PRIME Products

PRIME Manager User Guide

Overview

The PRIME Manager is a PC software application that connects to Service or Base Nodes allowing easy management of the device functionality.

Features

- Connection by USI Protocol to PRIME Devices
- Supports PRIME 1.3 Service Nodes with Firmware Version 1.3.9.0 or Later
- Supports PRIME 1.3 Base Nodes with Firmware Version 1.3.10.0 or Later
- Supports PRIME 1.4 Service or Base Nodes with Firmware 1.4.1.0 or Later
- Multi-Client Connection
- PRIME API Management
- Manage Certification
- Manage MTP
- Embedded Sniffer Support
- Run DLMS Over TCP Protocol as Application (Base Node)
- Run PRIME Over UDP as Application (Base and Service Node, PRIME 1.3 Only)
- USI Serial Profile Certification Bridge
- Firmware Upgrade with Signature Options (PRIME 1.4)
- Python Script Example to Sign Firmware Files

Table of Contents

Overview....1

Features....1

1. Introduction....4
   - 1.1. Description....4
   - 1.2. Application Structure....4

2. Initial Steps....5
   - 2.1. Software Installation....5
   - 2.2. Target Firmware....6
   - 2.3. Starting....6

3. Network Topology View....11
   - 3.1. Info Request Dialog....12
   - 3.2. Network Management Dialog....12
   - 3.3. Firmware Upgrade Management Dialog....13

4. Base Management View....14
   - 4.1. Signing Firmware....15

5. PRIME Management View....16
   - 5.1. PLME/MLME PIBs....16
   - 5.2. Serial Profile....17
   - 5.3. PRIME Profile....17
   - 5.4. MAC....18
   - 5.5. 4-32....18
   - 5.6. PLME....19
   - 5.7. MLME....20
   - 5.8. Certification....21
   - 5.9. Manufacturing (MTP) Test....22
   - 5.10. PRIME over UDP (PRIME 1.3 only)....23

6. Sniffer Window....24

7. Revision History....25
   - 7.1. Rev A - 02/2015....25
   - 7.2. Rev B - 01/2016....25
   - 7.3. Rev C - 09/2016....25
   - 7.4. Microchip Rev A - 06/2018....25

The Microchip Web Site....26

Customer Change Notification Service....26

Customer Support..... 26

Microchip Devices Code Protection Feature..... 26

Legal Notice.....27

Trademarks..... 27

Quality Management System Certified by DNV.....28

Worldwide Sales and Service.....29

1. Introduction

1.1 Description

The PRIME Manager is used to monitor and manage PRIME power line networks. This tool requires a hardware device connected to the power line.

The PRIME Manager can be used for:

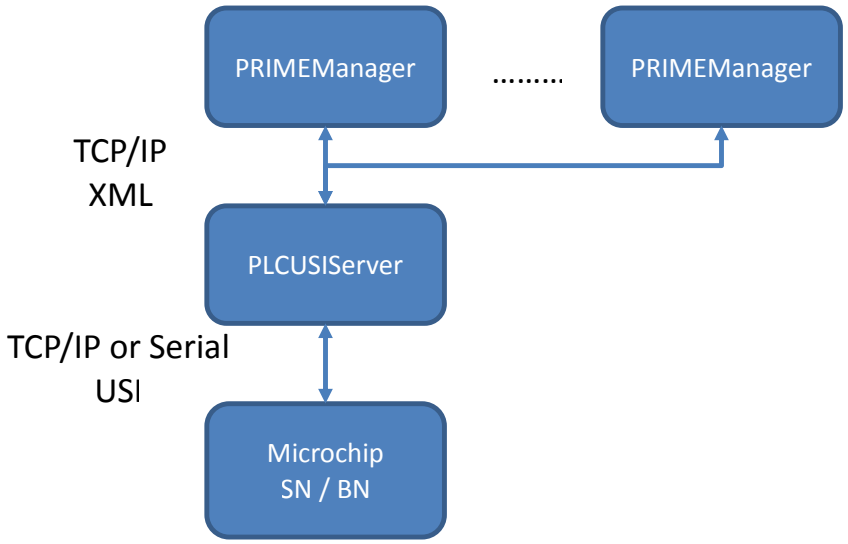
- PIB management
- Testing embedded firmware
- Monitorizing embedded Sniffer

The USI messages are processed and the results displayed in the different views of the main window (see Figure 2-9).

1.2 Application Structure

The application is designed with the following structure:

Figure 1-1. Application Structure



The *PRIMEManager* is the main application – it configures and launches the *PLCUSIServer* application and its USI connection. The *PLCUSIServer* allows connection of several *PRIMEManager* instances.

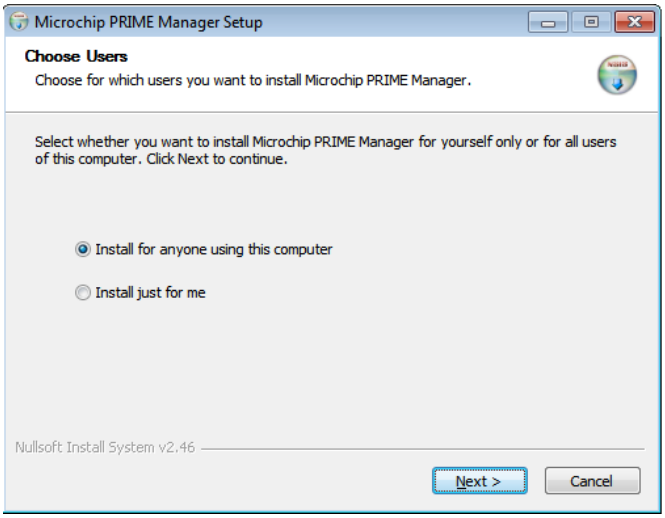
2. Initial Steps

2.1 Software Installation

To install the software, execute the provided installation wizard.

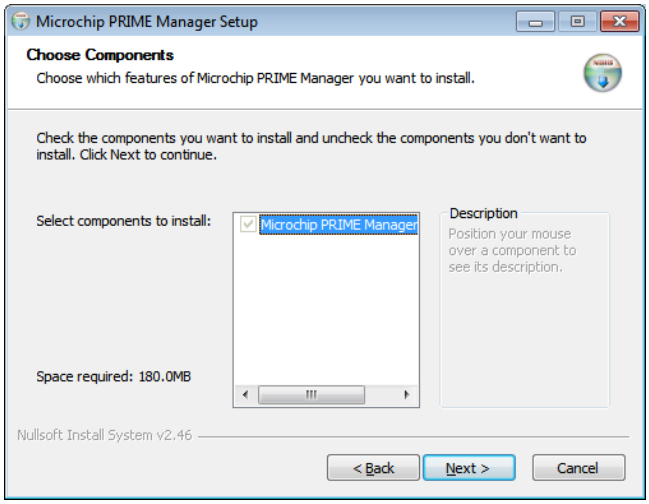
First, select between multiuser support or current user.

Figure 2-1. First Wizard Window



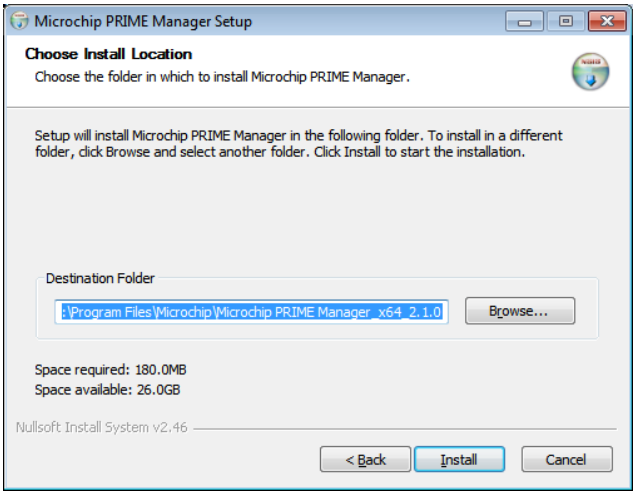
Next, select the components to install.

Figure 2-2. Select Components



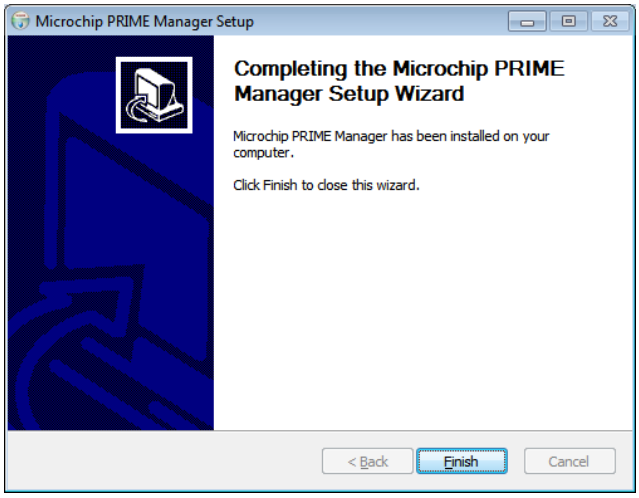
And finally, select the folder where the software must be installed or just simply use the default location.

Figure 2-3. Select Folder



The installation does not require any other configuration.

Figure 2-4. Installation Completed



The installation procedure generates a desktop link and start menu link. Use any of them to start PRIME Manager.

2.2 Target Firmware

Along with the Microchip PLC Kit, you have received the instructions to build/install the appropriate firmware in your hardware devices. Refer to the “Kit User Manual” to install the appropriate Base/Service Node firmware.

