SNMP V2c Getting Started Guide

Table of Contents

Introduction to SNMP V2c Demo Application

This document addresses the following FAQs and also provides more information on the SNMP V2c:

1. Why are there two separate mib scripts (mchip.mib and snmp.mib) with Microchip TCP/IP Stack SNMP support?
2. What are the Tools needed to compile and upload the MIB scripts to the agent and the manager?
3. How will the SNMP V2c agent in TCP/IP stack v5.0 onward support the existing SNMPV1 applications implemented with previous stack releases?
4. How is the SNMP MIB browser used, and how are MIB scripts uploaded and interpreted?

The SNMP stack in the Microchip TCP/IP Stack suite is separated into two parts:

- SNMP stack implementation (`SNMP.c`)
- Application and demo specific implementation (`CustomSNMPApp.c`)

The Microchip SNMP V2c agent (V2c) follows RFC 3416 and is implemented to address the requirements of embedded applications. The V2c supports and responds to SNMP V1 (V1) queries also.

The V2c is implemented with multiple community names configuration support, which are stored in the selected non volatile memory (SPI EEPROM or SPI Flash). The community names can be configured through the TCPIP Configuration Wizard and also by using the HTTP interface. A separate, access restricted web page is provided in the Microchip TCP/IP Stack v5.0 onward in the HTTP2 server for dynamic configuration of SNMP communities.

Note: For existing Microchip SNMP V1 users.

X. SNMP V1 users wanting to upgrade the Microchip TCP/IP Stack from older versions to the latest version, and continue to use SNMP V1 can get the SNMP V1 services from the V2c agent, provided they do not modify the default settings of the SNMP module in v5.0 onward.

X. The implementation framework for V1 and V2c remains the same, except for few new features, and functions. The names and parameters of some of the functions have been changed. V1 users may have to make changes to their application-specific code. There should not be any change in the V2c stack code unless users have incorporated application code in the SNMP stack.

X. Users should build a new MPFS image using the MPFS File System Generator utility and upload to the selected EEPROM or Flash memory, as the *APPConfig* structure is updated to accommodate community names of V2c.

Microchip SNMP V2c MIB Scripts and Corresponding Tools

The V2c comprises two MIB files:

- *snmp.mib* (Microchip Custom MIB script)
- *mchip.mib* (ASN.1 MIB script)

The Microchip TCP/IP Stack includes the "**mib2bib.exe**" utility, which compiles the Microchip MIB script and generates the "*snmp.bib*" and "*mib.h*" files.

- Copy the "*snmp.bib*" file to "C:\Microchip Solutions\TCPIP Demo App\WebPages2\" directory.
- Copy the "*mib.h*" file to "C:\Microchip Solutions\TCPIP Demo App\".
- Now, use the "**MPFS2.exe**" tool.

See the "*Getting Started \Uploading Web Pages*" section for more information on this tool. With this utility, the generated *snmp.bib* file is bundled into the "*MPFS2Img.bin*" file, and is stored into the non-volatile memory. The SNMP agent searches for the required MIB variable information in this MPFS image using MPFS file system support.

- Compile the "TCPIP Demo App-Cxx" project with the "*mib.h*" file copied in "TCPIP Demo APP".

  The SNMP agent requires the #defines in "*mib.h*".

> **Note:** Do not make any changes in the "`mib.h`" file; the "**mib2bib.exe**" utility will automatically generate this file.

The "*mchip.mib*" file is the ASN.1 MIB script meant for the SNMP manager. The SNMP manager (browser) understands the ASN.1 format. Once the manager is installed, "*mchip.mib*" file should to be copied to its MIB directory.
The subsequent sections provide more information on how to use the SNMP manager and how to upload the MIB script.

SNMP Browsers and MIB Scripts

Note that the use of a MIB browser or other third-party tools may require that users review and agree to the terms of a license. Microchip's reference to the **iReasoning** MIB browser is for the users' convenience. It is the user's responsibility to obtain information about, and comply with the terms of, any applicable licenses.

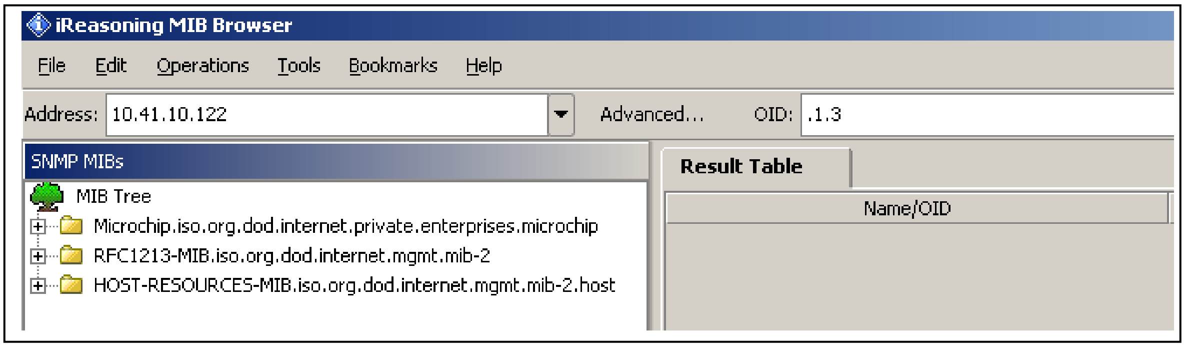
Uploading MIB Script to SNMP Browser

The iReasoning MIB browser can be downloaded from http://www.ireasoning.com/downloadmibbrowserlicense.shtml.

