DIGI INTERNATIONAL, INC.

Accessing NET+OS's SNMP agent using MG-Soft's SNMP management Software

Using mainly screen shots, demonstrates the use of MG-Soft's SNMP management software in accessing NET+OS's SNMP agent.

1. Document History

Date	Version	Change Description
4/8/09	V1.2	Initial version
9/01/09	V1.3	Enter corrections
9/24/09	V1.4	Enter into info and glossary
9/24/09	V1.4	Use consistent pointers
10/6/09	V1.5	Added Digi Logo

2. Table of Contents

1. Document History 2
2. Table of Contents 2
3. Introduction 3
a. Problem Solved 3
b. Audience 3
c. Assumptions 3
d. Scope 3
e. Description technique used in this document 4
4. SNMP v1 Access 5
a. Introduction 5
5. SNMP V2c Access 23
a. Introduction 23
6. SNMP V3 Access 27
a. Introduction 27
7 Glossary 37

3. Introduction

a. Problem Solved

With the introduction of SNMP V3, we have received a number of queries from customers asking the correct method for connecting an SNMP browser to NET+OS V7.x's SNMP agent. No such document shipped with the NET+OS documentation as each SNMP browser's screens and methods are different. This document represents the first of several documents that address the specifics of using SNMP browsers for connecting to NET+OS V7.x's SNMP agent. This particular document is demonstrates the use of MG-Soft's SNMP browser. Additionally this document discusses using MG-Soft's browser in version 1, version 2c and version 3 modes.

b. Audience

This document is written for both technical and non-technical users can gain knowledge and ability to access a device running NET+OS V7.X and its SNMP agent, over the internet. The intent is that when followed, virtually any user should be able to both read and update SNMP MIBs using MG-Soft's MIB browser with the aid of this document. Screenshots are used extensively to facilitate this.

c. Assumptions

We assume that the user of this document has access to a Digi module of some kind, which is running an application built with some version of DIGI's NET+OS V7.X. Further we assume that the user has, at least, a small amount of knowledge about SNMP and what it is used for. No other knowledge should be required to gain useful information from this document.

d. Scope

The document's intent is to instruct a user in using MG-Soft's MIB Browser for connecting to, accessing and updating a MIB contained in a Digi NET+OS V7.X application, running on a Digi-based device. The device could be a Digi development board or a customer-developed board based on a Digi chip or module. Further this document could be used for training purposes or as a desk reference for later use.

The following are outside the scope of this document:

- Any description of ip, tcp, udp or any other protocols of the tcp/ip protocol stack.
- Any description of the implementation or operation of SNMP internals
- Any description is using any other SNMP MIB browser or the net-snmp command line MIB browser
- Any description of developing applications under Digi's NET+OS development environment (cli and ESP)

- Any description of compiling MIBs or including compiled MIBs into a MIB browser (the manufacturers include adequate information about doing this operation)
- Any detailed information about the differences between SNMP versions 1, 2c or 3 (this is briefly touched on in the glossary)

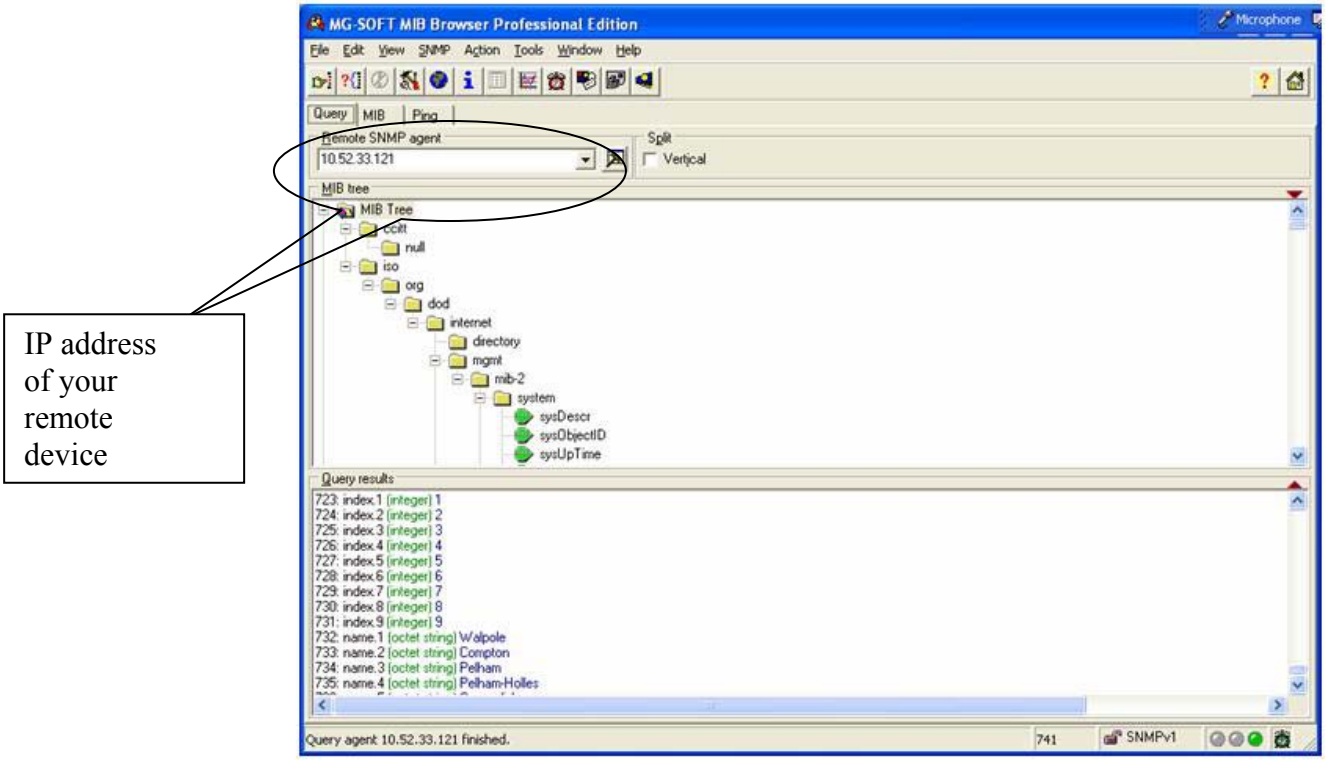
e. Description technique used in this document

This document demonstrates accessing the NET+OS SNMP agent using MG-Soft's SNMP management software. Further this document relies mainly on screen shots with small amounts of supporting text to guide the user through accessing (contacting) the device, getting field values and setting field values. In addition, in places where I felt it was appropriate, I have included screen shots of errors that can occur when attempting some of these operations.