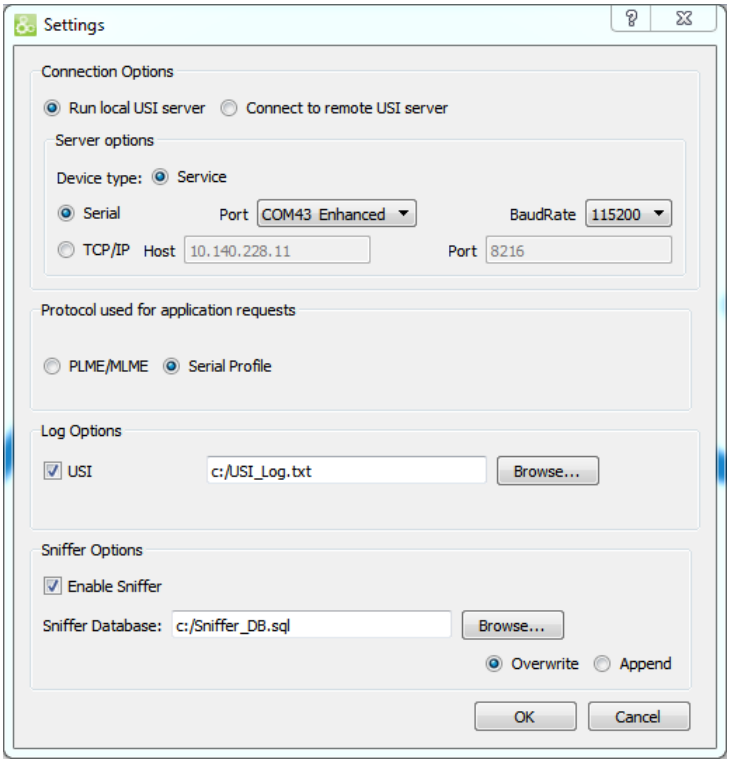
2.3 Starting

First, plug the hardware device to the power line. Then, connect the USB cable to the host computer. Finally, start the PRIME Manager using, for example, the link created on your desktop during the install process. This opens the main window.

Figure 2-5. PRIME Manager Main Window

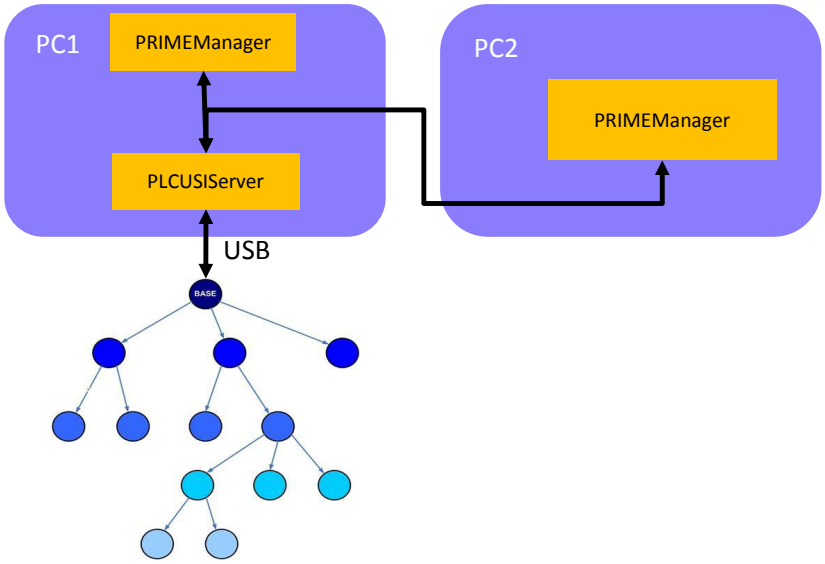
In order to connect, the user needs to setup input and log parameters through the settings window. To modify the settings, click File>Settings on the menu and the settings window will be shown (Figure 2-6). First, choose between running a local USI server (PLCUSIServer) instance or connecting to a remote USI server.

Figure 2-6. Settings Window



The normal usage is to run a local server and connect by USB (PC1 in Figure 2-7). After that, choose between serial and TCP/IP link for the hardware connection. When running a local server, the TCP/IP option allows the connection to a UART Hub or USI Splitter.

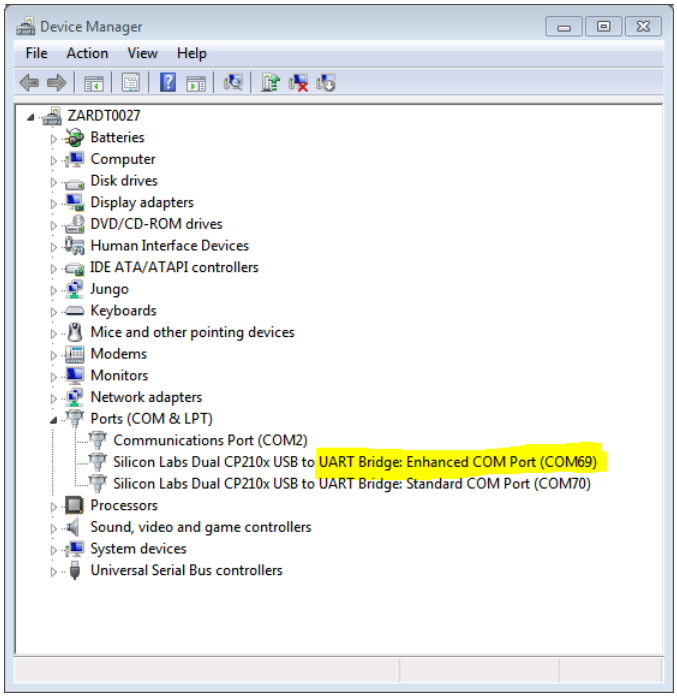
Figure 2-7. Connection Diagram



When connecting to remote server (PC2 in Figure 2-7), the TCP/IP option requires the IP address of the server (PC1) and the opened port by the server. Note that the opened port is shown in the status bar of the tool.

If the COM port is not known, it can be located at the Windows Device Manager in the Port (COM & LPT) section. In this example, COM69 is used:

Figure 2-8. Windows Device Manager



Note: Some Microchip kits use a dual USB UART Bridge providing two COM devices on the same USB cable. Firmware is configured to use the "Enhanced COM Port" by default.

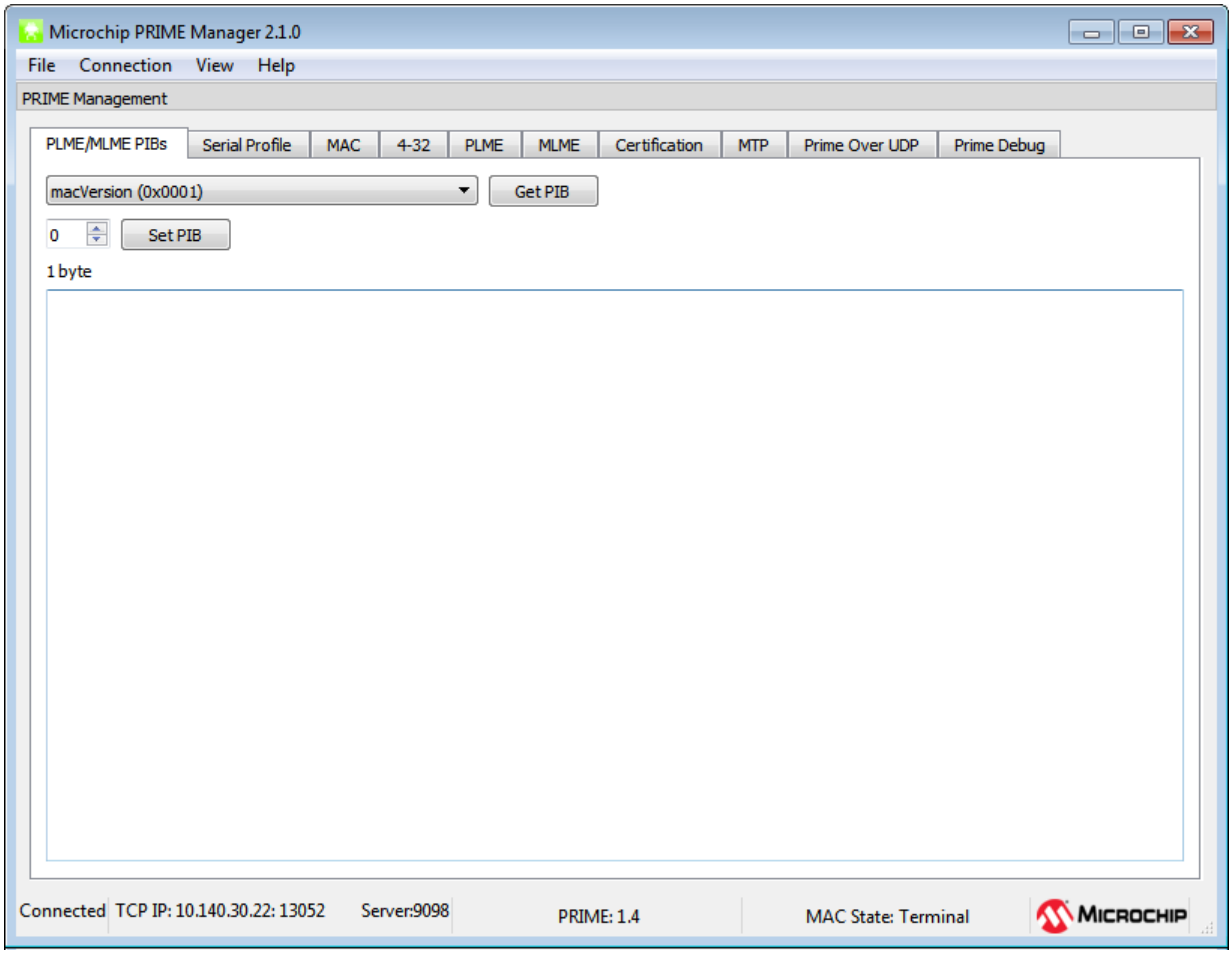
Sniffer options (Figure 2-6) allow enabling the embedded sniffer. The database to store the sniffer log can be selected. Furthermore, overwrite or append options can be selected.

It is also possible to enable a USI log (see Figure 2-6). If it is enabled, all USI traffic from PC to device and from device to PC will be written on the selected text file. It can be useful for debugging.

The protocol used for application requests (see Figure 2-6) can be chosen (PLME/MLME or Serial Profile). This is the protocol that will be used to get/set PIBs automatically by the tool. If both PRIME API and MNGP (Serial Profile) are serialized, this option is not of relevance, but it can be useful if one of those protocols is not serialized.