Once the browser installation is done, perform the following steps:

1. Copy the “*mchip.mib*” file to “C:\Program Files\ireasoning\mibbrowser\mibs”.
2. Go to File->Load MIBs menu and select the “*mchip.mib*” file.

The Microchip MIB directory (“SNMP MIB” pane) displays as shown in Figure 1.



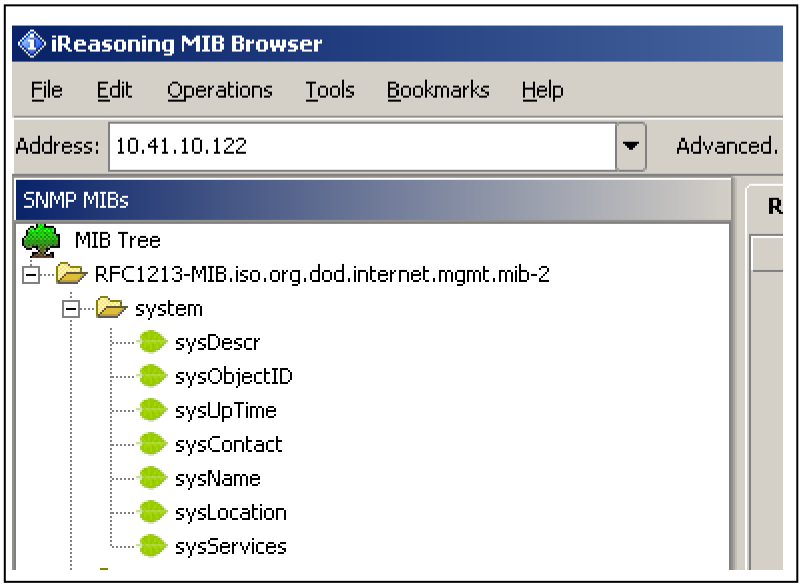
Address: 10.41.10.122

OID: .1.3

iReasoning MIB Browser
File
Edit
Operations
Tools
Bookmarks
Help
Advanced...
SNMP MIBs
Result Table
MIB Tree
Microchip.iso.org.dod.internet.private.enterprises.microchip
RFC1213-MIB.iso.org.dod.internet.mgmt.mib-2
HOST-RESOURCES-MIB.iso.org.dod.internet.mgmt.mib-2.host
Name/OID

Figure 1: Microchip “SNMP MIBs” Directory

Figure 2 shows the RFC1213 - MIB2 variables implemented in the Microchip SNMP Agent. Minimum set of variables are implemented, required to identify the Microchip node as an SNMP node in a network. These variables can be accessed by any SNMP browser with a “public” type community name. Refer to AN870 – “*SNMP V2c Agent for Microchip TCP/IP Stack*” for more details on the MIB script, community names and Demo SNMP MIB variable tree structure.



Address: 10.41.10.122

Figure 2: RFC1213 MIB2 Variables

Figure 3 shows the Microchip private MIB variable tree structure in the browser. The ASN.1 format “*mchip.mib*” file is defined with this tree structure for the MIB variables. The browser can access every variable in the MIB database provided the community name matches.

> **Note:** To modify the MIB variables, the corresponding changes should be made in both the MIB scripts (“*snmp.mib*” and “*mchip.mib*”).

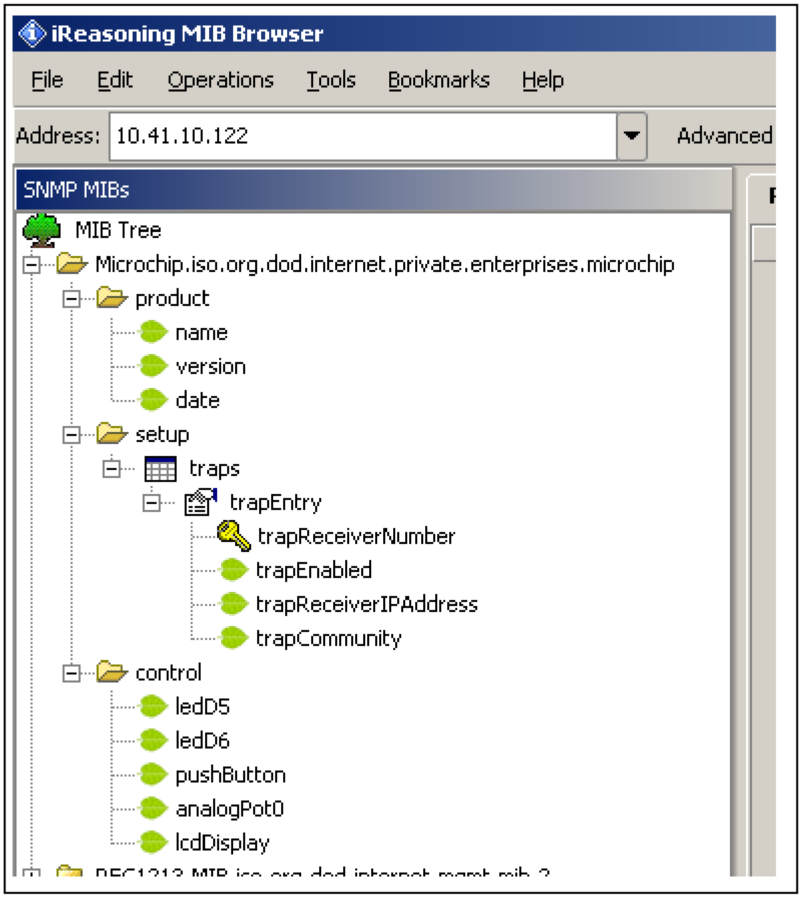
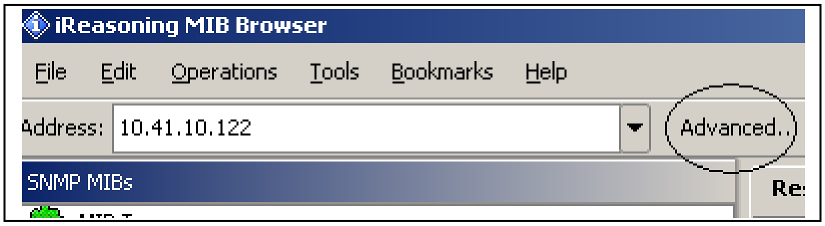