4. SNMP v1 Access

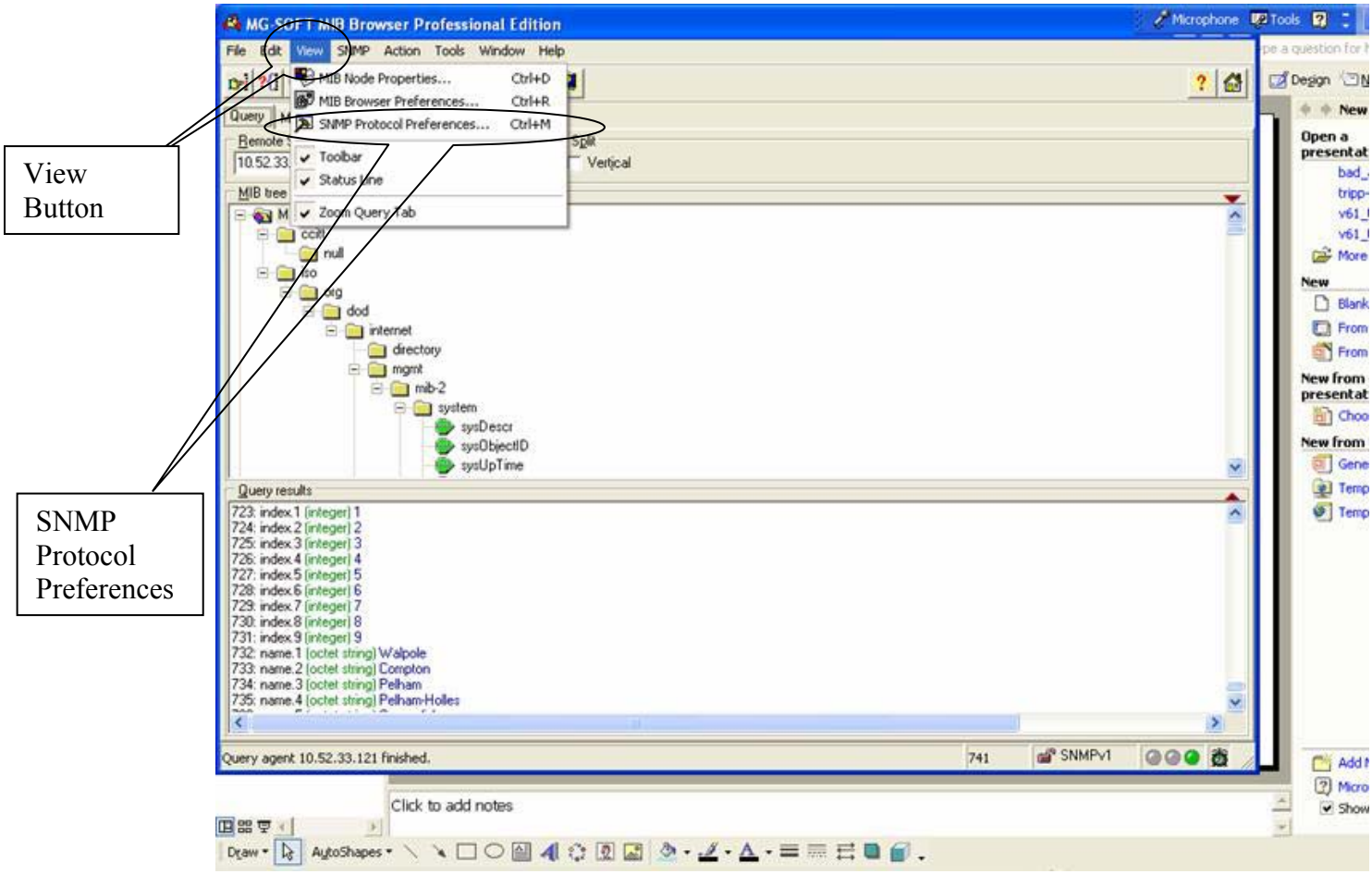
a. Introduction

This section uses screen shots to demonstrate accessing a NET+OS SNMP agent using MG-Soft's management software. This section demonstrates setting your SNMP version to V1 mode and setting your SNMP community name. It also demonstrates performing a get and a set. Lastly it displays some common errors that can be encountered when accessing an SNMP agent.

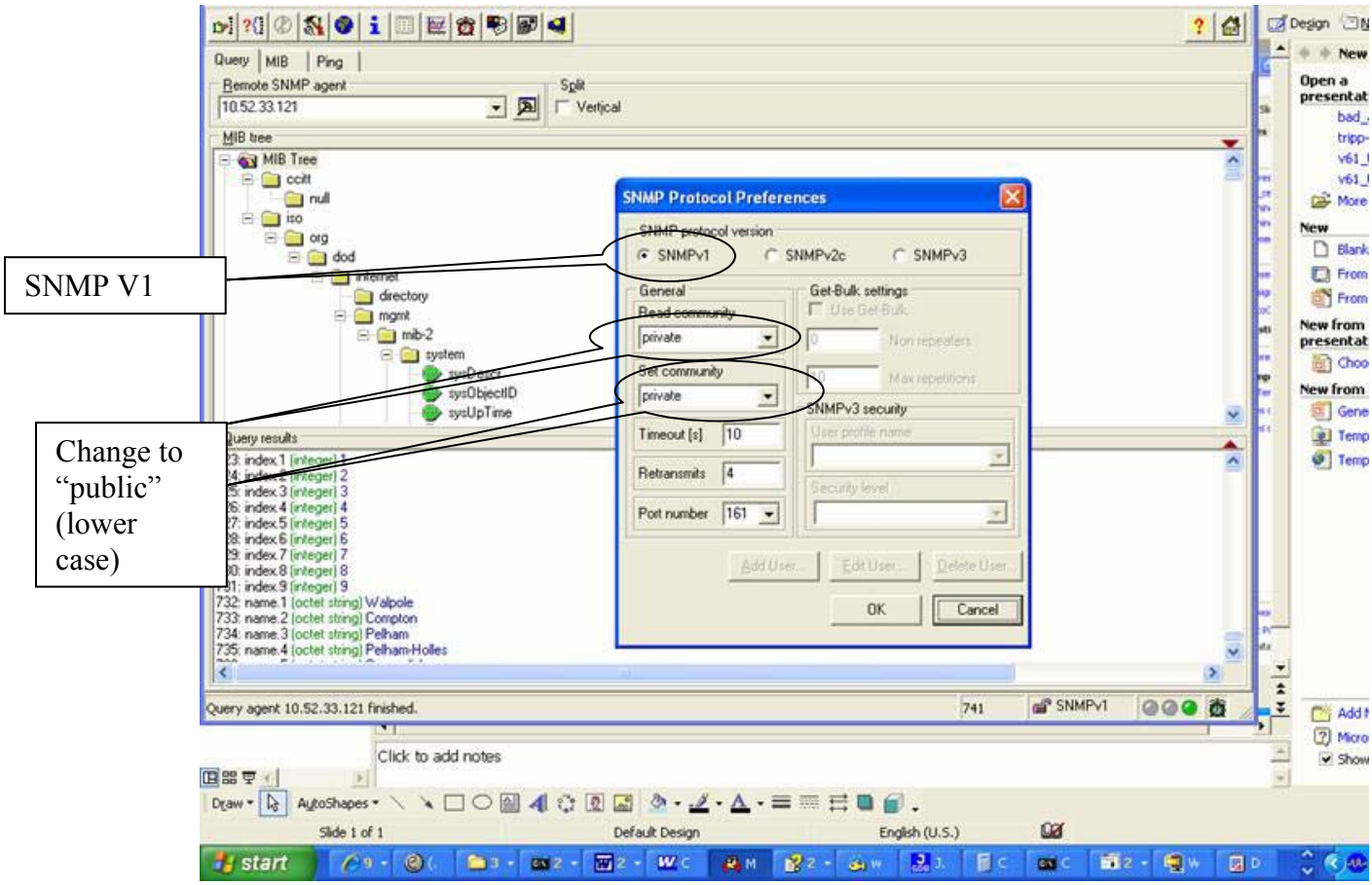


When you first start MG-Soft, you should see a page that looks like this screenshot. Type in your device's IP address, in the space circled above.

SNMP allows access by V1, V2c or V3 users. Advance to the next page, to see how to change the access version.