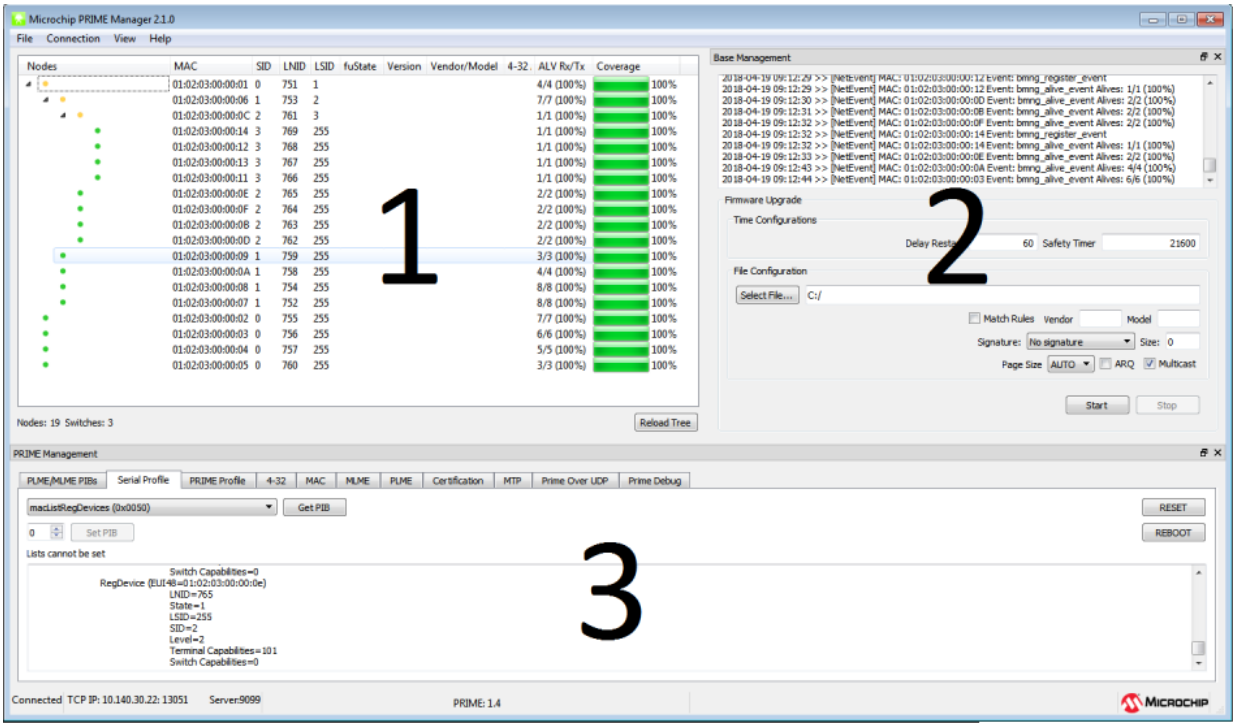
Now, the tool is ready to connect. Accept the changes and click on menu Connection>Connect in the Main Window to start. The status bar at the bottom of the window will show the current setup and the status of the tool. The Main Window is shown in the next figure.

Figure 2-9. Main Window when Connected to a Service Node



When clicking Connect, if the sniffer was enabled in the settings dialog, a new window would be shown with the sniffer (see section 3. Network Topology View). Such window is similar to the PLC Sniffer tool. Note that once the tool is connected, it is not possible to show the sniffer if it was not activated before clicking Connect.

Figure 2-10. Main Window when Connected to a Base Node

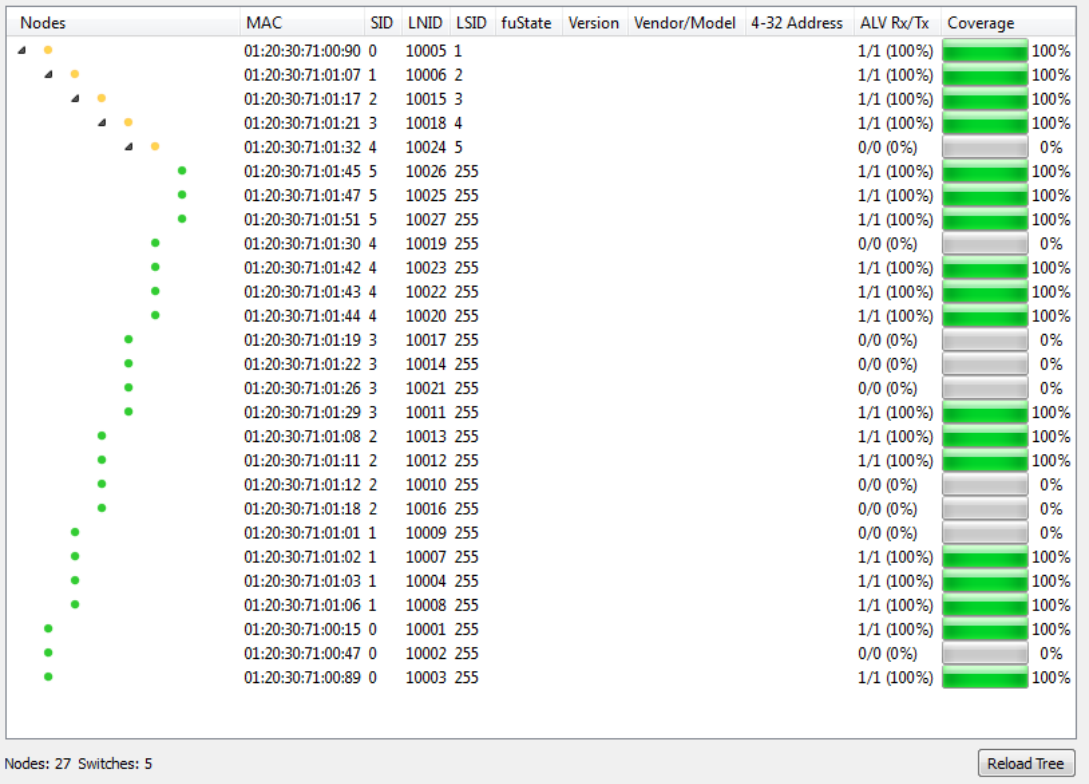


1. **Network Topology view.** This is the basic presentation in the main application window and it is always visible when connected to a Base Node. It is not available when connected to a Service Node. This view displays the logical network structure. The structure is inferred analyzing the network events received from the Base Node. In addition, this view shows node information such as MAC, LNID, LSID, SID, firmware upgrade state, firmware version, model and vendor, 4-32 address, ALV message count and coverage
2. **Firmware Upgrade view.** This view displays firmware upgrade options and information about the current upgrade process. It is not available when connected to a Service Node
3. **PRIME Management.** This view allows requesting information and other functionalities provided by the different protocols available in the tabs. It is available in both Base and Service Node connection, but there are some differences (to be described in section 5. PRIME Management View)

3. Network Topology View

The Network Topology View looks like this:

Figure 3-1. Network Topology View Showing a 27-node Network



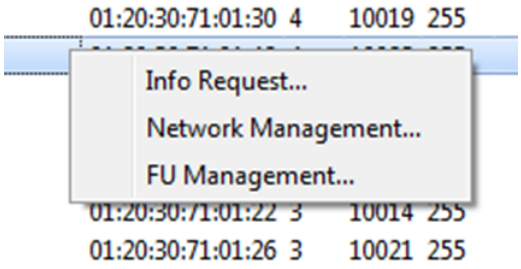
This view shows the current status of the network inferred by the tool. It is automatically refreshed every time a change in the network is detected; for example, a new device is registered or promoted to switch. It is also possible to refresh this view with the Reload Tree button, which requests to the Base Node the list of registered nodes in order to rebuild the network structure. This is useful if network events were lost and thus the topology is not up-to-date.

This view displays the following information:

- Node State. A green dot is a terminal node and a yellow dot is a switch node
- MAC address
- SID (Switch Identifier)
- LNID (Local Node Identifier)
- LSID (Local Switch Identifier)
- fuState (Firmware Upgrade State)
- Firmware version
- Firmware vendor and model
- 4-32 Address
- ALV Rx/Tx (number of ALV messages received and transmitted)
- Coverage (moving average with the last three ALV messages)

There is a right-click menu in this view with further options, as shown in the following figure:

Figure 3-2. Right-Click Menu



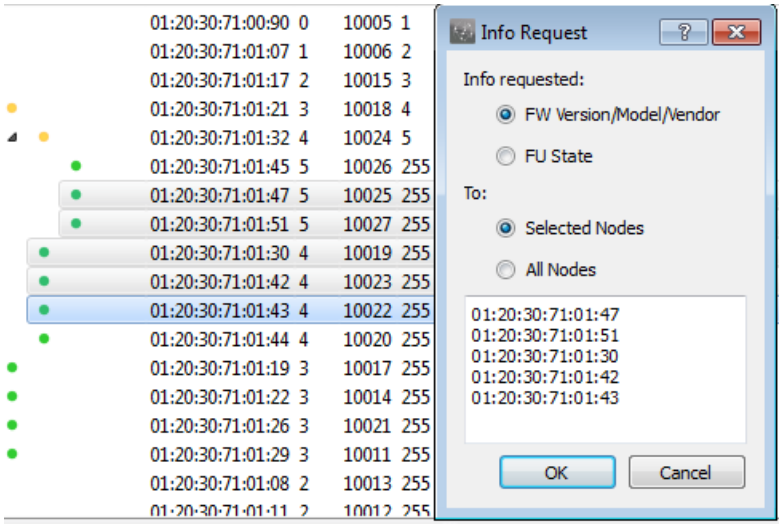
3.1 Info Request Dialog

This dialog allows requesting information from the Service Nodes by means of the Base Management Protocol.

Available information to be requested is firmware version, model and vendor, and firmware state. The firmware state is only returned when a firmware upgrade process is running. The responses will be shown in the rows of Figure 3-1.

The information can be requested to all registered nodes or just to selected nodes (multiple selection is enabled in Network Topology View).