Address: 10.41.10.122

Figure 3: Private MIB Variable Tree Structure

Configuring the Browser for SNMP Version and Community

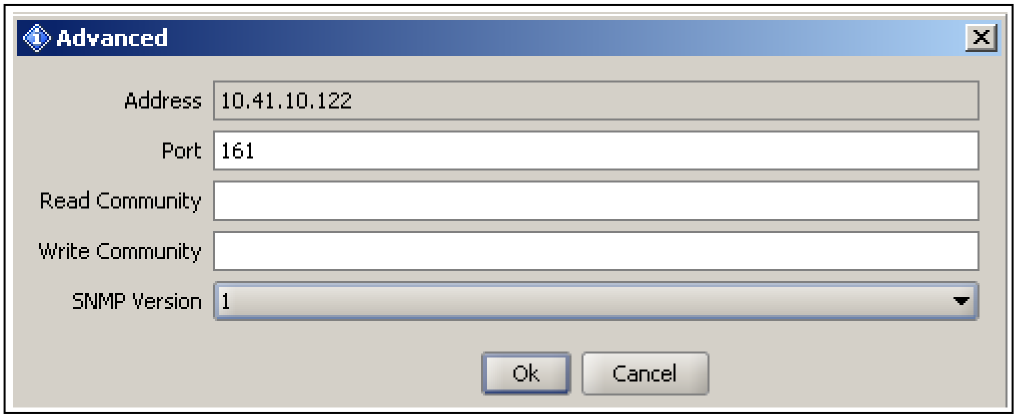
1. Select the "Advanced" tab in the browser as shown in Figure 4.



Address: 10.41.10.122

Figure 4: Advanced Tab Location

The Configuration window as shown in Figure 5 displays.



Address 10.41.10.122
Port 161
Read Community
Write Community
SNMP Version 1

Figure 5: Advanced Configuration Window

2. Configure the Read and Write community to the browser.
   - If the community fields are blank, the manager sends the SNMP request with the community name as "public".
   - The V2c agent is configured by default with 3 Read {"public", "read", " "} and 3 Write communities {"private", "write", "public"}
   - The default maximum community length is 8 characters.
   - As the default communities also contain the "public" community name, the agent will respond to all the browsers requesting for "public" community.
   - The TCPIP Configuration Wizard can be used to configure the default SNMP community names. At run time, the community names can be dynamically configured using the HTTP interface for SNMP community name configuration.

> **Note:** The V2c agent will respond only to the queries from the SNMP browsers of the same community. That is, the V2c agent and the browser should be the member of the same community.

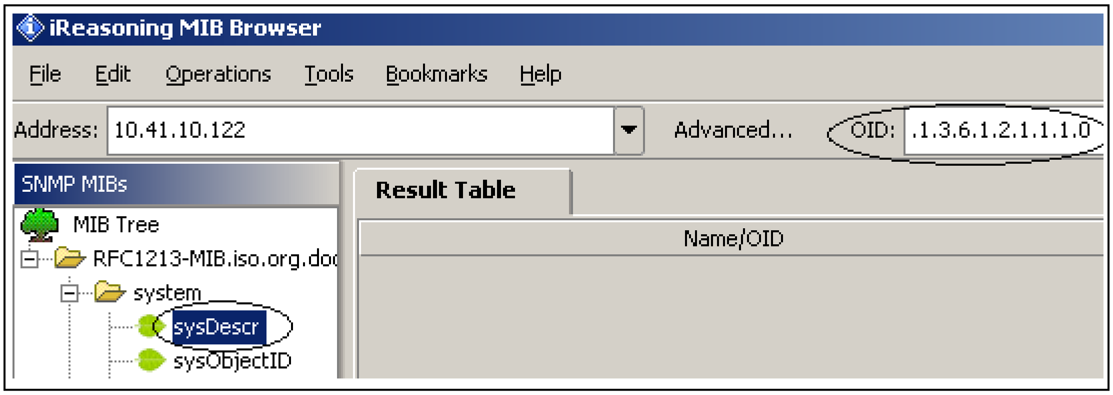
If the V2c agent receives an SNMP request with an unknown community name, the agent will generate an Authentication trap.

The V2c agent's multiple community support feature enables the user application to provide limited access to the requesting browser based on the community name used by the browser to access the MIB database variables of the agent.

MIB Variable and Operation Selection

1. Select the variable to be accessed from the agent MIB database from the "**SNMP MIBs**" pane.

The selected variable's OID can be seen in the OID tab as shown in Figure 6.