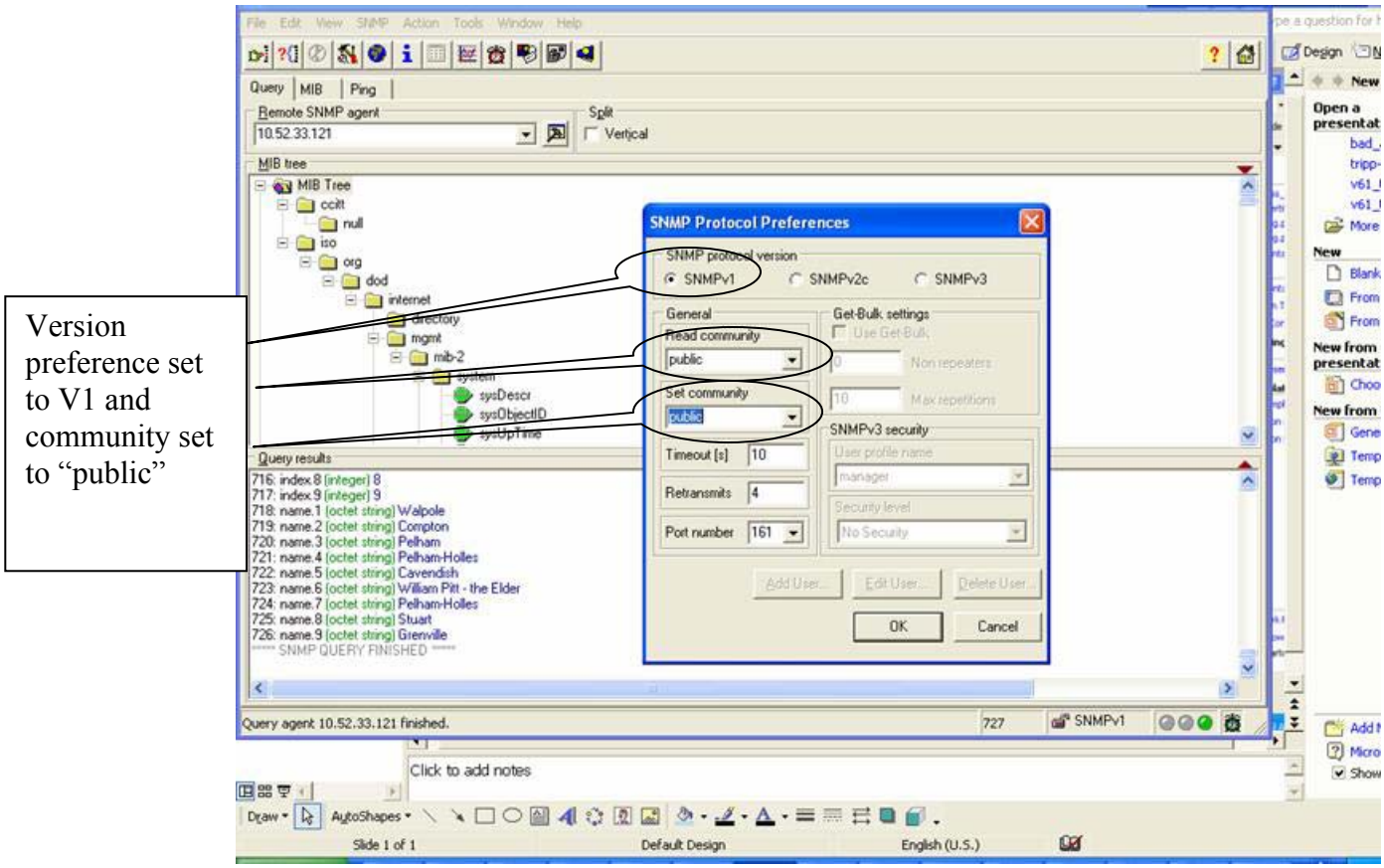


Click on the view menu item.
In the sub-menu that appears as a result of hitting the view menu button, select the menu item entitled “SNMP Protocol Preferences”.

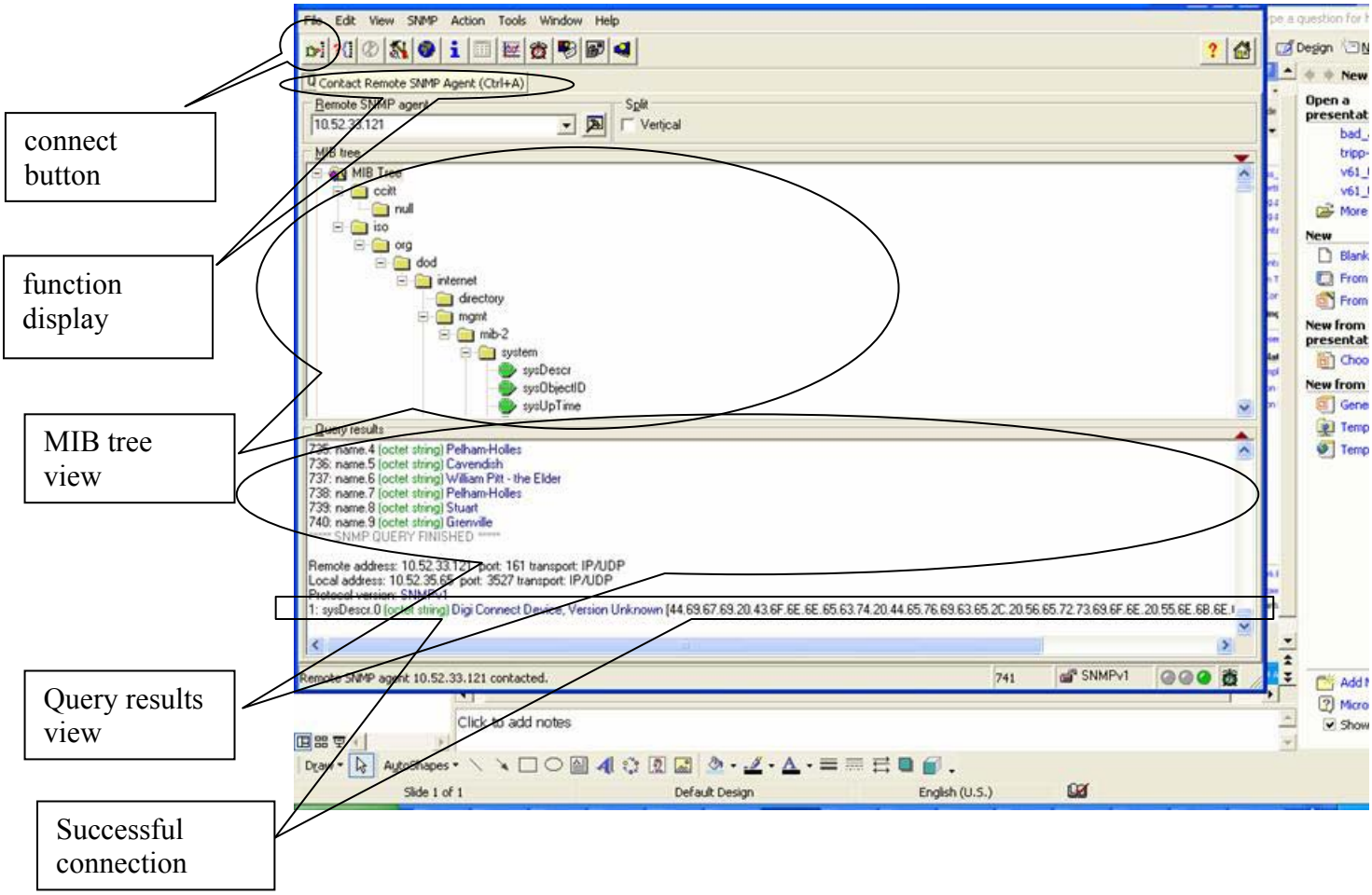


The discussion of SNMP usage begins with SNMP V1. So if the SNMP V1 radio button is not selected, then use your mouse to select it (only one of V1, V2c or V3 can be selected at one time). Since, at the moment, we will be performing gets, type "public" (lower case letters) into the two places where it may be displaying "private" in your screen and where it currently displays "private" in the screen above.

Hit the OK button when you are done.

