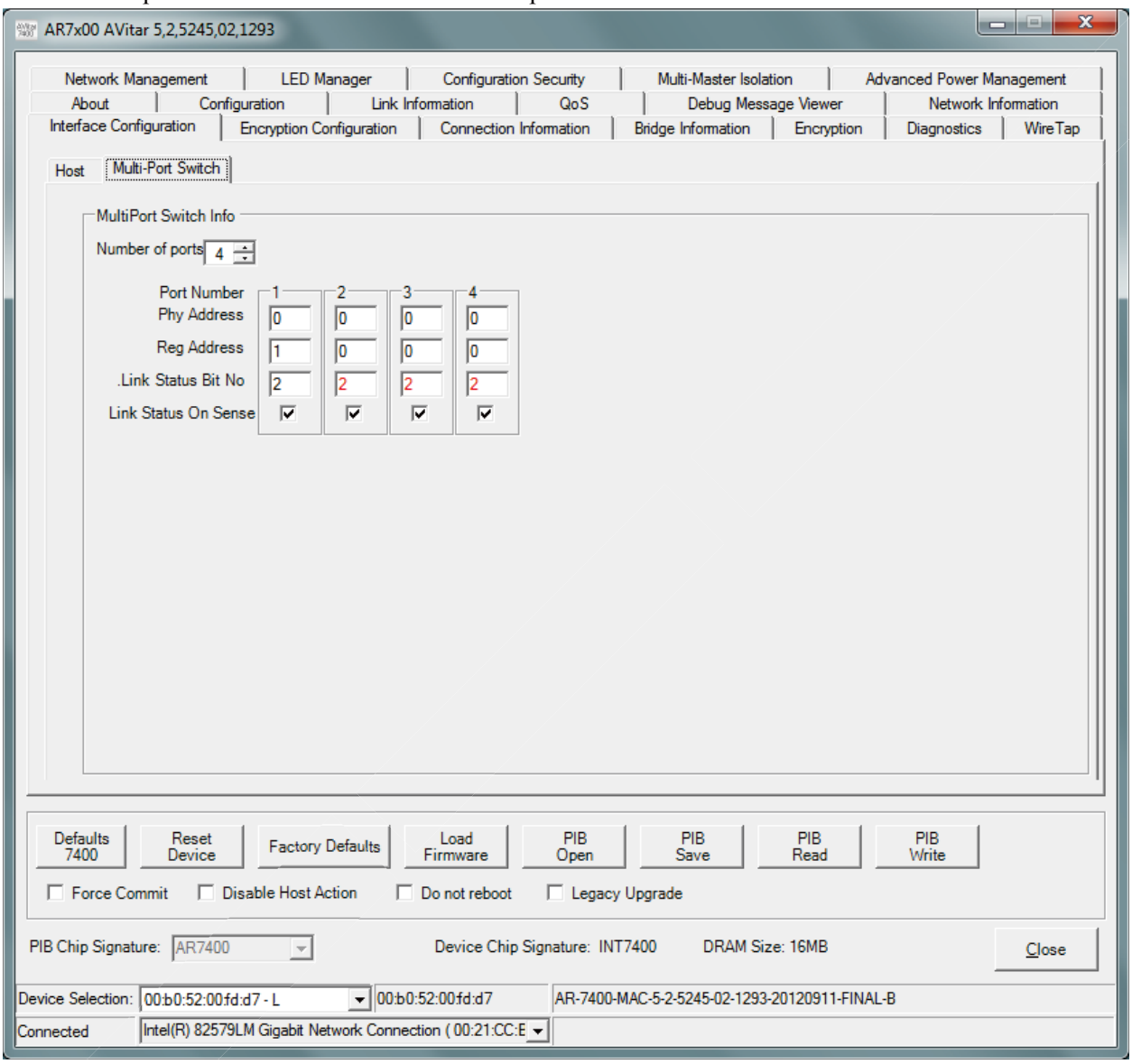


Figure 3-26: Multi-Port Switch Tab Showing Four Port Application

NOTE: The multi-port switch devices need to configure the AR7400 device for MAC mode operation to enable firmware access to the switch chip MDIO interface. This configuration is also required to use the Multi-Port Switch Standby feature.