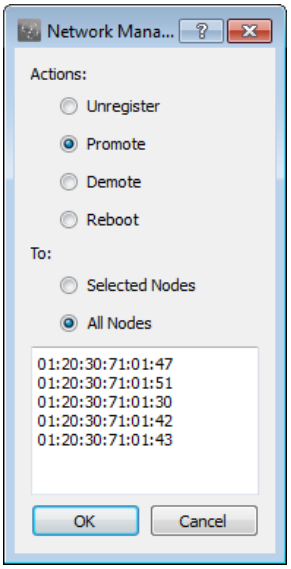
Figure 3-3. Info Request Dialog



3.2 Network Management Dialog

This dialog lets the user manage the network with functions Unregister, Promote, Demote and Reboot.

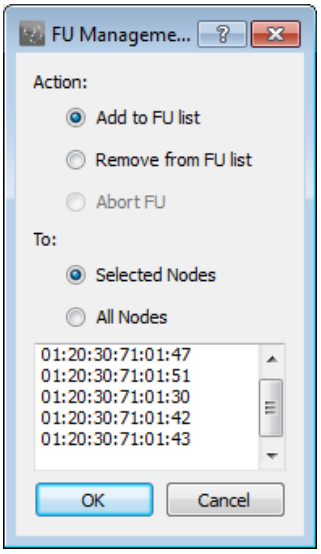
Figure 3-4. Network Management Dialog



3.3 Firmware Upgrade Management Dialog

The available options in this dialog depend on whether or not a firmware upgrade process is running. When not running, nodes can be added to and removed from the list. When the process starts, the Remove option is disabled but the Abort option is enabled so that the upgrade process can be cancelled at any time. It is always possible to add nodes to the list.

Figure 3-5. Firmware Upgrade Management Dialog



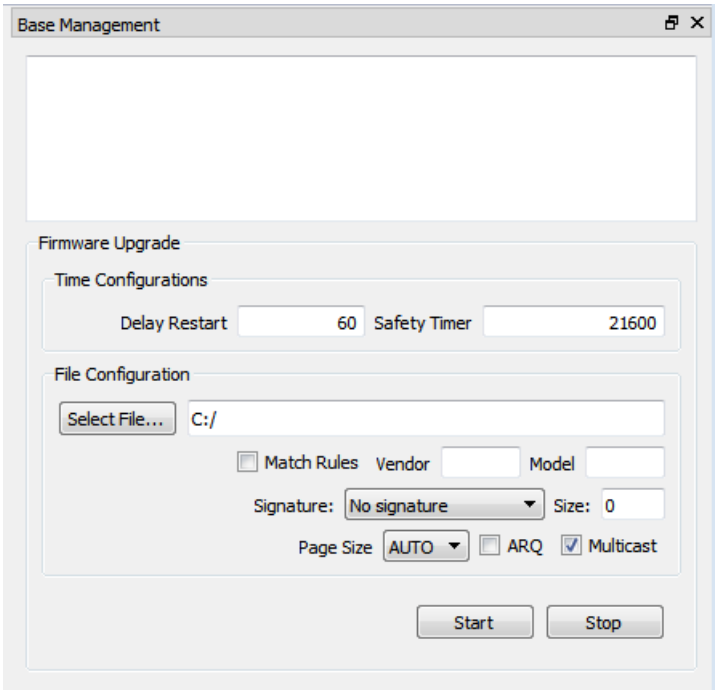
This dialog only adds the nodes to the Firmware Upgrade, but the process does not start when the OK button is clicked. The next section describes how to start the Firmware Upgrade Process.

4. Base Management View

This view allows the configuration of the firmware upgrade parameters:

- **Delay Restart.** Number of seconds that a device must wait before performing a restart after receiving the new firmware
- **Safety Timer (in seconds).** If an upgraded node cannot register before this timer expires, it will return to the last firmware version
- **File.** File with the new firmware version
- **Match Rules.** When marked, the Base Node checks that vendor and model firmware of the Service Node match those of the new firmware. If they do not match, the Base Node will not upgrade this node
- **Signature Type (PRIME 1.4 only):** No signature, RSA3072+SHA256 or ECDSA256+SHA256
- **Signature Size (PRIME 1.4 only):** Size of the signature data that is appended to firmware binary file
- **Page size.** Size of the data packets sent through the PLC line. By default the AUTO option is 64 bytes
- **ARQ.** Enable or disable the ARQ protocol in the Base Node
- **Multicast.** Enable or disable PRIME multicast capabilities to transfer the firmware to a list of devices

Figure 4-1. Base Management View



If you already selected the devices to be upgraded in the Network Topology View (see section 3.3 Firmware Upgrade Management Dialog), click the Start button to start the firmware upgrade process. If not, go to select the devices.

To cancel a firmware upgrade process, use the Stop button or abort it from the Network Topology View (see section 3.3 Firmware Upgrade Management Dialog).

The upper text browser in Figure 4-1 shows real-time changes in topology (Network Events) and the stages of the firmware upgrade process.

4.1 Signing Firmware

In order to test signed firmware upgrades, this tool provides a Python® script that will sign a binary using Microchip´s test keys. The script and test keys are located at *{Install-dir}\signature-scripts*. ECDSA algorithm has been chosen to perform this test. Elliptic curve private and public keys are provided to sign and verify. Remote nodes performing the firmware upgrade must also know the public key to verify the signature. Also, remote nodes must know the ECC curve chosen. Microchip ECC test keys use the standard curve SECP256k1. The provided Python script will create a file concatenating the original file and its signature (coded in ASN.1 format). The signed file will have the same name with the extension “ECDSAxx.bin”, where “xx” is the signature length. In a command line window, execute the command (or edit and execute the batch file provided):

```
C:\>cd "C:\Program Files (x86)\Atmel\Atmel PRIME Manager_2.0.8\signature-scripts"
C:\ …s>c:\python34\python.exe prime-fw-sign.py -f C:\temp\prime_service_bin.bin \
-k ecc_secp_256k1_atmel_private.pem \
-p ecc_secp_256k1_atmel_public.pem
```

It is also possible to sign the firmware binary with your own keys (as long as Service Nodes know your public key) or use a different software. For example, follow the next steps to sign with OpenSSL:

1. Generate (if needed) ECC private key with OpenSSL using SECP256k1 curve (256 bits key):

   ```
   openssl ecparam -out private_key.pem -name secp256k1 -text -genkey
   ```

2. Generate ECC public key from private key (if needed). Service Nodes performing the signature verification must know this key and the curve used to generate it:

   ```
   openssl ec -in private_key.pem -pubout  -text
   ```

3. Show ECC key parameters (curve, public/private):

   ```
   openssl ec -in private_key.pem  -text
   ```

4. Calculate SHA256 digest for your firmware file:

   ```
   openssl dgst -sha256 -binary -out hash_sha256.md file.bin
   ```

5. Sign SHA256 digest with ECDSA:

   ```
   openssl pkeyutl -sign -inkey private_key.pem  -in hash_sha256.md \
   -out signature_asn1.bin
   ```

6. Print binary data, concatenate input file and signature:
   (LINUX)

   ```
   $ cat signature_asn1.bin | xxd
   $ cat file.bin signature_asn1.bin > prime_fw_sig.ECDSA.bin
   ```

   (WINDOWS)

   ```
   c:\> type file.bin signature_asn1.bin > prime_fw_sig.ECDSA.bin
   ```

7. Find out the size of signature, parameter needed by the PRIME Manager
   (LINUX)

   ```
   $ls -l signature_asn1.bin
   ```

   (WINDOWS)

   ```
   C:\> dir signature_asn1.bin
   ```

5. PRIME Management View

This view has several tabs with different functionalities. As shown in Figure 5-1, there are several tabs:

- **PLME/MLME PIBs.** Get or set PIBs through PLME or MLME
- **Serial Profile.** Get or set PIBs through the Serial Profile
- **MAC.** Send and receive messages through null convergence sublayer
- **4-32.** Send and receive messages through IEC-432 convergence sublayer
- **PLME.** PHY Layer Management Entity functions
- **MLME.** MAC Layer Management Entity functions
- **Certification.** PIB management for certification
- **Manufacturing (MTP) Test.** PIB management for manufacturing test
- **PRIME over UDP.** PRIME “Ticket 65” interface through PRIME Manager

Note that each tab has its own text browser to show its corresponding protocol information. Messages can appear on a text browser even if its tab is not selected, e.g. when a 4-32 message is received but another tab is selected.

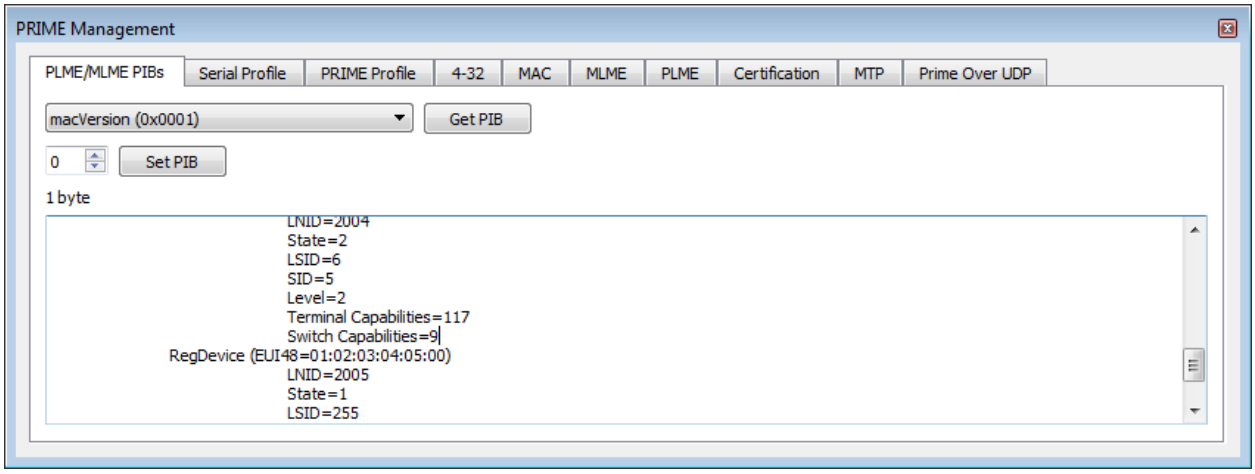
The following subsections describe each tab in detail.

5.1 PLME/MLME PIBs

This tab allows getting or setting a PIB from the connected device through PLME (for PIBs belonging to the PHY layer) or MLME (for PIBs belonging to the MAC layer). Figure 5-1 shows the tab appearance.