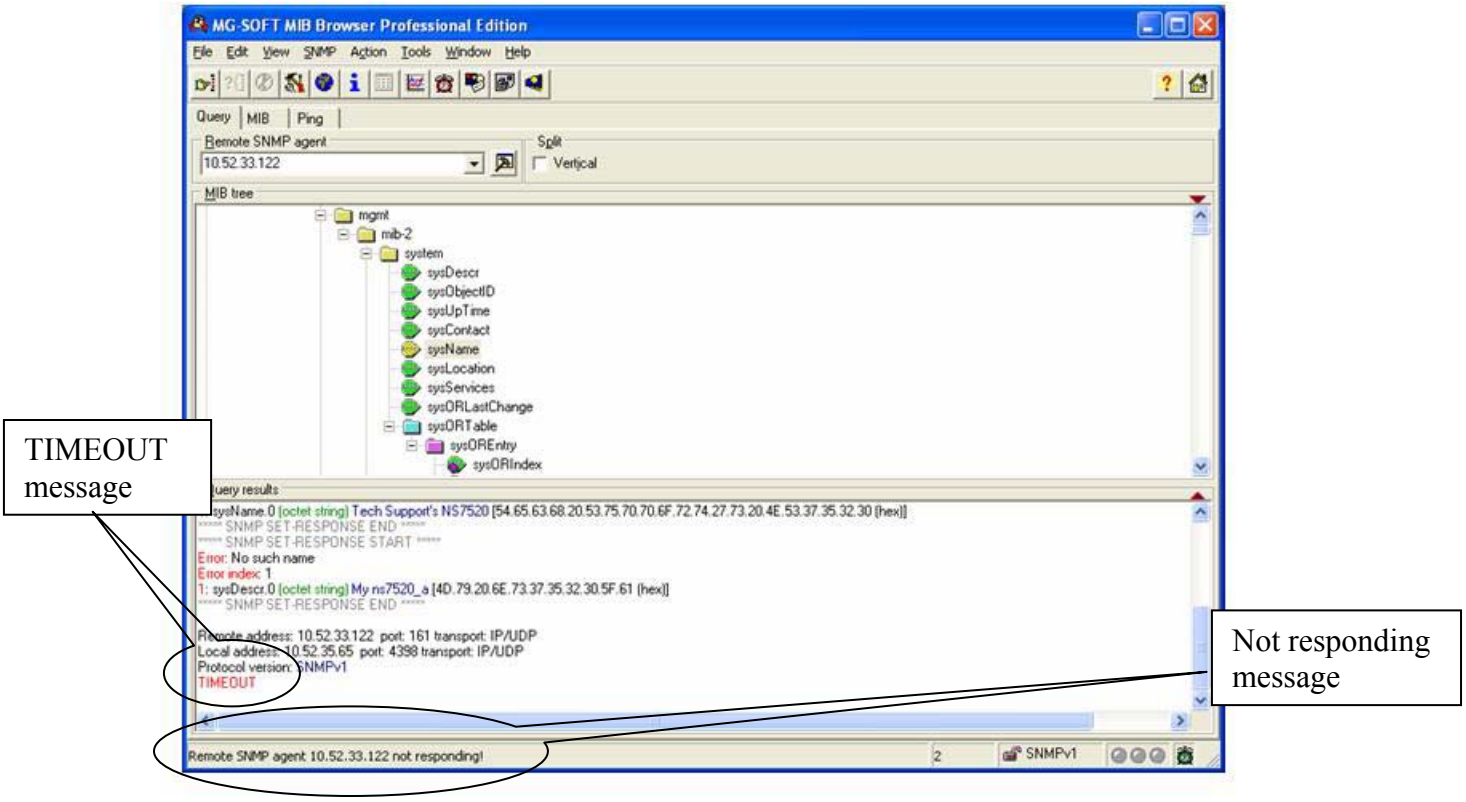


In this slide, the community named "private" has been changed to the community named "public".



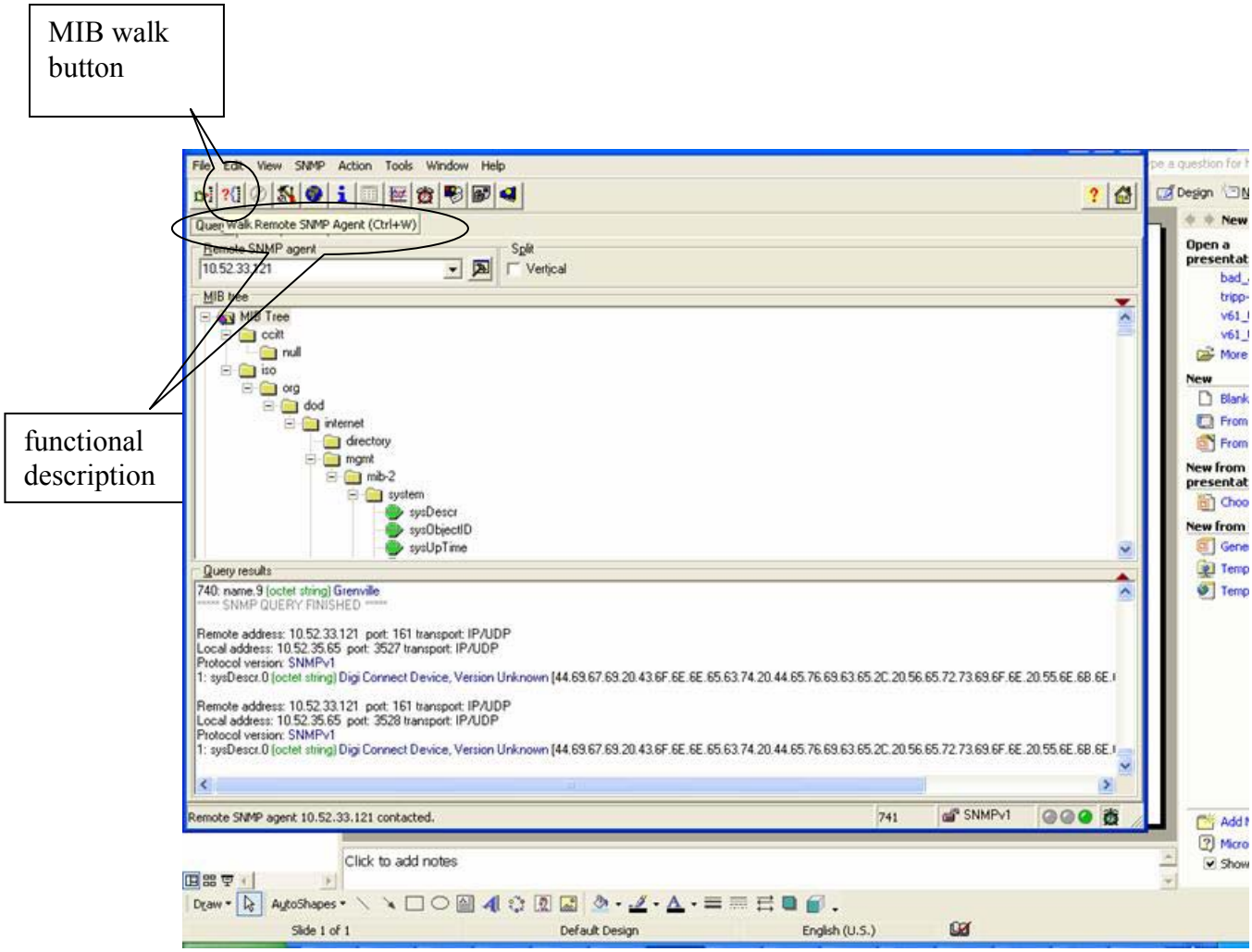
By default, the MG_Soft screen is split in two. The top part is the MIB tree view. The bottom part is the query view. At the bottom of the query results view, the line marked 1: sysDesc shows that we successfully connected with the SNMP agent in our device. Changing the community name forces a connect.

The button on the far left of the top row of iconized buttons, will also force a connect attempt to your device. Placing your mouse pointer over the button causes its function to be displayed below the button, as shown above.