3.16 Encryption Configuration Tab *(Configuration Window)*

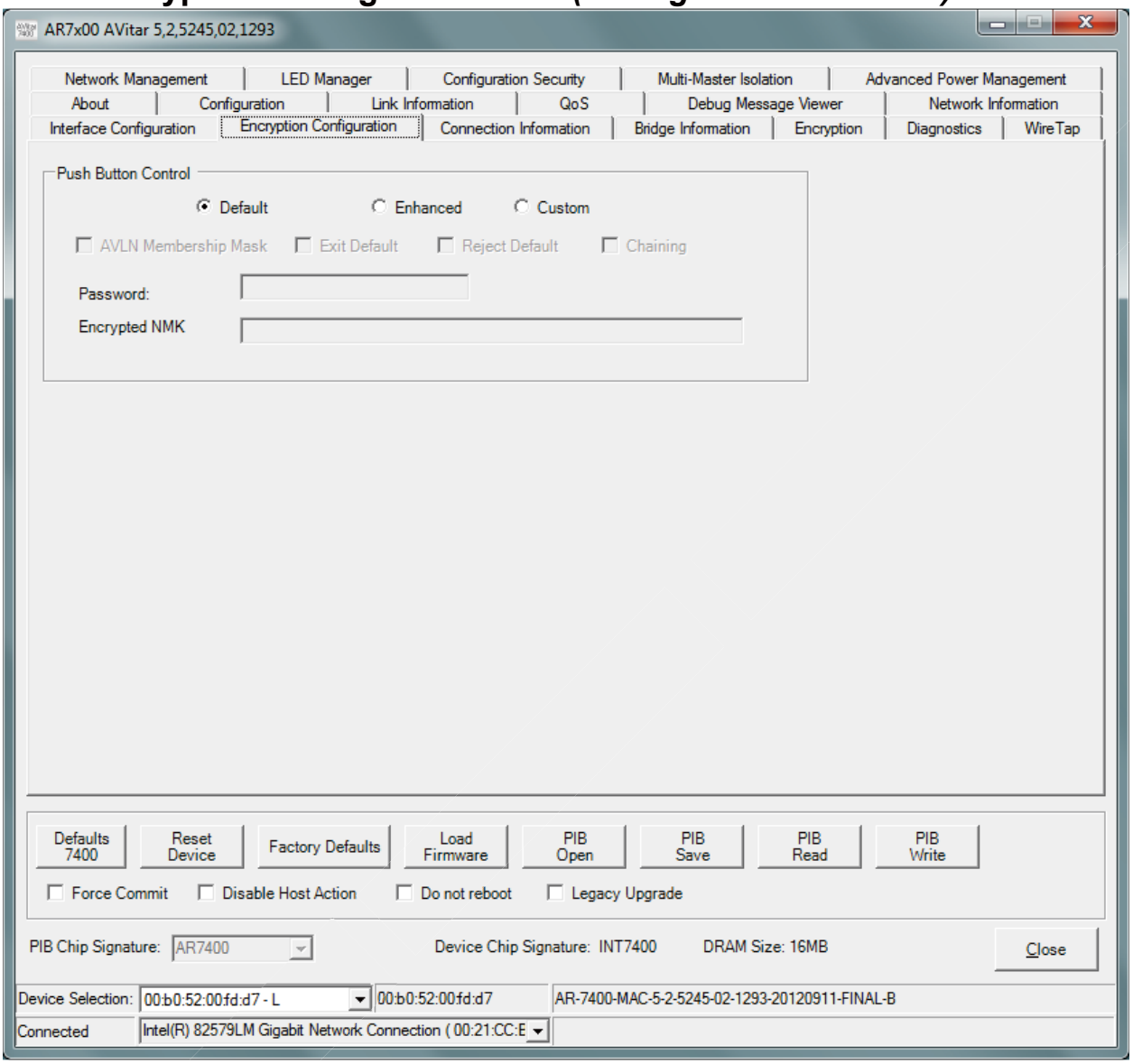


Figure 3-27: Encryption Configuration Tab Window

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

3.16.1 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.

3.16.2 Enhanced

Enables the following fields in their default configuration (see Table 1).

3.16.3 Custom

Enables the following fields (see Table 3-3) 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.

Table 3-3: Summary of Push Button Behavior Customization Defaults

PIB Fields	ALVN Membership Mask (See Section 3.11.4)	Exit Default (See Section 3.11.5)	Reject Default (See Section 3.11.6)	Chaining (See Section 3.11.7)
Default	N/A	N/A	N/A	N/A
Enhanced	Default On, Not User Selectable	Default On, Not User Selectable	Default On, Not User Selectable	Default Off, User Selectable
Custom	Default Off, User Selectable	Default Off, User Selectable	Default Off, User Selectable	Default Off, User Selectable

3.16.4 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.

3.16.5 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.

3.16.6 Reject Default

Devices shall neither propagate nor accept either the password HomePlugAV or the password hash stored as the vendor-specific default password.

3.16.7 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.