Note: The device´s firmware must support this feature. Base/Service Node´s firmware must be configured to support MLME/PLME serialization. Otherwise, commands executed from this window will not have any effect.

Figure 5-1. PLME/MLME PIBs Tab



The PIB is selected from the combo box.

Clicking the Get PIB button, a message similar to the one in Figure 5-1 appears in the text browser showing the result. The PIB value is displayed both in hexadecimal and decimal base (only for PIB attributes up to 32 bits).

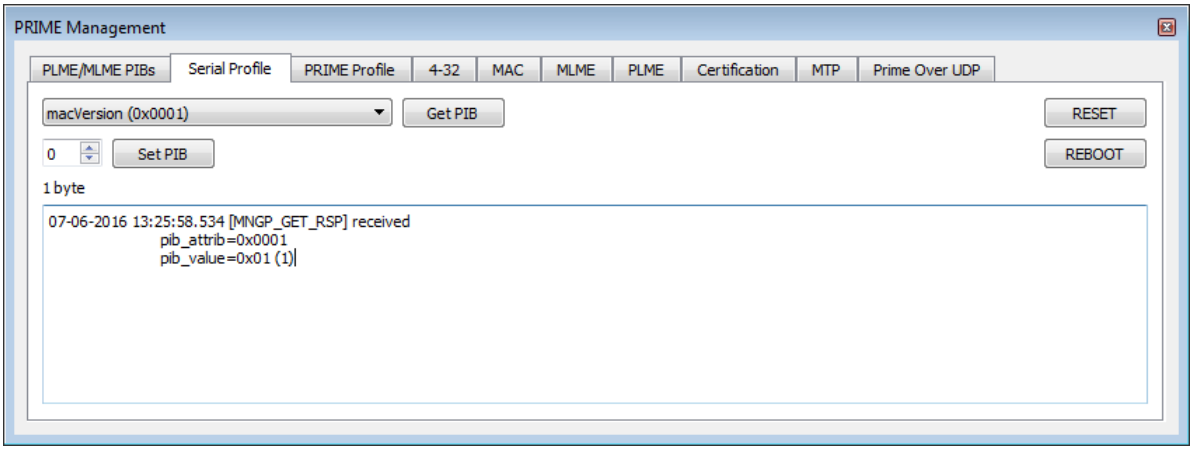
In order to set a PIB, write the value and then click the Set PIB button. The comment below the line edit shows the length of the PIB selected. The new value must be coherent with such length, but if such new value is out of the range, the tool will inform in the text browser. If the length is 1, 2 or 4 bytes, the value must be given in decimal base, otherwise hexadecimal (with 0x…) base must be used.

5.2 Serial Profile

This tab allows getting or setting a PIB from the connected device through the Serial Profile. The Figure 5-2 shows the tab appearance. The list of PIBs is the same as in PLME/MLME PIBs.

For PIB management, this tab is used like the previous one. Apart from that, it is also possible to send *reset statistics* and *reboot* commands to the connected device.

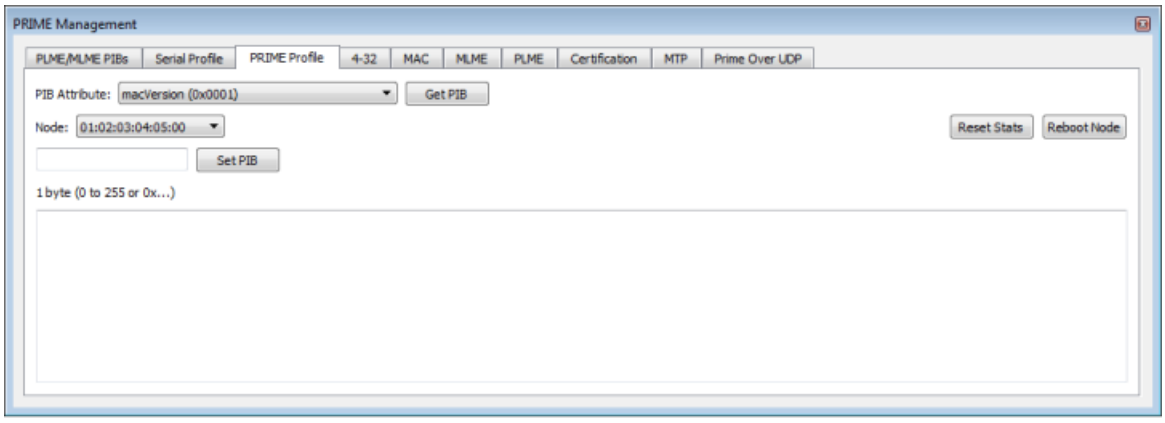
Figure 5-2. Serial Profile Tab



5.3 PRIME Profile

This tab allows getting or setting PIBs to remote nodes through PLC´s PRIME Profile. Also, it allows sending a remote Reset (of statistics) and reboot signal to a registered node.

Figure 5-3. PRIME Profile Tab



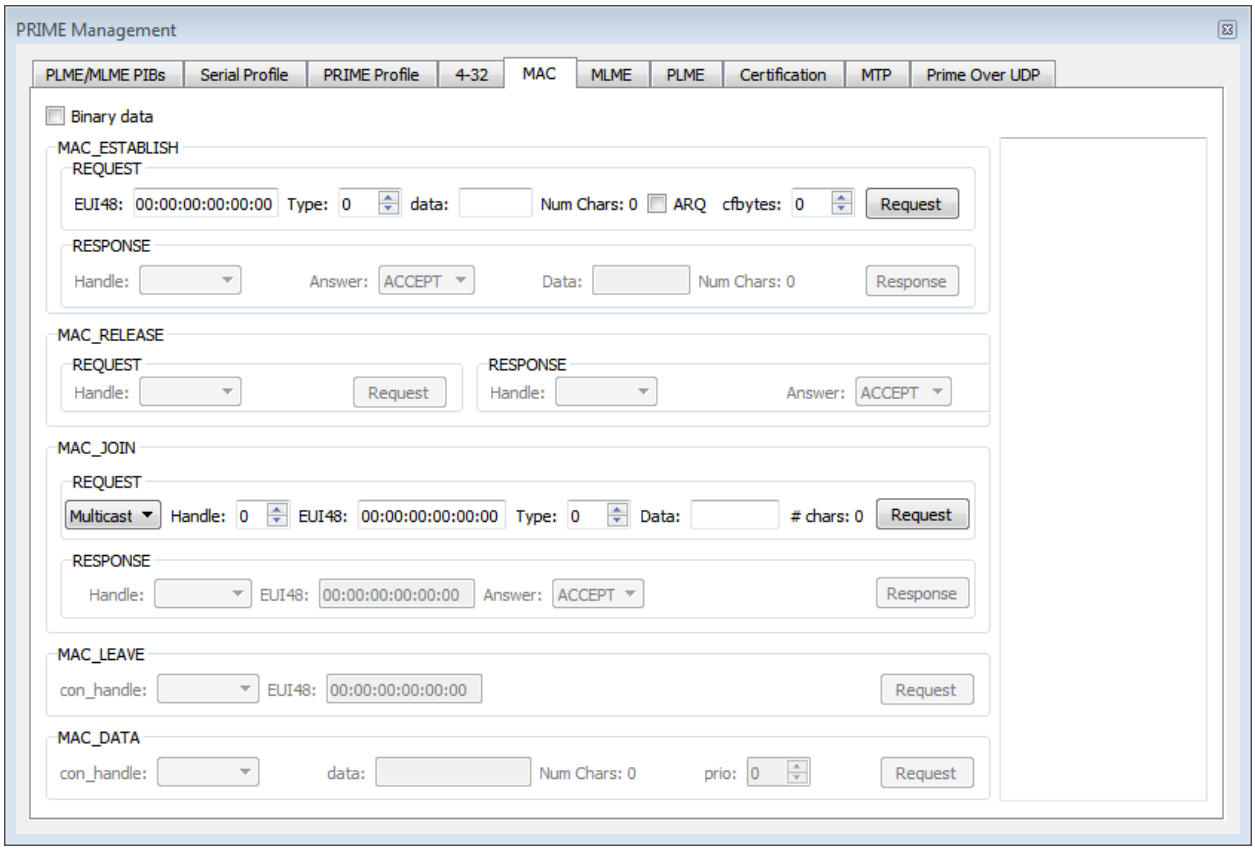
5.4 MAC

This tab allows sending messages through null convergence sublayer. It is the interface with MAC primitives (see PRIME specification). Such primitives are:

- **Establish.** Send establish request or respond to an establish indication
- **Release.** Send release request or respond to a release indication
- **Join.** Send join request or respond to a join indication
- **Leave.** Send leave request
- **Data.** Send data request

Functionalities are dynamically enabled/disabled with received/sent commands, e.g. when a connection is opened, it will be possible to close the connection (release/leave) or send a message through the corresponding connection handler.

Figure 5-4. MAC Tab



5.5 4-32

This tab allows sending messages through the IEC-432 convergence sublayer. The Service Node can connect, disconnect and send messages to the Base Node. Figure 5-5 shows the appearance of this tab.

When the option Binary format (DATA) is marked, the messages must be introduced in hexadecimal format, otherwise ASCII format is used. The received messages are also shown in such format.

Furthermore, if the option Ping – Pong is marked, a message is automatically sent whenever a message is received. Thus, if an instance of the PRIME Manager (version 1.x.x or later) is connected to a Base

Node, another one is connected to a Service Node and Ping - Pong is marked in both, the Base and the Service Node will be continually sending messages to each other.

Base Node tab also permits enabling the DLMS over TCP protocol. This allows a remote concentrator to connect the PRIME Manager/Base Node and gather DMLS/COSEM data directly from the service nodes that implement such layer. When enabled, PRIME Manager opens a TCP server in port 4059 and waits for a connection from a remote concentrator. Only one remote connection is allowed.