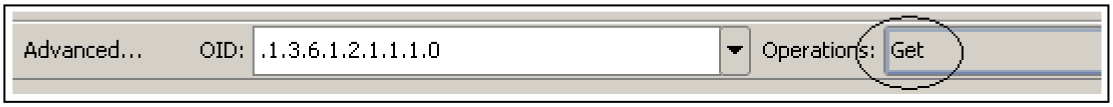


Address: 10.41.10.122

OID: .1.3.6.1.2.1.1.1.0

Figure 6: Agent MIB Database Variable and its OID

2. Select the SNMP Request from the "**Operations**" tab as shown in Figure 7.



OID: .1.3.6.1.2.1.1.1.0

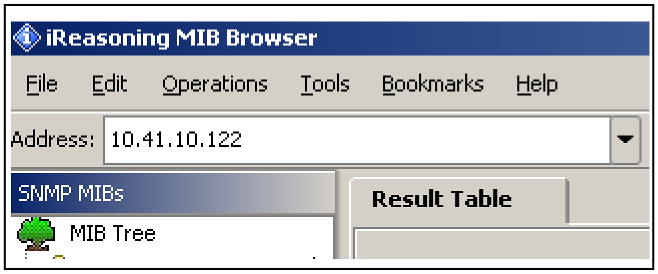
Operations: Get

Figure 7: SNMP Request and Operations Tab

Exploring the Microchip SNMP V2c Agent Demo

After the MIB script is uploaded to the SNMP browser, the MIB tree structure will be displayed in the browser as shown Figure 1 through Figure 3 and Figure 6. Any of these variables can be accessed (SNMP operations can be performed) from the agent if the agent supports these variables. The browser and agent should be members of the same community.
To learn more about the SNMP operations, PDU types, and terminology, refer to AN870 – "*SNMP V2c Agent for Microchip TCP/IP Stack*".

Configure the IP address of the V2c agent to the "Address" field as shown in Figure 8.



Address: 10.41.10.122

Figure 8: SNMP V2c Agent IP Address Configuration

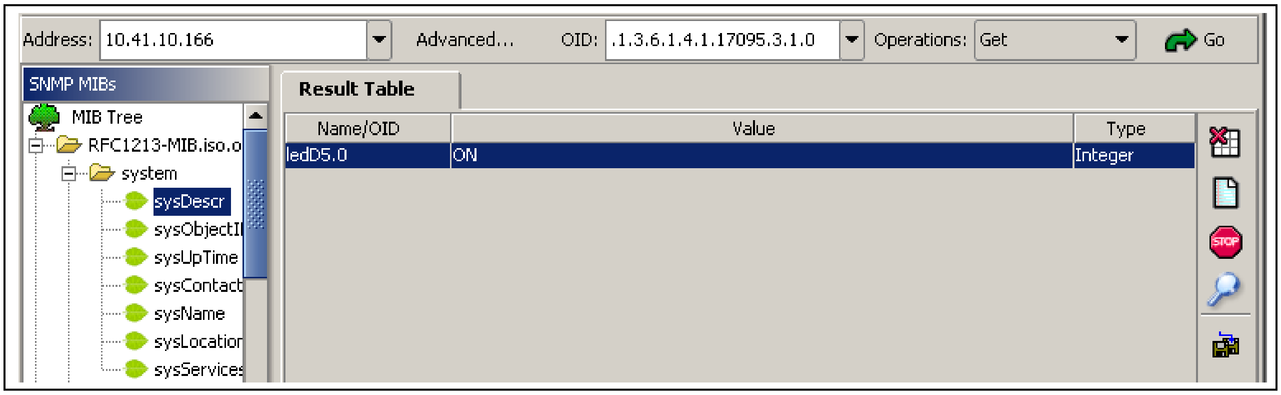
SNMP Operations

Get

1. Select “**Advanced**” tab and configure the SNMP version to ‘1’, and Read Community to “**public**”.
2. Select “**Get**” from Operations.
3. Select the “**sysDescr**” variable from the MIB Tree.

The “**Result Table**” displays “**sysDescr**” variable information.

Repeat this procedure for any MIB variable. For SNMP V2c, repeat the above procedure, replacing ‘2’ in place of ‘1’ in the Advanced>SNMP version configuration as shown in Figure 9.


Address: 10.41.10.166
Advanced...
OID: .1.3.6.1.4.1.17095.3.1.0
Operations: Get

Result Table

Name/OID	Value	Type
ledD5.0	ON	Integer

Figure 9: Get Operation Configuration

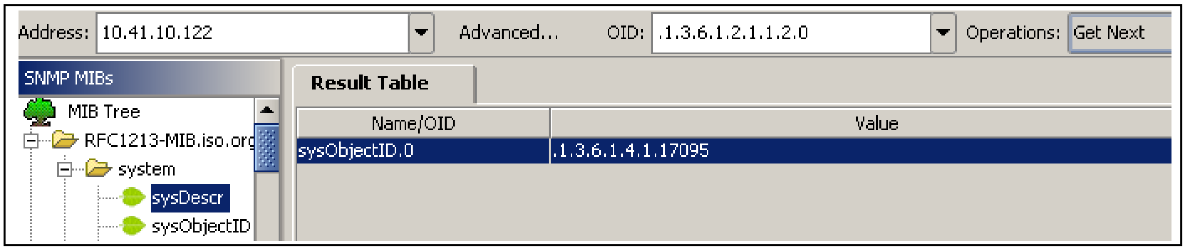
The V2c agent is provided with three Read and Write community defaults as explained earlier. Configure any of these communities to the browser and try accessing the MIB variables. You should be able to access all the MIB variables even with ‘write’ communities configured as Read Community. For GET operations, if the Read or Write community matches, the agent processes the request. For SET operations, the received community name must match to any of the configured ‘write’ community names.