3.17 Connection Information Tab *(Operation Analysis Window)*

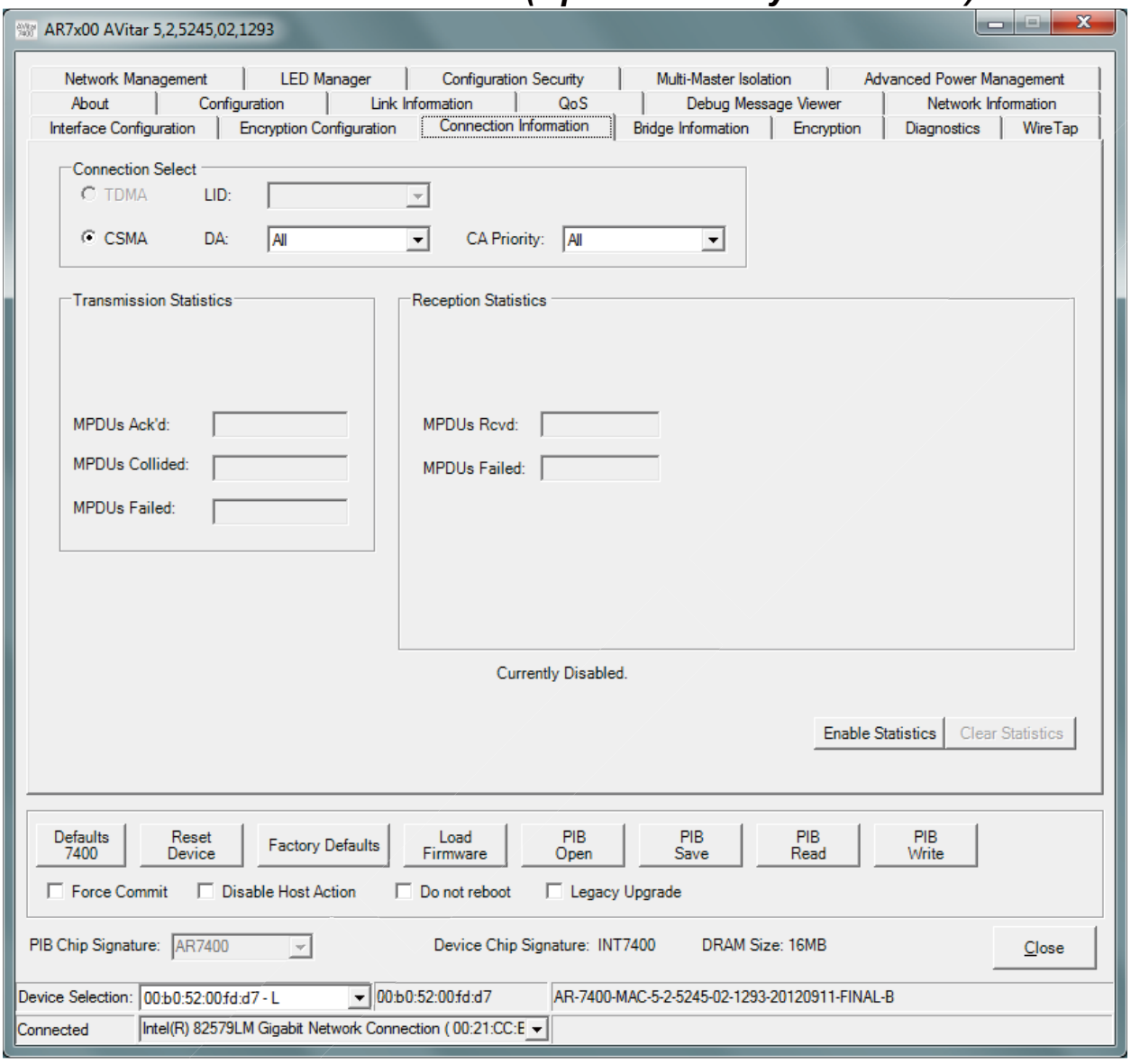


Figure 3-28: Connection Information Tab Window

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

3.17.1 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

3.17.2 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.

3.18 Bridge Information *(Operation Analysis Window)*

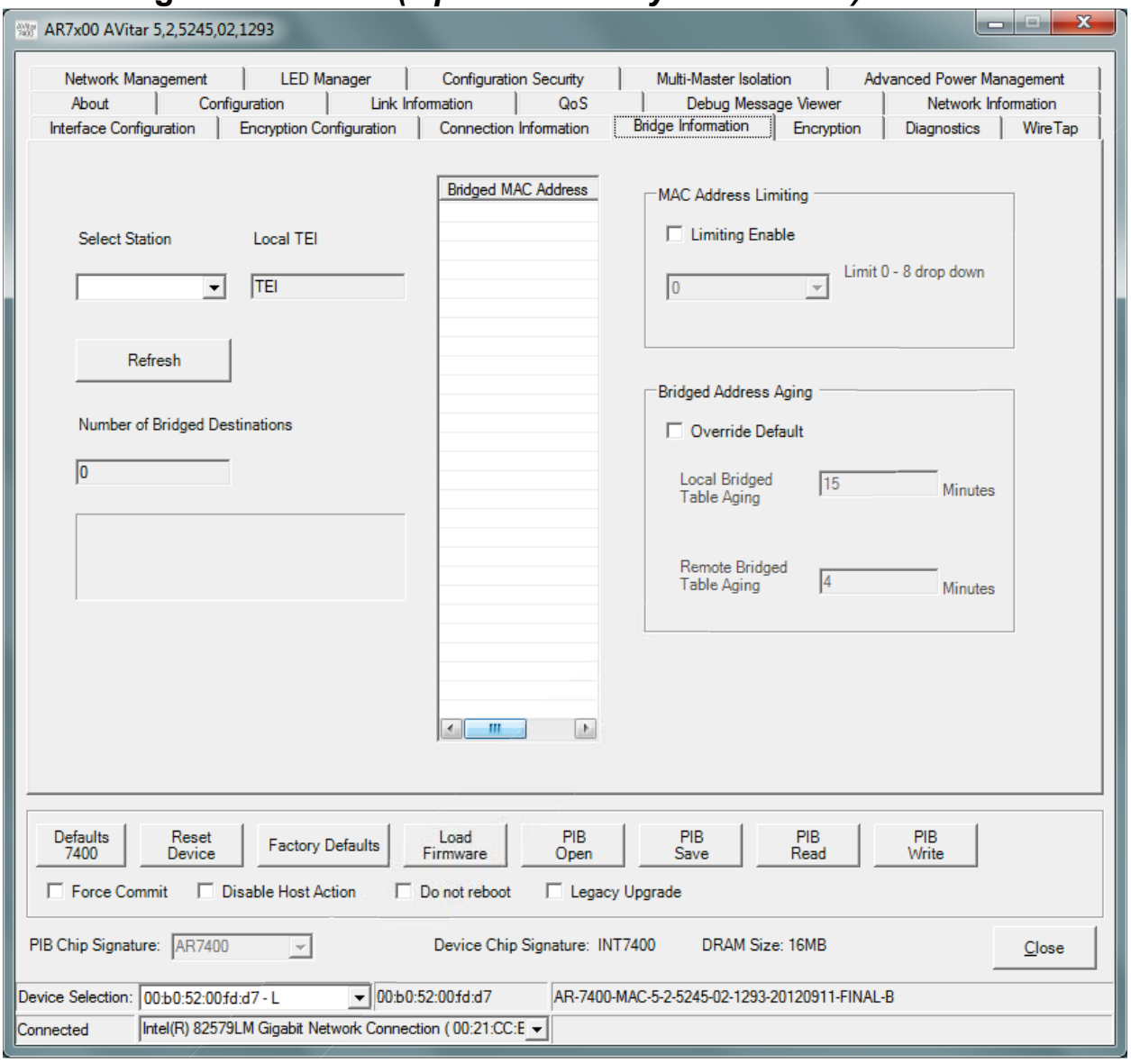


Figure 3-29: Bridge Information Tab Window

3.18.1 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.