Figure 5-5. 4-32 Tab for a Base Node

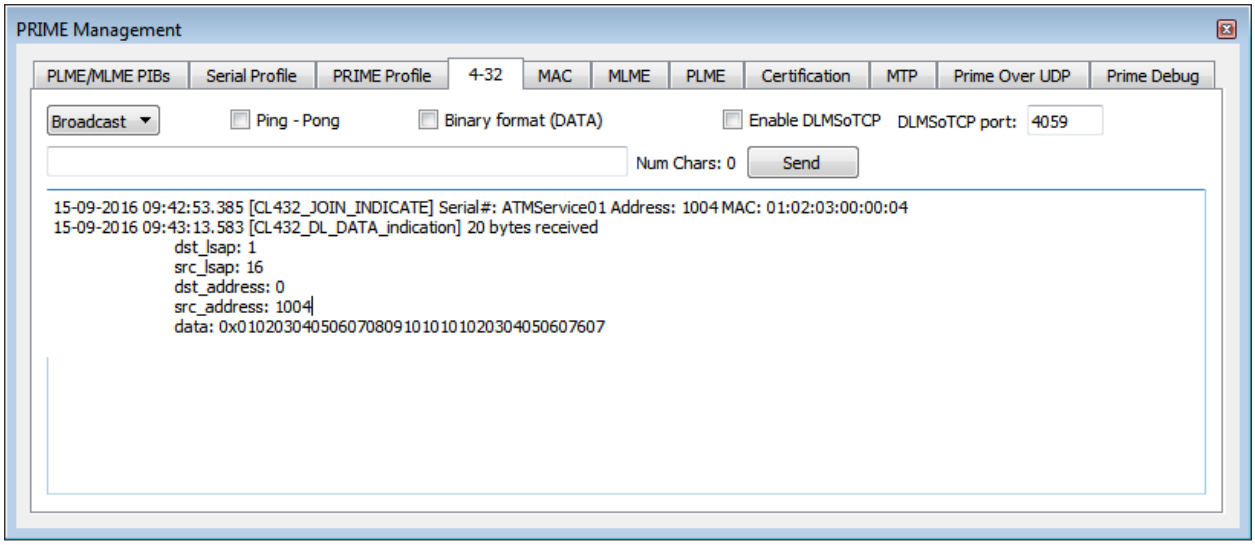
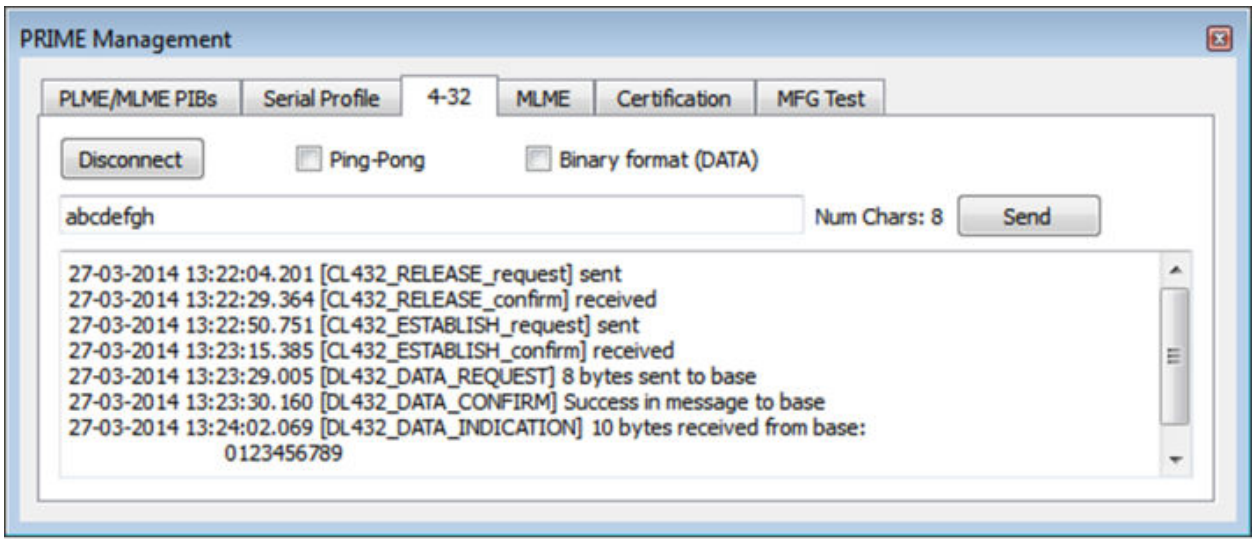


Figure 5-6. 4-32 Tab for a Service Node



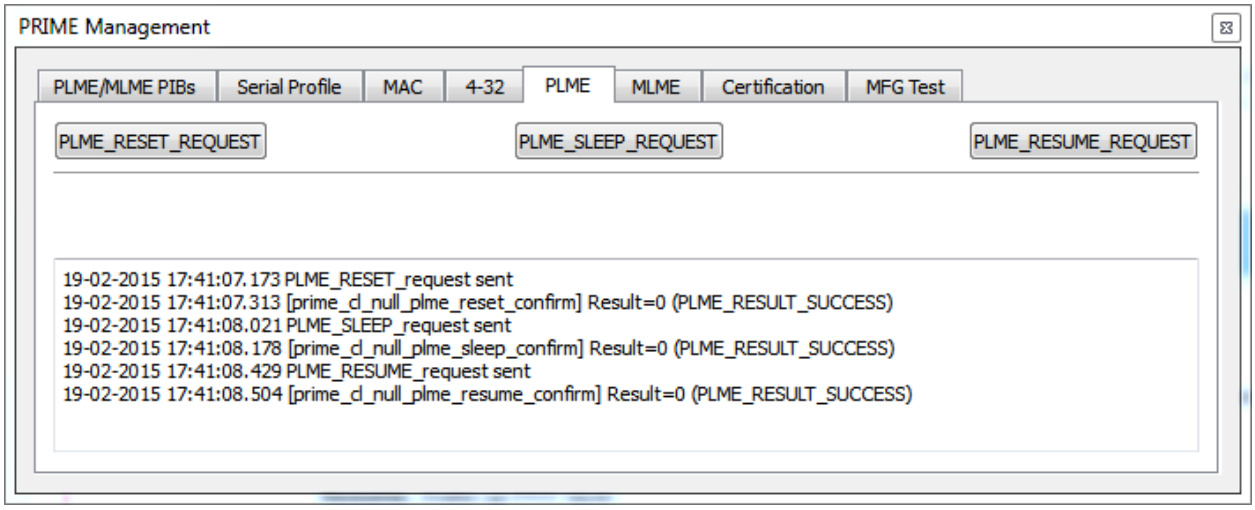
5.6 PLME

This tab is the interface with PHY Layer Management Entity primitives (see PRIME specification). Such primitives are:

- **Reset.** Reset PHY layer
- **Sleep.** Sleep PHY layer. The node will not be able to transmit/receive packets

- **Resume.** Wake up PHY layer

Figure 5-7. PLME Tab



5.7 MLME

This tab allows sending MLME commands. The commands are different depending on the connected device.

Available commands for the Base Node are:

- **Promote.** Promote a terminal node to switch. The Base Node sends the command to the selected Service Node
- **Demote.** Demote a switch node to terminal. The Base Node sends the command to the selected Service Node
- **Unregister.** Unregister a registered node. The Base Node sends the command to the selected Service Node

Info: Note that these commands in the Base Node are also available in the Network Topology View (see section 3.2 Network Management Dialog).

Available commands for the Service Node are:

- **Promote.** Promote the connected node to switch
- **Demote.** Demote the connected node to Terminal state
- **Unregister.** Unregister the connected node

Additionally, there is a common command – Reset MLME – to reset the MAC of the connected device.

Figure 5-8 and Figure 5-9 show the appearance of this tab for a Base Node and a Service Node, respectively.

Figure 5-8. MLME Tab for a Base Node

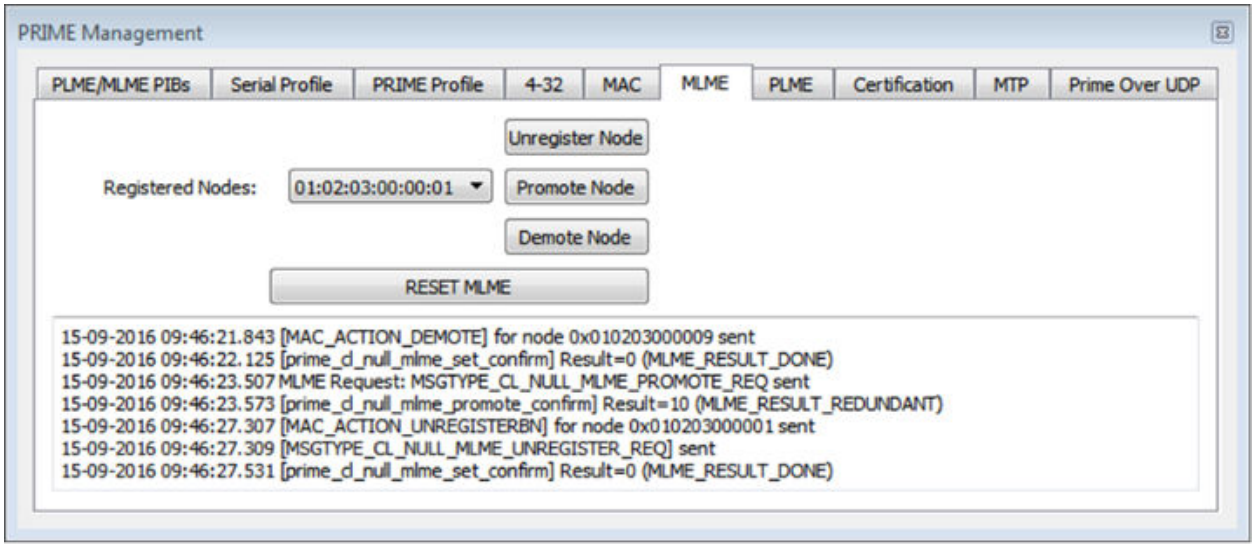
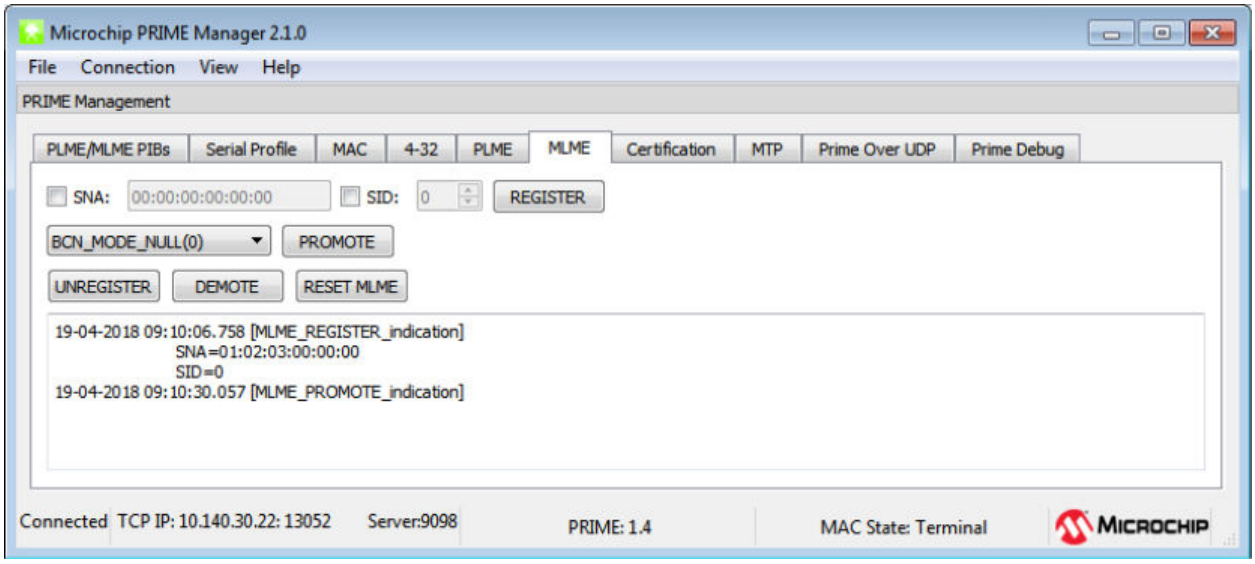