Get_Next

1. Repeat the process for “**Get**”. Select “**sysDescr**” variable from MIB. Select “**Get Next**” from “**Operations**”.

   The “**Result Table**” displays the “**sysObjectID**” variable information as shown in Figure 10.

2. Repeat for different MIB variables and get the information of the corresponding next variable.



Address: 10.41.10.122

OID: .1.3.6.1.2.1.1.2.0

Operations: Get Next

Result Table

Name/OID	Value
sysObjectID.0	.1.3.6.1.4.1.17095

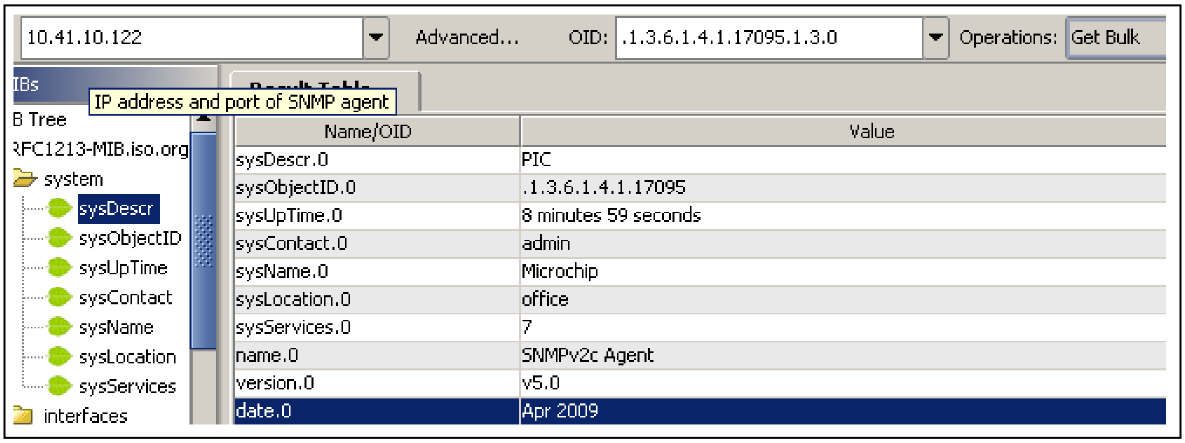
Figure 10: Get_Next Operation Configuration

Get_Bulk

This operation is supported in SNMPV2c. Get_Bulk enables collection of bulk information from the agent with a single request from the manager.

1. Configure SNMP version as V2 in SNMP browser. Select “**Advanced**”, configure SNMP version to “**V2**” and Read Community to “**public**” or “**read**”.
2. Select “**SysDescr**” variable from MIB.
3. Select “**Get Bulk**” from “**Operations**” and press “**Go**”.

The “**Result Table**” displays information for 10 MIB variables in a single request as shown in Figure 11.
These variables are lexicographical successors of the “**SysDescr**”. The number of variables that the agent will respond with can be configured in the browser through ‘Tools>Options>Non-Repeaters’ and ‘Tools>Options>Max-Repetitions’ menus. The Non-Repeaters and Max-Repetitions numbers are extracted by the agent from the received Get_Bulk request, and the number of variables to be in response PDU is calculated.
For more information on calculating the number of variables and Non-Repeaters and Max-Repetitions, refer to RFC 3416.



10.41.10.122

OID: .1.3.6.1.4.1.17095.1.3.0

Operations: Get Bulk

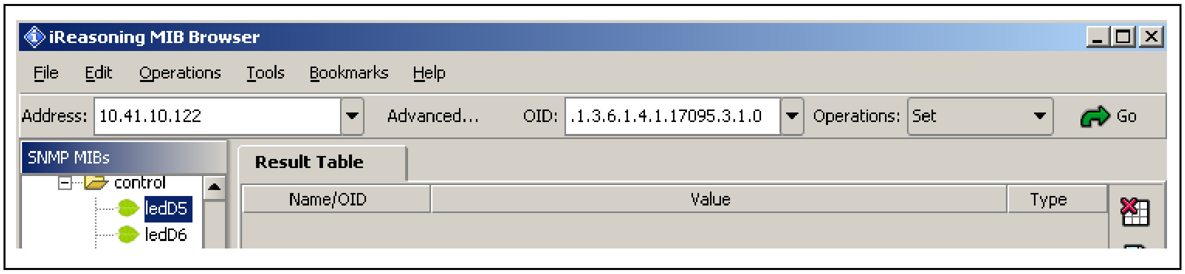
Name/OID	Value
sysDescr.0	PIC
sysObjectID.0	.1.3.6.1.4.1.17095
sysUpTime.0	8 minutes 59 seconds
sysContact.0	admin
sysName.0	Microchip
sysLocation.0	office
sysServices.0	7
name.0	SNMPv2c Agent
version.0	v5.0
date.0	Apr 2009

Figure 11: Get_Bulk Operation Configuration

Set

The Set command updates the variable information of the MIB database of the agent. The Set command can be performed only on those variables which are declared as 'READWRITE' in the MIB scripts, and only if the community name matches any one of the 'write' community names configured with the agent.

1. Select '**ledD5**' variable from MIB.
2. Select '**Advanced**'. Configure SNMP version to '**V1** or **V2**'. Write Community to '**public**' or '**write**' or '**private**'.
3. Select '**Set**' from '**Operations**' as shown in Figure 12.