3.19 Encryption Tab *(Configuration Window)*

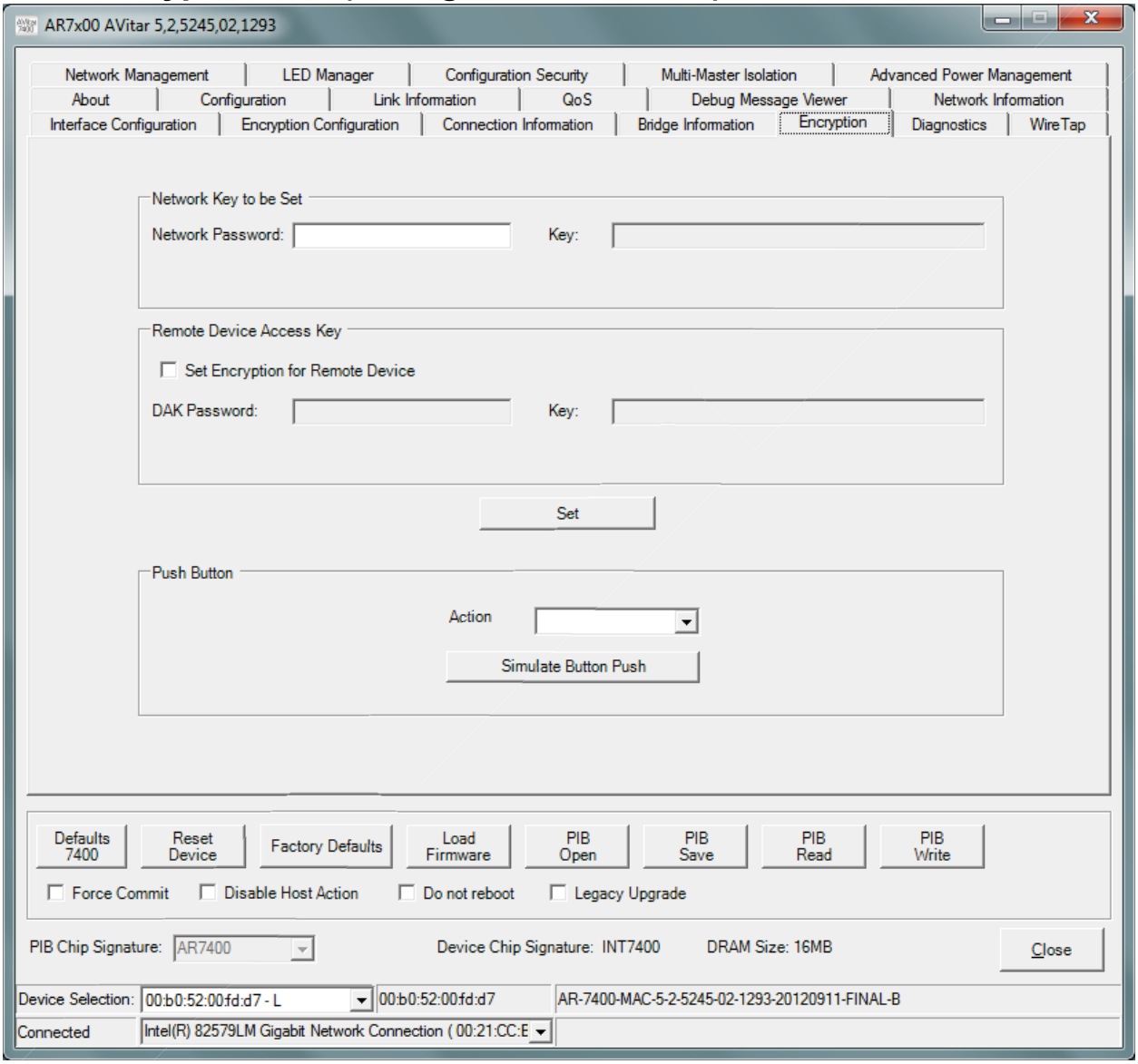


Figure 3-30: Encryption Tab Window

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.