Figure 5-9. MLME Tab for a Service Node



5.8 Certification

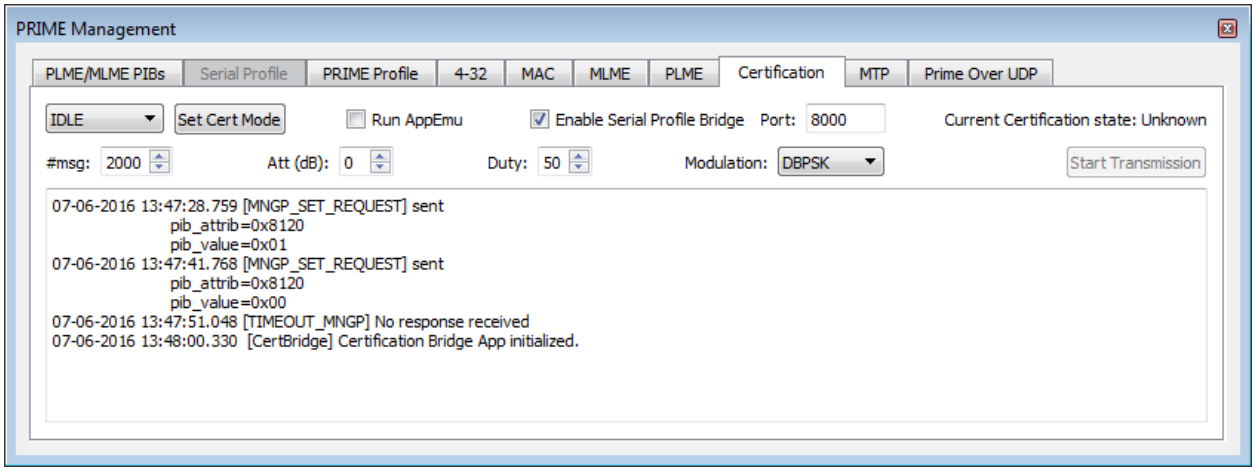
This tab is used to help during the certification process. The PIB handling could be done in the PIB management tabs but in this tab only certification-related PIBs are handled. The following options are available:

- **Set Cert Mode.** PIB *mngCertMode* (0x8120) is set to the mode selected in the combo box (IDLE, PHY v1.3.6, MAC or PHY v1.4)
- **Start Transmission.** Transmit the required number of PHY Test Case type PPDU messages with the selected modulation scheme, signal attenuation and duty cycle (PIB *phyCertTx,* 0x8121). It is required to set PHY mode before
- **Run AppEmu.** Starts/Stops the AppEmu application as defined in the PRIME Certification Test Cases documents

- **Enable Serial Profile Bridge/Port.** This check box enables a TCP server (in the selected port) to which the Certification Tool will connect using Management Plane Interface commands

Note: Serial Profile Bridge/Port option is designed to allow external certification tools to communicate with Base/Service Nodes under test. While this option is enabled, do not use PRIME Manager to perform any task as it may interfere with any external tests.

Figure 5-10. Certification Tab



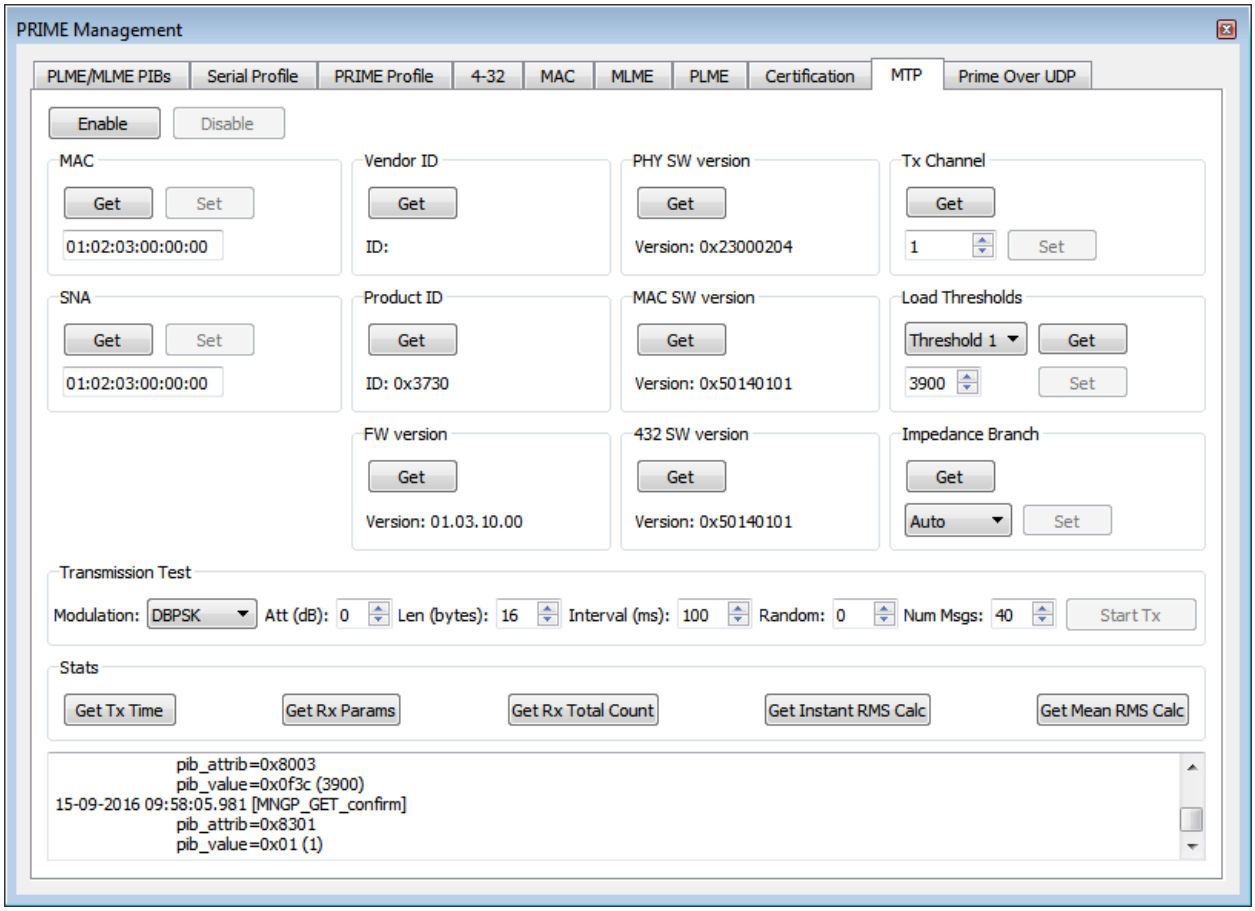
5.9 Manufacturing (MTP) Test

This tab can be used for manufacturing tests. The following options are available:

- **Enable/Disable.** Enable/disable the MTP mode (*phyMtpEnabled,* 0x808E)
- **Get/Set MAC.** Get and set the MAC address of the connected device
- **Get/Set SNA.** Get and set SNA
- **Get version and ID information.** Get SW versions, product ID and vendor ID
- **Get/Set PHY parameters.** Get and set Tx Channel, Load Thresholds and Impedance Branch
- **Transmission Test.** Set PIB *phyTxParams* (0x8089) according to the selected parameters. Len (bytes) is the length of the payload. If random is 0, the content of packets is fixed, otherwise the content is random (the lower the value, the more random is the message)
- **Get Stats.** Get PHY stats. Mean RMS calc retrieves 0 if transmission test is running

Note: Set operations are only allowed when MTP mode is enabled.