Address: 10.41.10.122

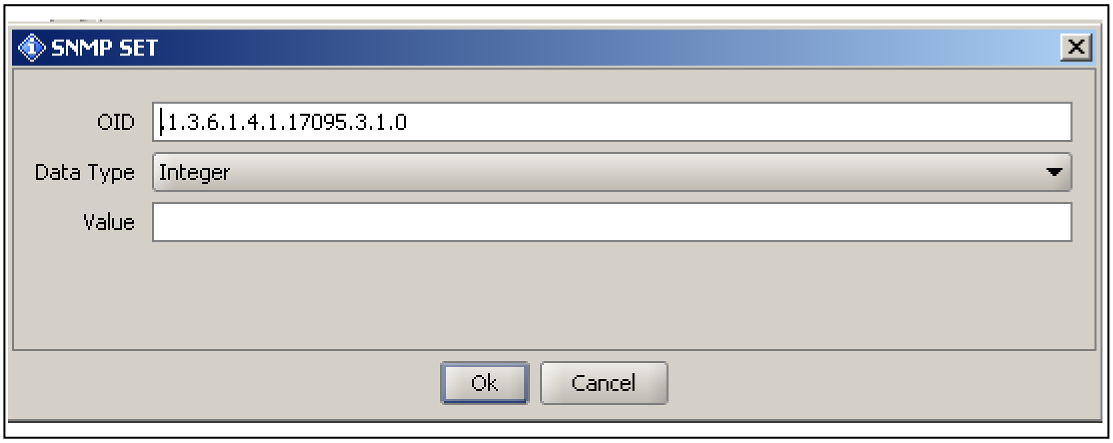
OID: .1.3.6.1.4.1.17095.3.1.0

Operations: Set

Figure 12: Set Operation Configuration

The SNMP SET window pops up (Figure 13).

1. Enter the value for the browser in OID field.



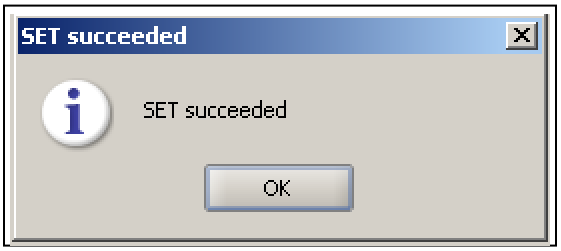
OID: 1.3.6.1.4.1.17095.3.1.0

Data Type: Integer

Value:

Figure 13: SNMP Set Window

A success message appears as shown below.



SET succeeded

A ‘**Get**’ operation for the same variable should now return the new ‘**Set**’ value for this variable.
The LED5 on the PICDEM.net™ 2 or the Explorer16 board should be ON.
A ‘**Get**’ operation on the LED5 displays the LED5 as ‘ON’.
Repeat the procedure to ‘**Set**’ LED5 to OFF.
If required, LED6 can also be set ON and OFF.

Traps

Traps are notifications from the agent to the manager that are used if a predefined event occurs at the agent. For the Trap demonstration, two events are defined with the V2c agent:

- If the Analog Pot value is more than 512, the agent sends Trap every 5 seconds to the configured "**trapReceiverIPAddress**".
- If the '**Push Button 0**' is pushed, an organization specific PUSH_BUTTON trap will be sent.

The current implementation of the V2c agent also generates a standard "Authentication Failure Trap" –

- If the private MIB variable values are requested to modify (Set) a variable, or
- If the value of the variable is requested (Get) by browsers with the wrong community name.

1. Select '**Advanced**' and configure SNMP version to '**V2**' and '**Write**' community to '**public**' or '**write**' or '**private**'.
2. Select 'trapEnabled.0' variable from MIB.
3. Select 'Set' from 'Operations'.
4. Enter '1' in the value field of the "SNMP SET" window.
5. Select '**trapReceiverIPAddress.0**'.
6. Set the IP address if the PC on which the SNMP browser is installed and running.
7. Select '**trapCommunity.0**'.
8. Set the community name of the SNMP browser. (Default community, if not Set is 'public').
9. Configure 'trapCommunity' to the community name at which the browser will receive the trap (Default community, if not Set is 'public').

The 'trapCommunity' name will work as a filter for the SNMP browsers on a monitoring server to receive the trap.

1. Open the 'Trap Receiver' utility of the **iReasoning** MIB browser as shown in Figure 14 (Start>All Programs>iReasoning>MIB Browser>Trap Receiver).