3.20 Diagnostics Tab *(Event Log)*

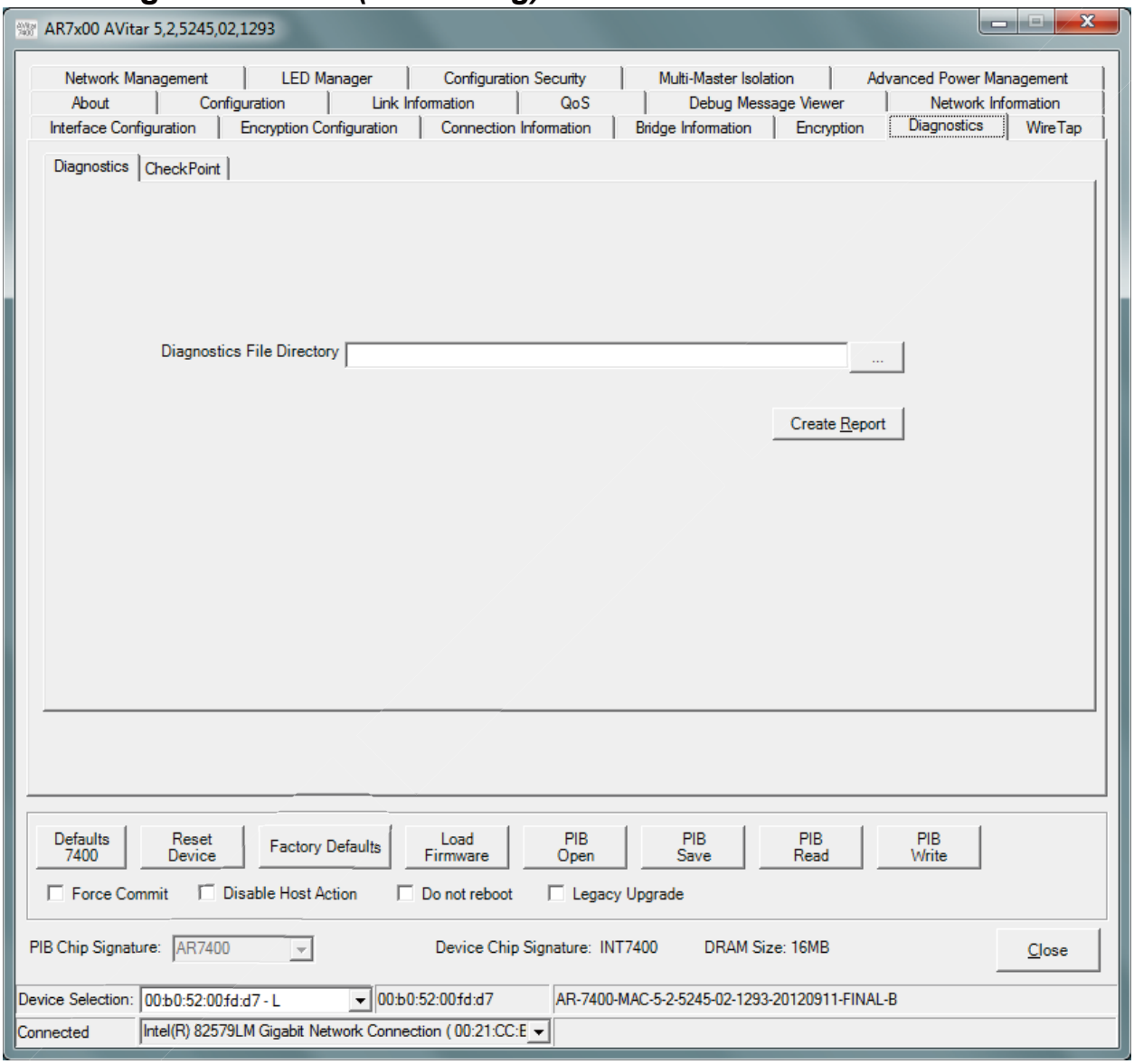


Figure 3-31: Diagnostics Tab Window

3.20.1 Two Sub-tabs

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

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 Qualcomm Atheros field application engineers.