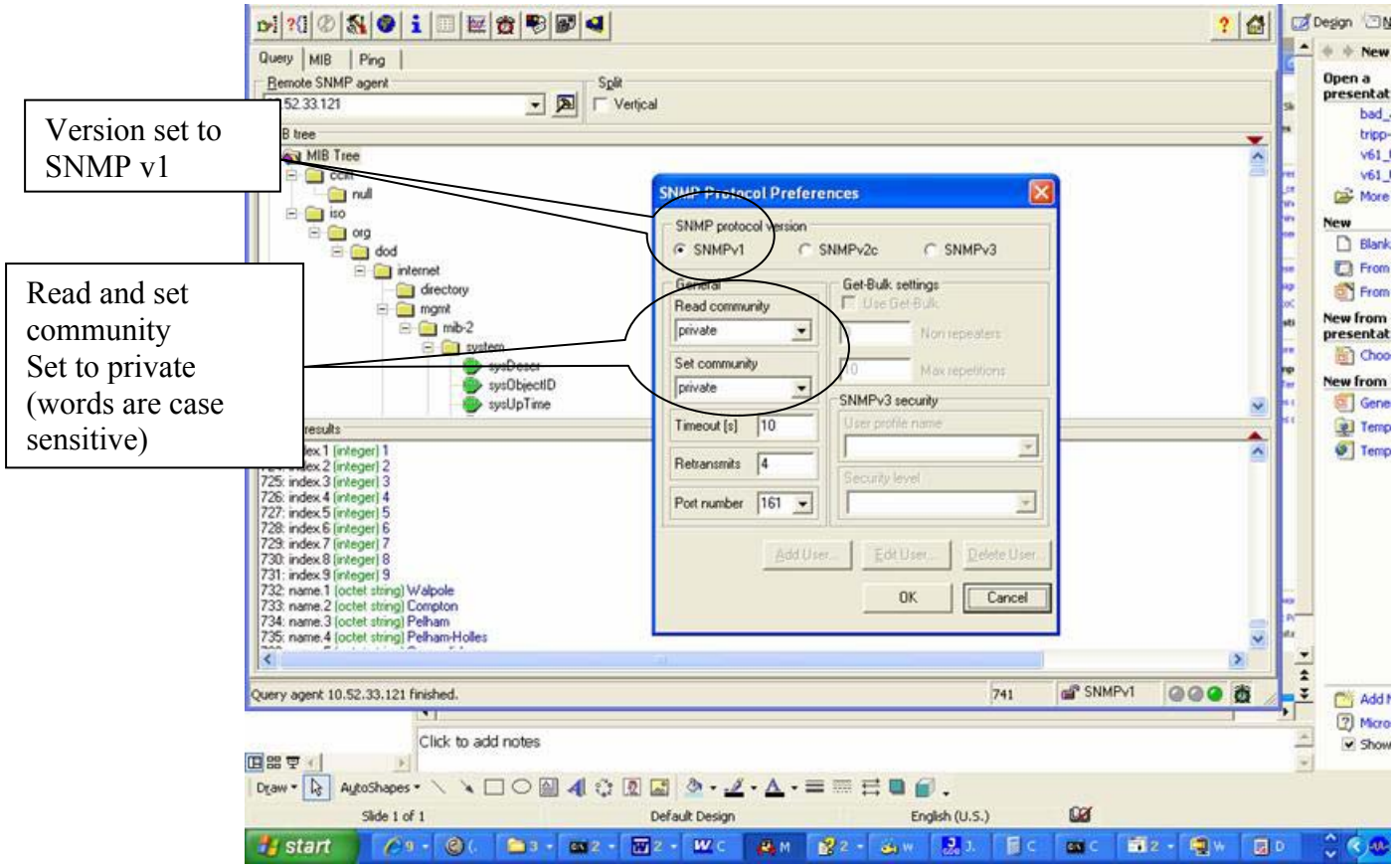


This screenshot demonstrates a failed SNMP V1 connect attempt. There are a couple of things to notice. First, is the text "TIMEOUT" at the bottom of the screen. If you notice above, I have changed the IP address of the device from that of a functioning device with an SNMP agent running on it, to the IP address of a non-existent device. MG-Soft attempted to contact the device, but failed. Second, in the border area of the screen, there is the following message: "Remote SNMP agent 10.52.33.122 is not responding".

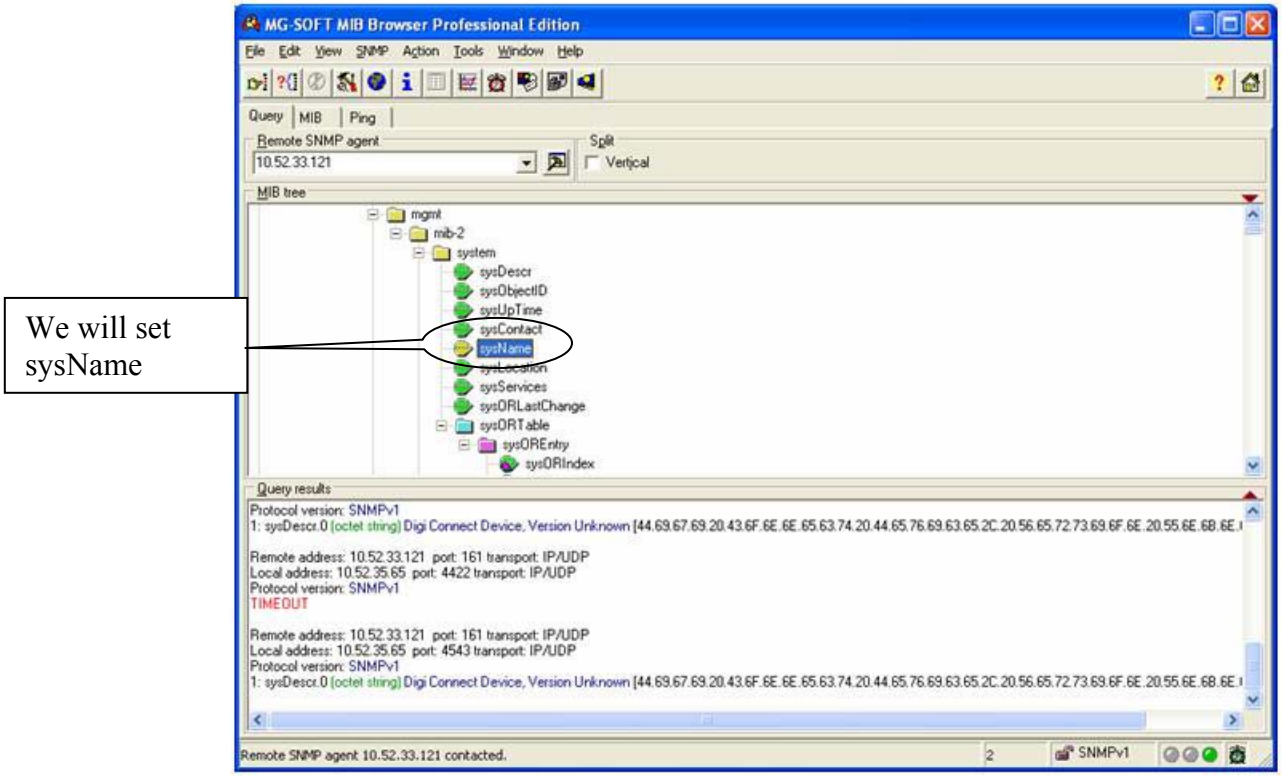
An additional note: If you have the community name wrong, you will get the same errors displayed in your MG-Soft screen as if you have the wrong IP address set. So, when you see this failure, check BOTH the community name AND the IP address of the device to which you are connecting.