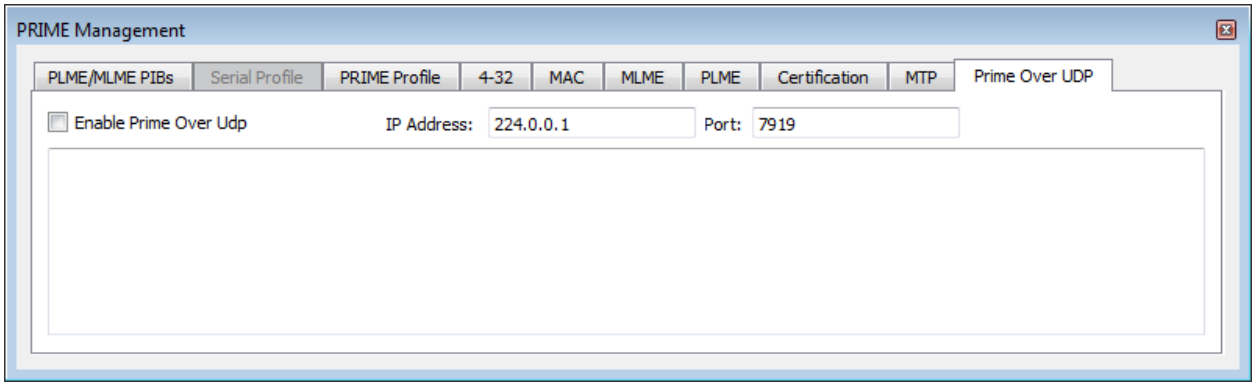
Figure 5-11. MTP Tab



5.10 PRIME over UDP (PRIME 1.3 only)

This tab window allows to start/stop the PRIME over UDP gateway through the PRIME Manager. It is enabled for both Base and Service node as both could perform as a slave UDP device. The Default IP Address corresponds to a multicast IP address, allowing multiple slave devices to communicate with a master concentrator node.

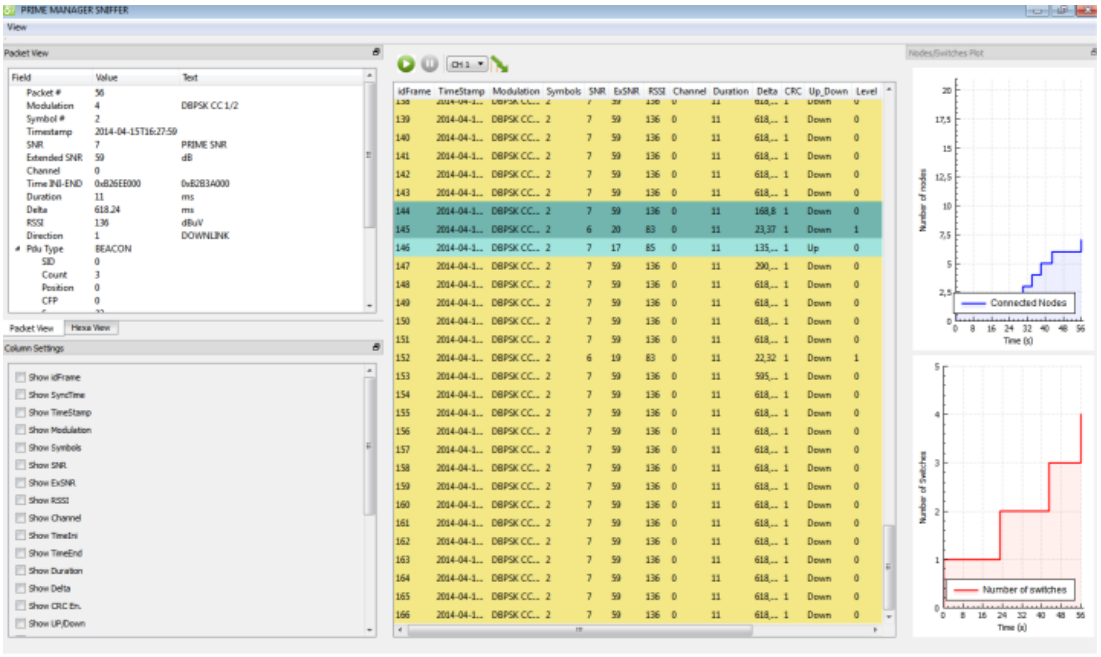
Figure 5-12. PRIME over UDP Tab



6. Sniffer Window

This window uses the same sniffer widgets (used in PLC Sniffer). That way, it is possible to use all the functionalities of PRIME Manager and at the same time, monitorize the PLC packets with the sniffer, all using the same COM port.

Figure 6-1. Sniffer Window



At the beginning, the sniffer table view is shown. Such view shows the PLC packets in real time.

Furthermore, more widgets can be selected to be shown in the view menu:

- **Packet View:** The selected packet in the table is decoded
- **Hexa View:** The selected packet in the table is shown in hexadecimal, byte by byte
- **Column Settings:** Additional columns can be selected to be shown
- **Nodes/Switches plot:** Shows the number of nodes and switches as a function of the time

For more information, see the PLC Sniffer documentation.

Note: The device´s firmware must have the embedded sniffer option enabled. Otherwise, no frames will be shown.

7. Revision History

Note: Revisions 7.1-7.3 (Rev A-C) refer to Atmel document number 43089. With the 06/2018 revision, the document was converted to the Microchip format and assigned DS number 50002766, beginning with Rev A.

7.1 Rev A - 02/2015

Document	Initial release.

7.2 Rev B - 01/2016

Document	Updated for software release v2.0.7.

7.3 Rev C - 09/2016

Document	Updated for software release v2.0.8. (Firmware versions: 1.3.9.x SN, 1.3.10.x BN, 1.4.2.1 SN and BS).

7.4 Microchip Rev A - 06/2018

Document	• Updated to new Microchip document number DS50002766. • Updated for software release v2.1.0.

The Microchip Web Site

Microchip provides online support via our web site at http://www.microchip.com/. This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQ), technical support requests, online discussion groups, Microchip consultant program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

Customer Change Notification Service

Microchip's customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip web site at http://www.microchip.com/. Under "Support", click on "Customer Change Notification" and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or Field Application Engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at: http://www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip devices:

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.

- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as “unbreakable.”

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip’s code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

Legal Notice

Trademarks

ISBN: 978-1-5224-3194-7

Quality Management System Certified by DNV

ISO/TS 16949

Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC® MCUs and dsPIC® DSCs, KEELOQ® code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: http://www.microchip.com/support Web Address: www.microchip.com **Atlanta** Duluth, GA Tel: 678-957-9614 Fax: 678-957-1455 **Austin, TX** Tel: 512-257-3370 **Boston** Westborough, MA Tel: 774-760-0087 Fax: 774-760-0088 **Chicago** Itasca, IL Tel: 630-285-0071 Fax: 630-285-0075 **Dallas** Addison, TX Tel: 972-818-7423 Fax: 972-818-2924 **Detroit** Novi, MI Tel: 248-848-4000 **Houston, TX** Tel: 281-894-5983 **Indianapolis** Noblesville, IN Tel: 317-773-8323 Fax: 317-773-5453 Tel: 317-536-2380 **Los Angeles** Mission Viejo, CA Tel: 949-462-9523 Fax: 949-462-9608 Tel: 951-273-7800 **Raleigh, NC** Tel: 919-844-7510 **New York, NY** Tel: 631-435-6000 **San Jose, CA** Tel: 408-735-9110 Tel: 408-436-4270 **Canada - Toronto** Tel: 905-695-1980 Fax: 905-695-2078	**Australia - Sydney** Tel: 61-2-9868-6733 **China - Beijing** Tel: 86-10-8569-7000 **China - Chengdu** Tel: 86-28-8665-5511 **China - Chongqing** Tel: 86-23-8980-9588 **China - Dongguan** Tel: 86-769-8702-9880 **China - Guangzhou** Tel: 86-20-8755-8029 **China - Hangzhou** Tel: 86-571-8792-8115 **China - Hong Kong SAR** Tel: 852-2943-5100 **China - Nanjing** Tel: 86-25-8473-2460 **China - Qingdao** Tel: 86-532-8502-7355 **China - Shanghai** Tel: 86-21-3326-8000 **China - Shenyang** Tel: 86-24-2334-2829 **China - Shenzhen** Tel: 86-755-8864-2200 **China - Suzhou** Tel: 86-186-6233-1526 **China - Wuhan** Tel: 86-27-5980-5300 **China - Xian** Tel: 86-29-8833-7252 **China - Xiamen** Tel: 86-592-2388138 **China - Zhuhai** Tel: 86-756-3210040	**India - Bangalore** Tel: 91-80-3090-4444 **India - New Delhi** Tel: 91-11-4160-8631 **India - Pune** Tel: 91-20-4121-0141 **Japan - Osaka** Tel: 81-6-6152-7160 **Japan - Tokyo** Tel: 81-3-6880- 3770 **Korea - Daegu** Tel: 82-53-744-4301 **Korea - Seoul** Tel: 82-2-554-7200 **Malaysia - Kuala Lumpur** Tel: 60-3-7651-7906 **Malaysia - Penang** Tel: 60-4-227-8870 **Philippines - Manila** Tel: 63-2-634-9065 **Singapore** Tel: 65-6334-8870 **Taiwan - Hsin Chu** Tel: 886-3-577-8366 **Taiwan - Kaohsiung** Tel: 886-7-213-7830 **Taiwan - Taipei** Tel: 886-2-2508-8600 **Thailand - Bangkok** Tel: 66-2-694-1351 **Vietnam - Ho Chi Minh** Tel: 84-28-5448-2100	**Austria - Wels** Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 **Denmark - Copenhagen** Tel: 45-4450-2828 Fax: 45-4485-2829 **Finland - Espoo** Tel: 358-9-4520-820 **France - Paris** Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 **Germany - Garching** Tel: 49-8931-9700 **Germany - Haan** Tel: 49-2129-3766400 **Germany - Heilbronn** Tel: 49-7131-67-3636 **Germany - Karlsruhe** Tel: 49-721-625370 **Germany - Munich** Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 **Germany - Rosenheim** Tel: 49-8031-354-560 **Israel - Ra'anana** Tel: 972-9-744-7705 **Italy - Milan** Tel: 39-0331-742611 Fax: 39-0331-466781 **Italy - Padova** Tel: 39-049-7625286 **Netherlands - Drunen** Tel: 31-416-690399 Fax: 31-416-690340 **Norway - Trondheim** Tel: 47-7289-7561 **Poland - Warsaw** Tel: 48-22-3325737 **Romania - Bucharest** Tel: 40-21-407-87-50 **Spain - Madrid** Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 **Sweden - Gothenberg** Tel: 46-31-704-60-40 **Sweden - Stockholm** Tel: 46-8-5090-4654 **UK - Wokingham** Tel: 44-118-921-5800 Fax: 44-118-921-5820