3.21 WireTap *(Configuration Window)*

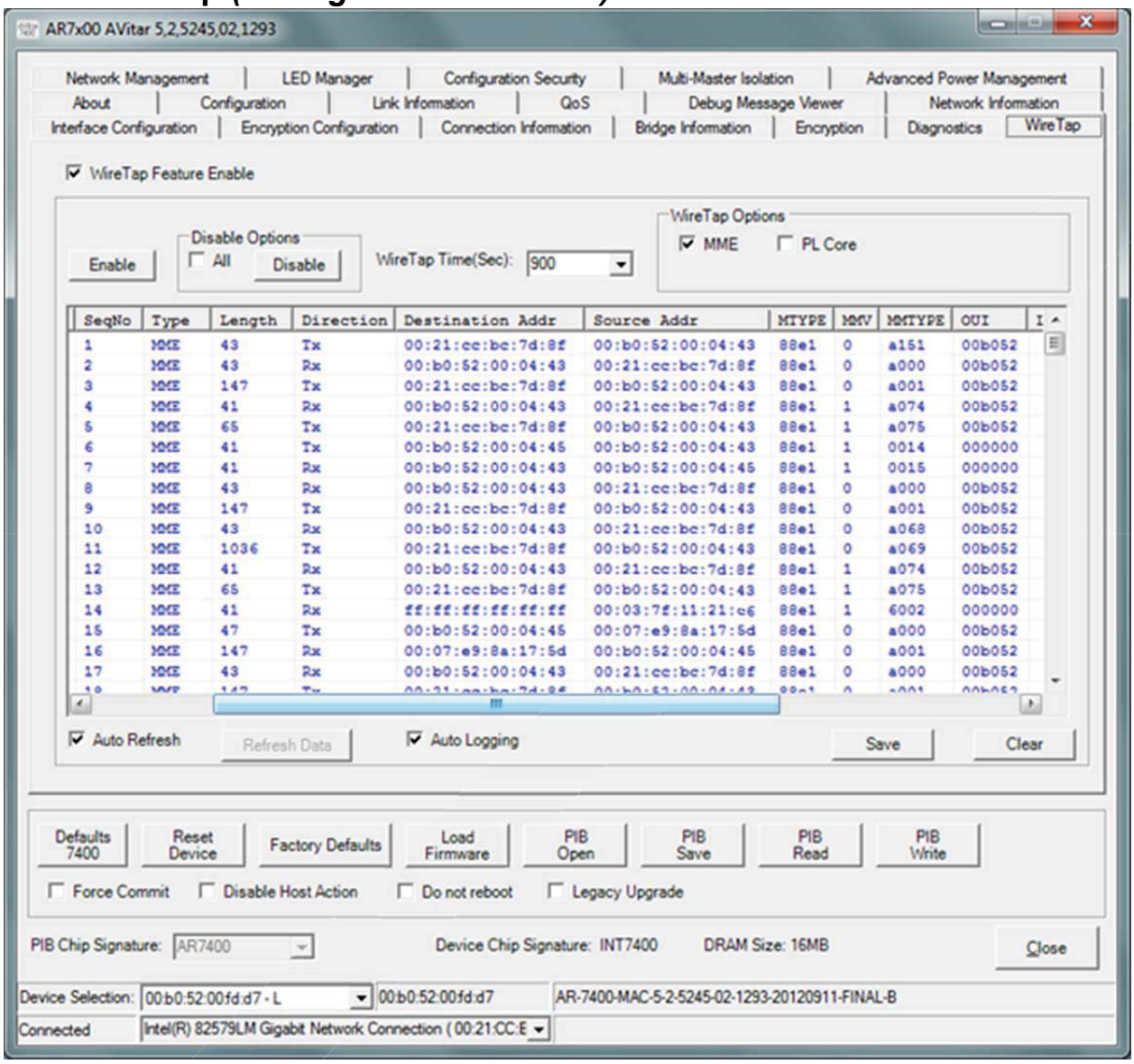


Figure 3-32: WireTap MME Capture

This is an example of MME traffic.

Enable the WireTap Feature in PIB by selecting the WireTap Feature Enable flag and write the configuration in the PIB.

Enable/Disable Options start and stop respectively the WireTap sniffing. Using Disable all option, the WireTap sessions could be terminated on all devices.

Unless stopped, Sniffing will continue for the time configured under 'WireTap Time(Sec)' – this defaults to 900 (i.e. 15 minutes)

Sniffing options includes either 'MME' or 'PL Core' (i.e. Beacons) or both.

All Sniffed information can be stored in a file using the 'Save' button. The 'Auto Logging' option when enabled will save Sniffed data automatically into .CSV file in the COMMON DOCUMENTS directory (e.g. c:\All Users\Documents\Qualcomm Atheros\AVitar).

Display data can be cleared using the 'Clear' button, refreshed using 'Refresh' button, the latter being done automatically with 'Auto Refresh' enabled.