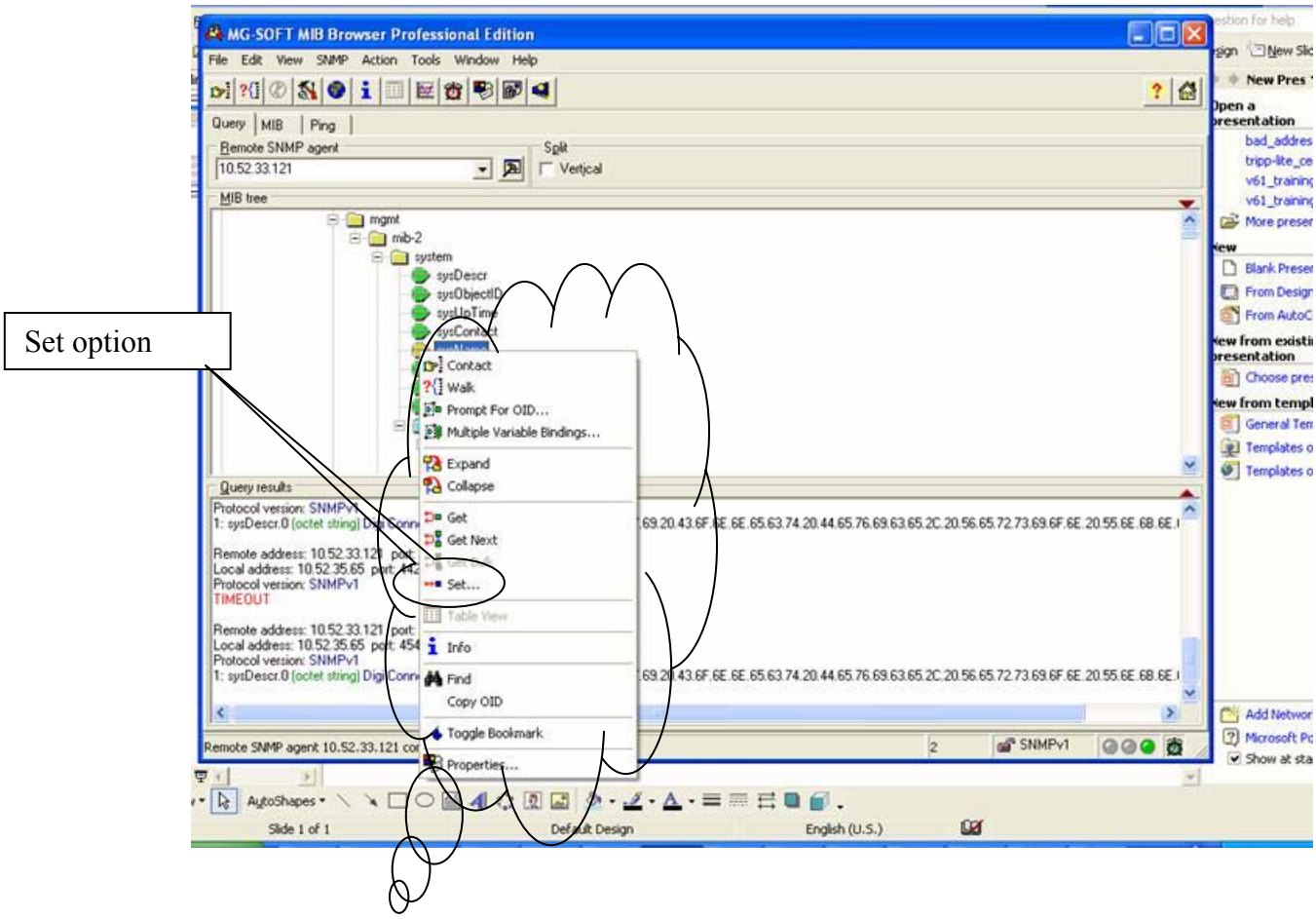
The second button from the left, at the top of the screen, causes a MIB walk to be performed, within the device to which you have connected. Again, placing your mouse pointer, over the button, causes its function to be displayed. If you are connected, hitting the MIB walk button will cause a MIB walk to commence. The results of the MIB walk are displayed in the query results window. (lower window)



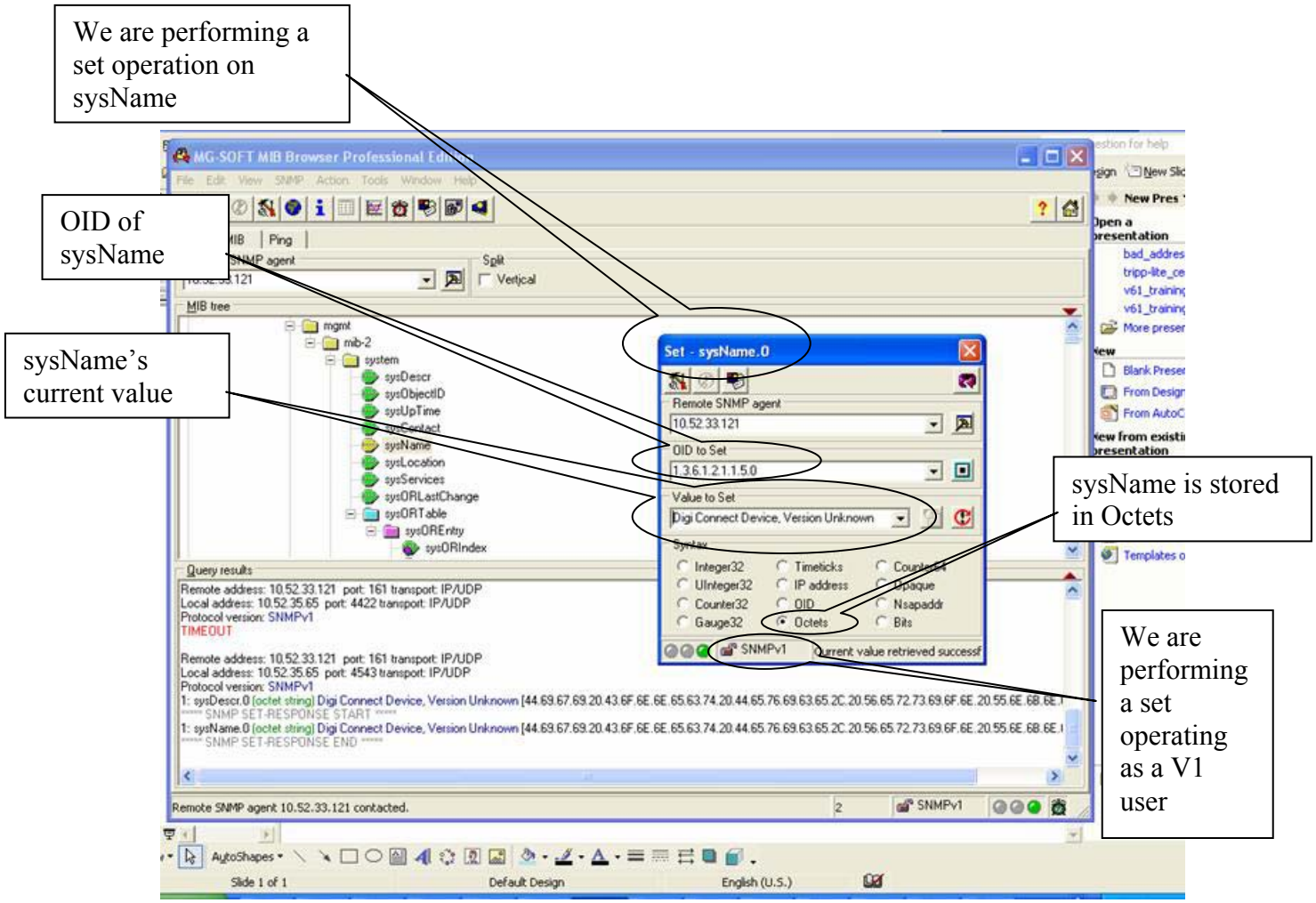
Next we'd like to set (update) a field in the MIB. In V1, you need to be in community private to perform a set operation. So going back to a previous step, click the view menu button and the SNMP protocol preferences menu option and you should see something like what is shown above. In the windows entitled Read community and Write community, change the community names from public to private. The community names need to be in lower case as they are case sensitive.
Click the OK button when you are done.