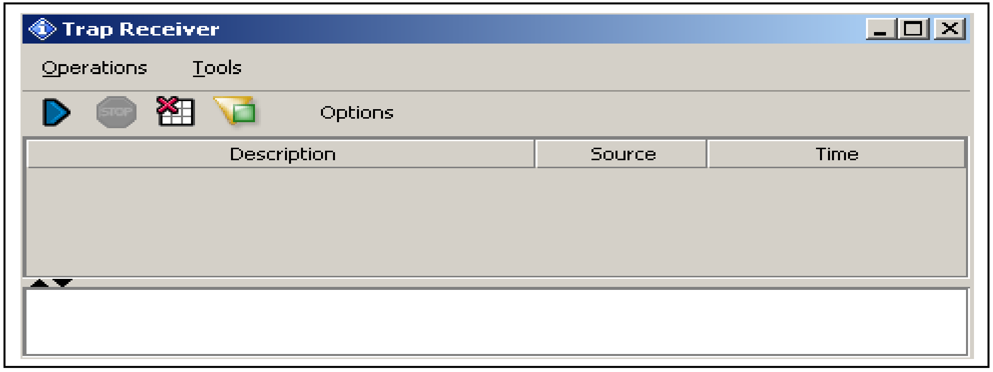
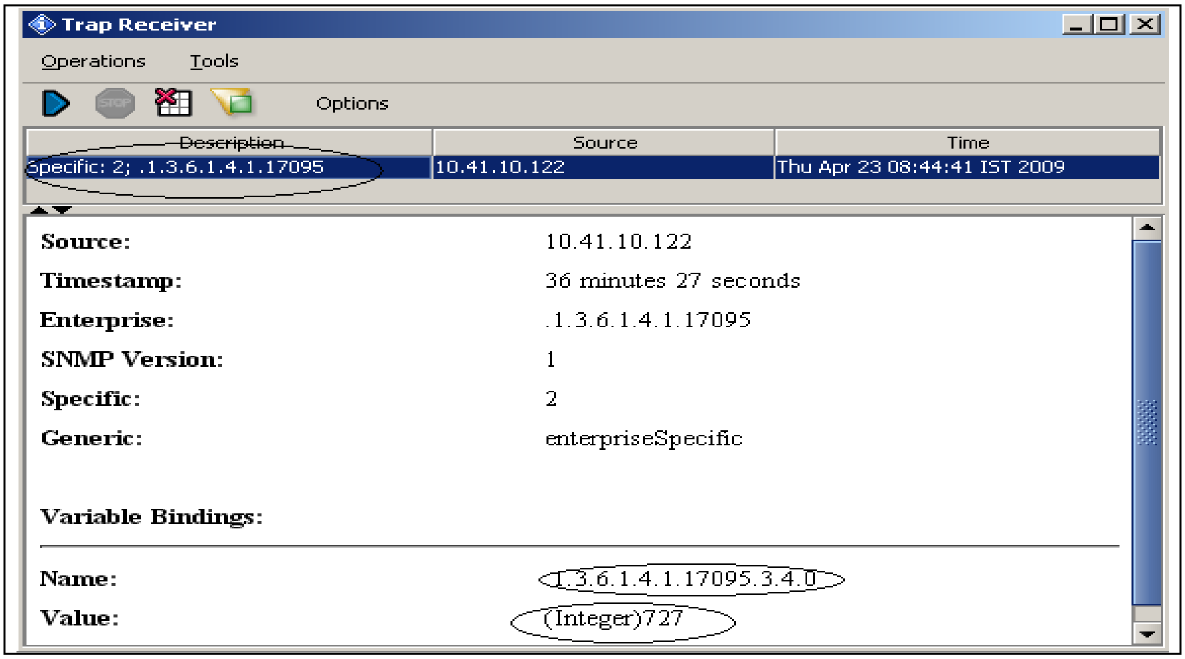


Figure 14: Trap Receiver Utility

Trap demo configurations requisites:

- Analog Pot Trap – Adjust the Analog Pot on the PICDEM.net™ 2 board or Explorer16 board to more than 512. The received trap is shown in Figure 15.

This is an enterprise-specific trap. The SNMP manager will receive the source IP address, the OID (as the name of the variable), the value, the time stamp, etc. for each event. The browser will interpret the data as AnalogPot variable information based on the OID name.



Description	Source	Time
Specific: 2; .1.3.6.1.4.1.17095	10.41.10.122	Thu Apr 23 08:44:41 IST 2009

Source:	10.41.10.122
Timestamp:	36 minutes 27 seconds
Enterprise:	.1.3.6.1.4.1.17095
SNMP Version:	1
Specific:	2
Generic:	enterpriseSpecific

Variable Bindings:

Name:	.1.3.6.1.4.1.17095.3.4.0
Value:	(Integer)727

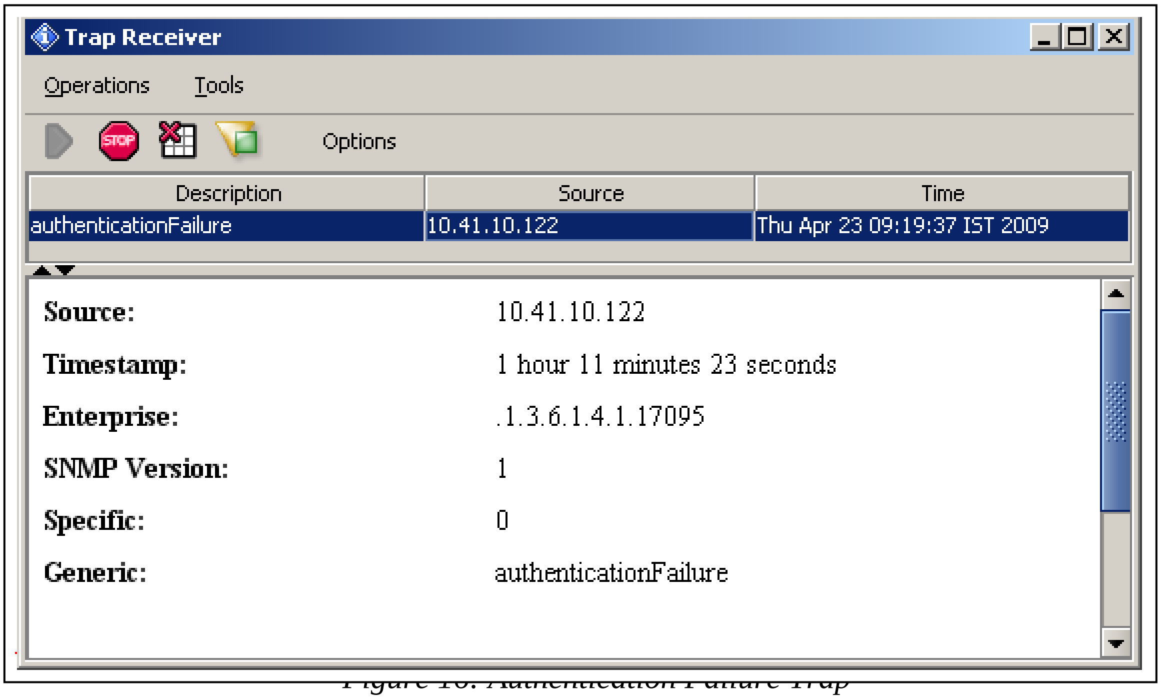
Figure 15: Analog Potentiometer Trap

- Push Button Trap – Press the appropriate button on the development board ('RB0' on PICDEM.net 2 board or 'S3' on Explorer 16 board) in order for the corresponding trap to be received by the 'Trap Receiver'.
- Authentication Failure Trap – By default, the Read Communities supported are 'public' and 'read'.

The configured Read Community name in the 'Advanced' tab should not be one of the Read Community names supported by the V2c agent for Authentication Failure Trap demo.
For example,

1. Configure 'mchp' as a Read Community to the browser.
2. Select the private MIB variable 'LED5' from the MIB tree and issue a 'Get' operation from the browser.

The ‘Result Table’ of the browser will not display any result, but the ‘Trap Receiver’ receives an ‘Authentication Failure’ trap as shown in Figure 16. This is intimation from the agent to the SNMP manager that there was an unauthorized attempt to access the private MIB variable of the data base.



Description	Source	Time
authenticationFailure	10.41.10.122	Thu Apr 23 09:19:37 IST 2009

Source: 10.41.10.122

Timestamp: 1 hour 11 minutes 23 seconds

Enterprise: .1.3.6.1.4.1.17095

SNMP Version: 1

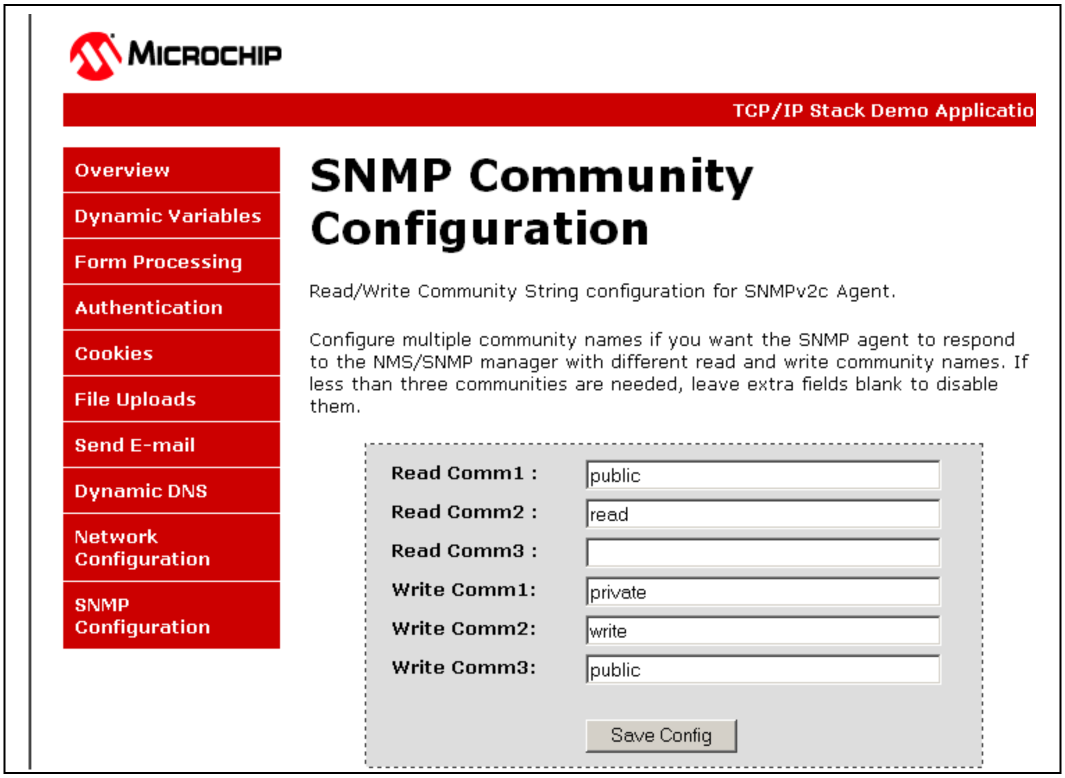
Specific: 0

Generic: authenticationFailure

Figure 16: Authentication Failure Trap

Configuring Multiple Communities to the V2c Agent

If an HTTP2 server is used with the Microchip TCPIP Stack, dynamically configure the Read and Write community names to the V2c agent from the "SNMP Configuration" web page. To access this web page, use "admin" as the username and "microchip" as the password.



SNMP Community Configuration

Read/Write Community String configuration for SNMPv2c Agent.

Configure multiple community names if you want the SNMP agent to respond to the NMS/SNMP manager with different read and write community names. If less than three communities are needed, leave extra fields blank to disable them.

Read Comm1 :	public
Read Comm2 :	read
Read Comm3 :	
Write Comm1:	private
Write Comm2:	write
Write Comm3:	public

Figure 17: SNMP Configuration Web Page