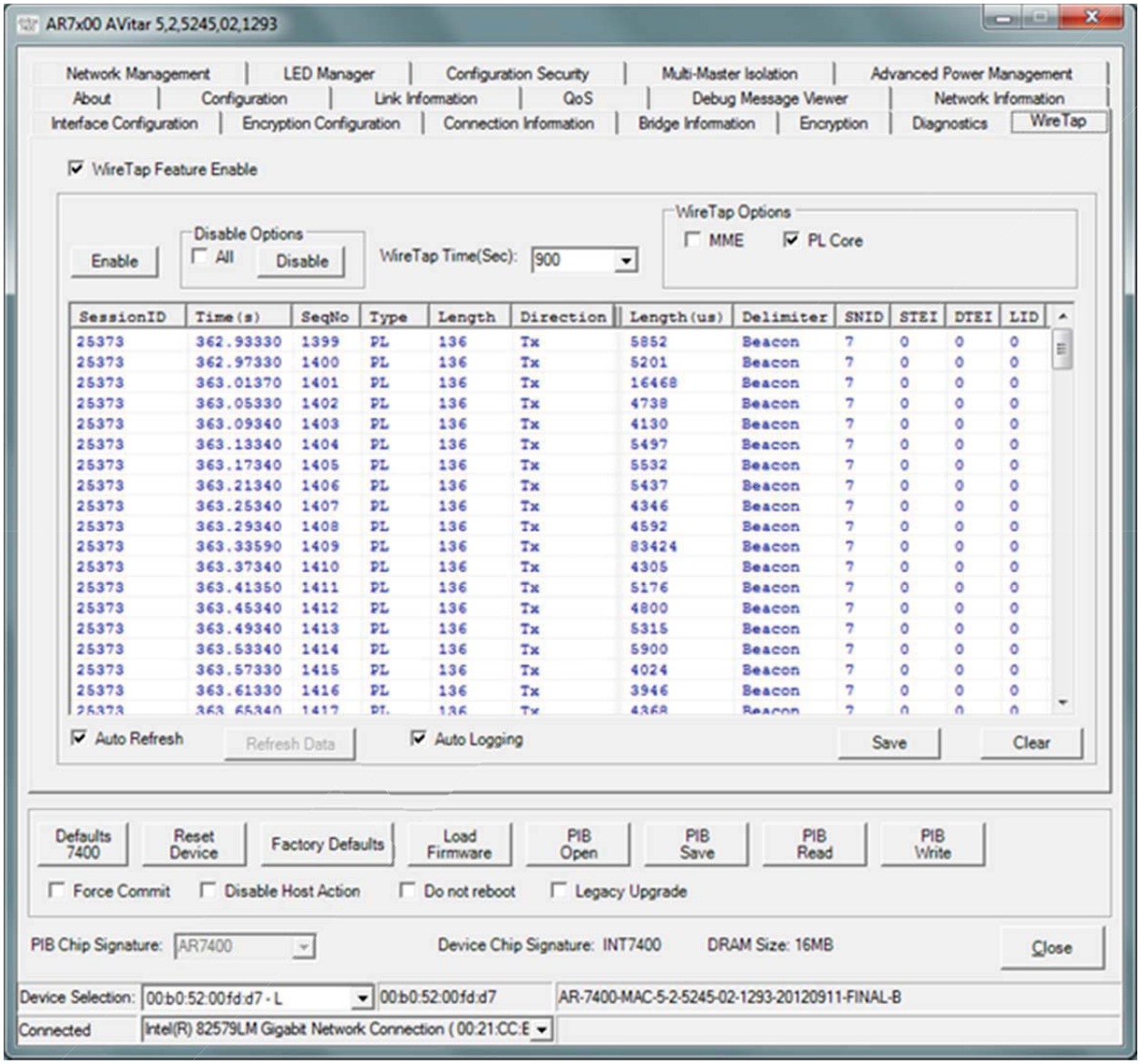


Figure 3-33: WireTap PL Data Capture

This is an example of PLC traffic.

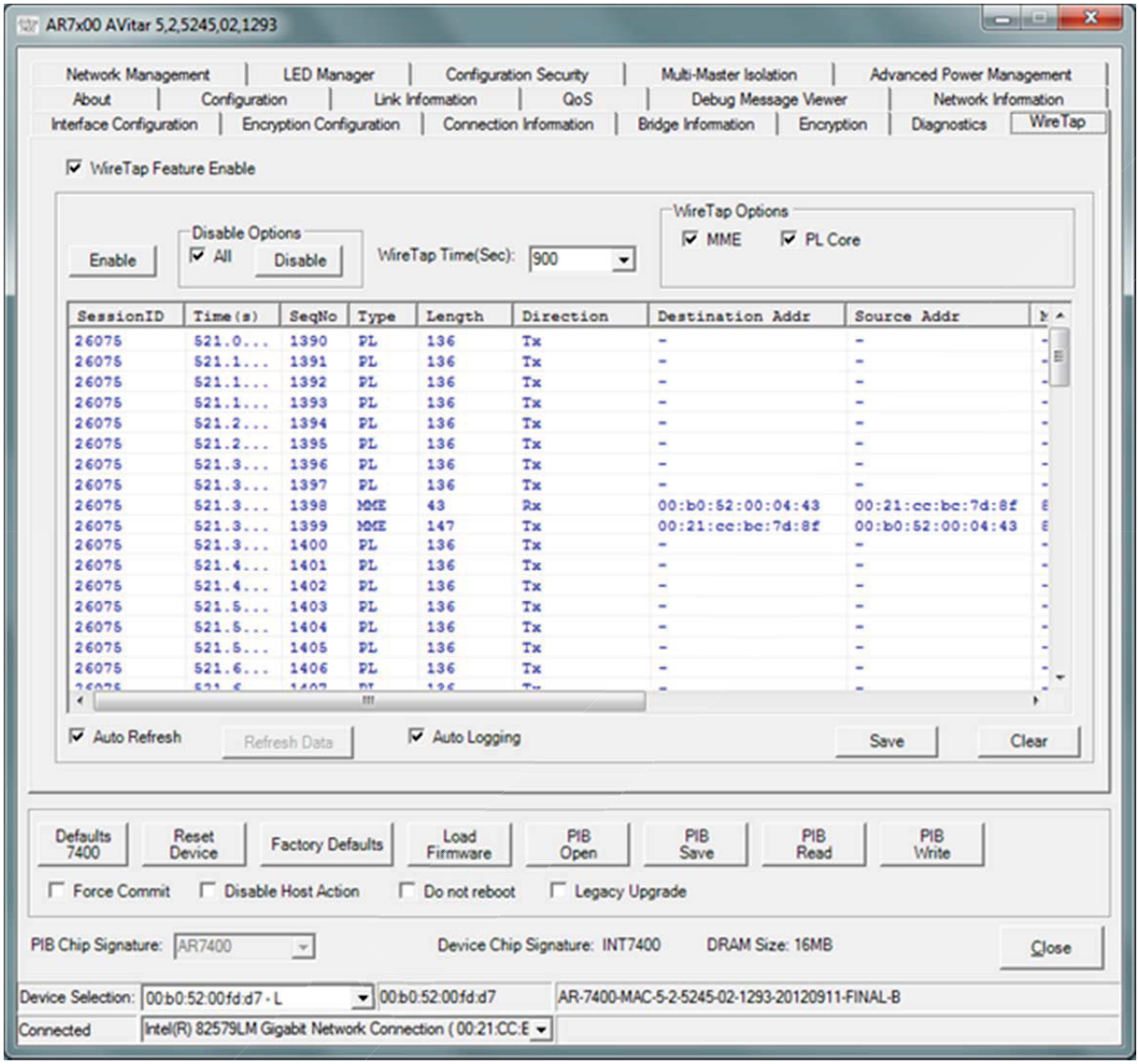


Figure 3-34: Capture Both MME & PL Data in Remote Device

This is an example of both MME and PLC traffic.

Appendix A: AR7400 Amplitude Map Modification

Windowed OFDM is used in the PHY layer as the analog medium interface. The Atheros IEEE 1901 Extended spectrum extends from approximately 1.8 MHz to 67.5 MHz and is divided into 2690 separately modulated carriers (tones). Absolute Tone Index 0 is 0 Hz. Relative Tone Index 0 occurs at Absolute Tone Index 74. When reading or writing a prescaler, exactly 2880 pairs of data are expected in a fixed format: The first element is the relative tone number in decimal, the second value is the tone amplitude adjustment value (prescaler value) expressed in hexadecimal format. Relative tones 2690 through 2879 are not enabled, but are required in this format.