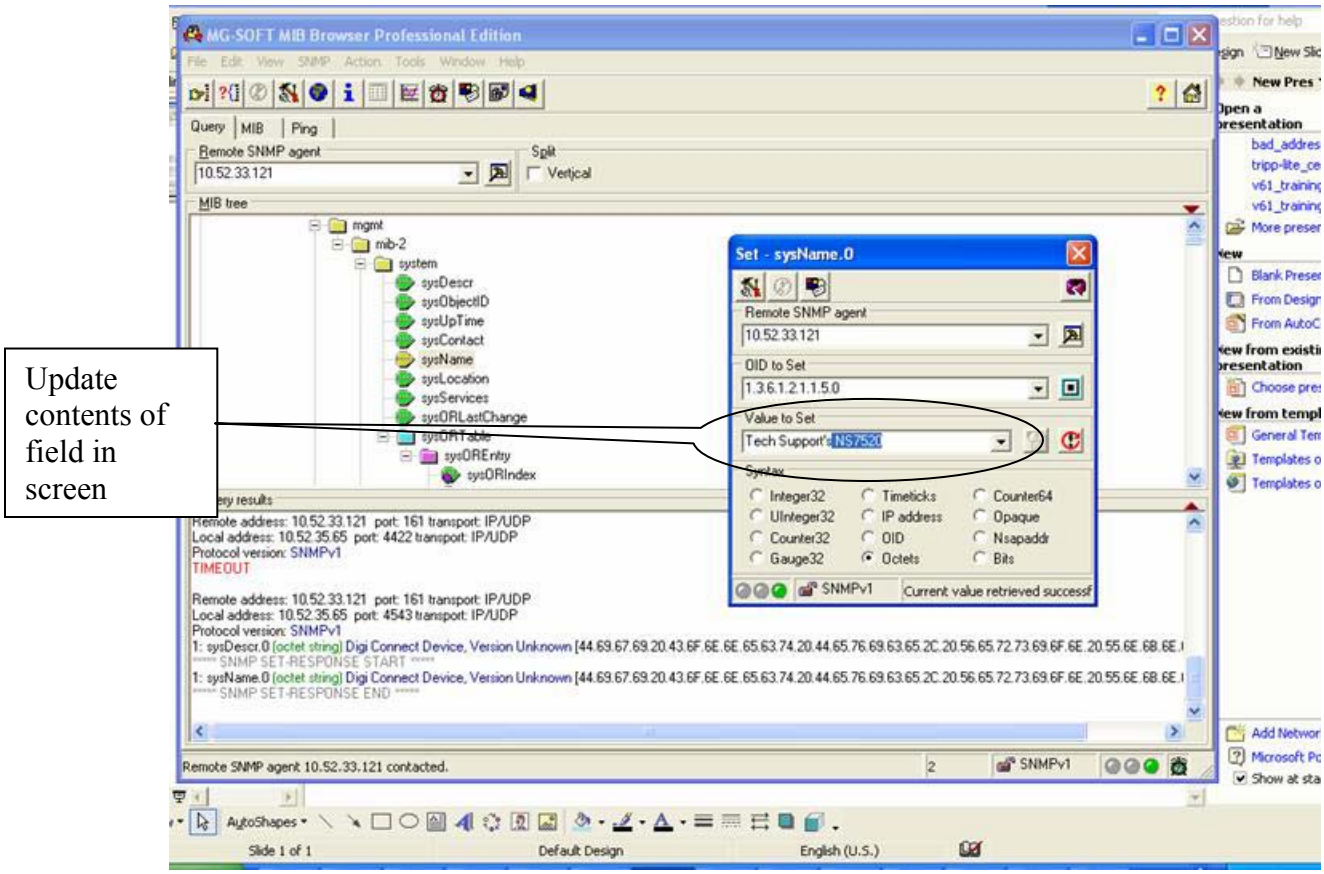
Before performing a set operation, you need to set the MIB tree view to the OID (the object) that is to be set. For this example, we are going to set sysName. In the above upper portion of the window, I have clicked on sysName, signaling that it is sysName that we want to set (update).



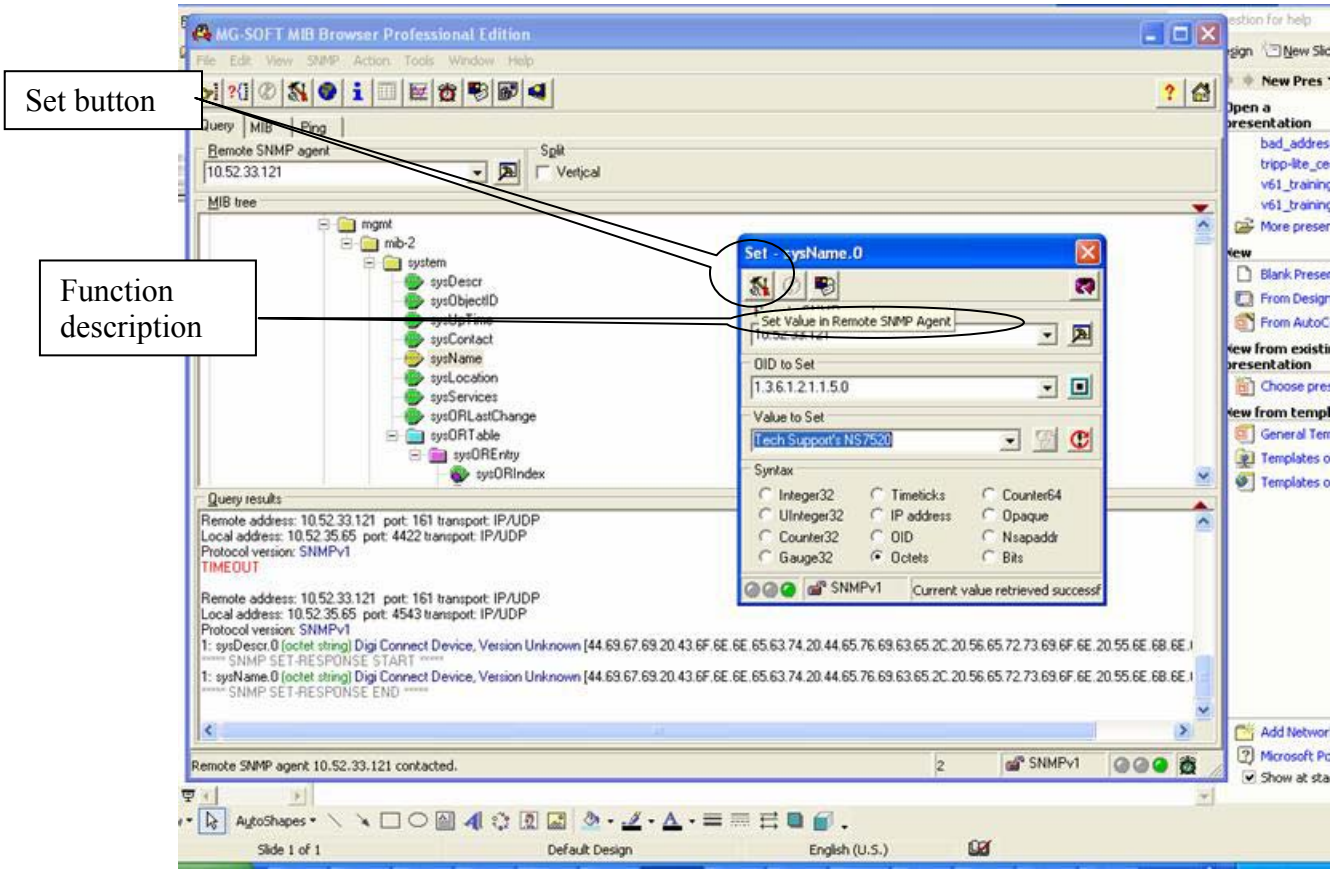
Right click on sysName. The following submenu appears. When this submenu appears, left click on the set option.