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

Relative Tone Index Column: The first (left-hand) column is the relative tone index, a list of all 2880 tones in decimal numerical order. The actual frequency of any tone can be determined as follows:

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

Examples: Relative Tone Index = 0 and frequency = 1.806 MHz,
Relative Tone Index = 1154 and frequency = 29.98 MHz,
Relative Tone Index = 2689 and frequency = 67.46 MHz

Prescaler Value Column: The second column is the assigned amplitude or prescaler value expressed in hexadecimal. The amplitude of a carrier (tone) is set by entering a hexadecimal prescaler value next to the tone index number, with one space separation. The maximum hexadecimal value is **0x3ff** which is equal to **1023** decimal. The hexadecimal value is derived from the desired amplitude level in decibels according to this formula:

Decibels = 20* $\log_{10}$(prescaler value/1024)

Resolve this formula for the 'prescaler value':
Prescaler value = 1024*[Inverse log $_{10}$(Decibels/20)]

The prescaler value 0 is a special case. This value indicates that this tone is turned off; i.e. this tone is not used.

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 Qualcomm Atheros corded Ethernet adapter (PL19/PL21 Reference Designs). 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.

The prescaler 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. Only integer values are allowed.

NOTE: The prescaler value is a numerical value that represents the tone's amplitude relative to full scale. For example: a prescaler value of 128 (decimal) indicates that the amplitude is 128/1024 = a multiplication factor of 0.25, which means the tone's power level, is one quarter of the reference level, or -12 dB (12 dB below the reference level). The maximum decimal range for the AR7400 prescaler value is from 0 to 1023 (0x3FF).

Examples Table

Prescale Value (Decimal)	Hexadecimal	Relative Amplitude PV/1024	dB
1023	000003FF	.999	~0
512	00000200	0.5	-6
256	00000100	.25	-12
64	00000040	0.0625	-24
26	0000001A	0.02539	-31.9
1	00000001	0.000976	-60.2
0	00000000	0	Off

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 AVitar.

Appendix B: Acronyms and Abbreviations

Acronyms	Definition
API	Application Programming Interface
AVLN	HomePlug AV Logical Network
CAP	Channel Access Priority
CCo	Central Coordinator
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
DRAM	Dynamic Random Access Memory
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

4. Trouble Shooting

1. Why my utility can not work properly after finish install steps?

Ans:

Please follow the steps to check the problem.

1. Check the Windows version, the utility only can support windows 2000, XP, 2003, vista and Win7.
2. Reinstall the utility again, you can remove it and reinstall the utility again

2. What kind of windows OS can install the Powerline utility?

Ans:

Now the Powerline utility only supports Windows 2000, XP, 2003, Vista and Win7.

3. Why the throughput of Powerline 500M bridge is bad?

Ans:

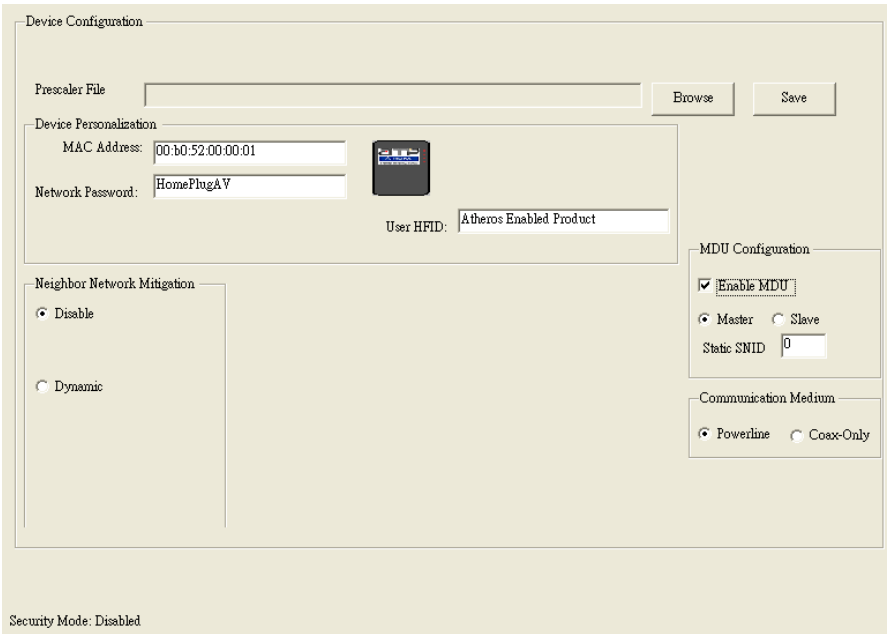
Please follow the steps to check the problem.

1. Due to the master/slave structure, you need to avoid plugging two Powerline bridge in the same time, so you had better plug the Powerline to the power outlet sequence.
2. Please unplug the Powerline bridge and plug again, please remember plug them in sequence. Check the Powerline utility and check the throughput again.

4. How to set MDU's Master/Slave for system integrator?

Ans:

The AVitar utility can enable MDU function and setup Master or Slave.



5. If need to use the Powerline/Cable in home, how can I do?

Ans: If the Powerline/Cable 500M Bridge need use with Powerline Bridge, the switch need switch to PL/Cable mode and set the Powerline/Cable 500M Bridge to Bridge mode, due to keep the high performance, use the high-pass filter to filter the signal interference from cable modem, the application as follows.