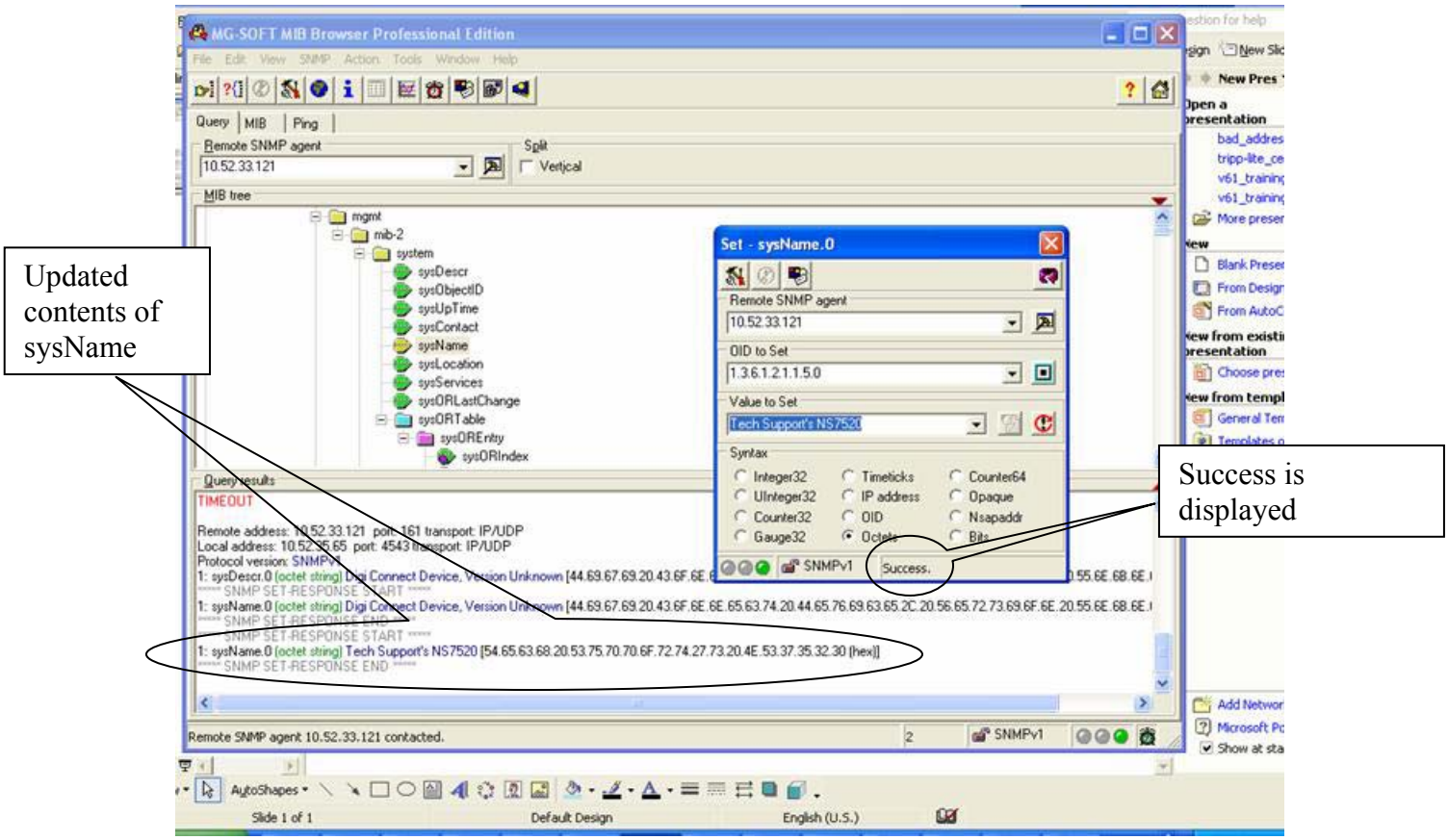
After clicking on the set option, the set submenu appears. There are a couple of things to notice. Set followed by the field to set are displayed on the top of the sub-window. Second the OID of sysName is displayed in the OID to set line. The current value of sysName is displayed in the Value to set line. This value is stored in Octets. Lastly we are running in V1 mode.



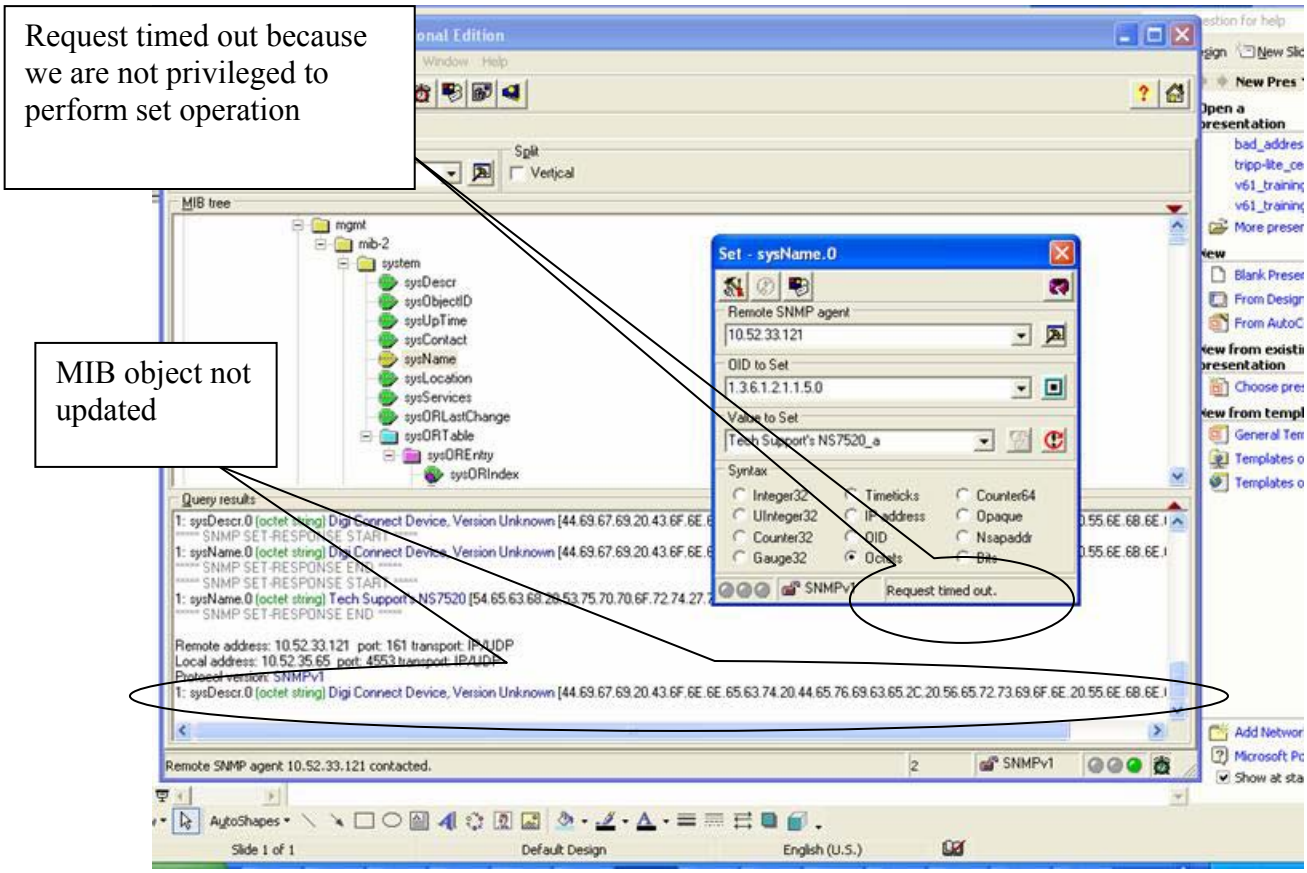
In this screen shot we have updated (changed) sysName from Digi connect device version unknown to Tech Support's NS7520. We have NOT yet updated the device. So far we have updated the screen only.



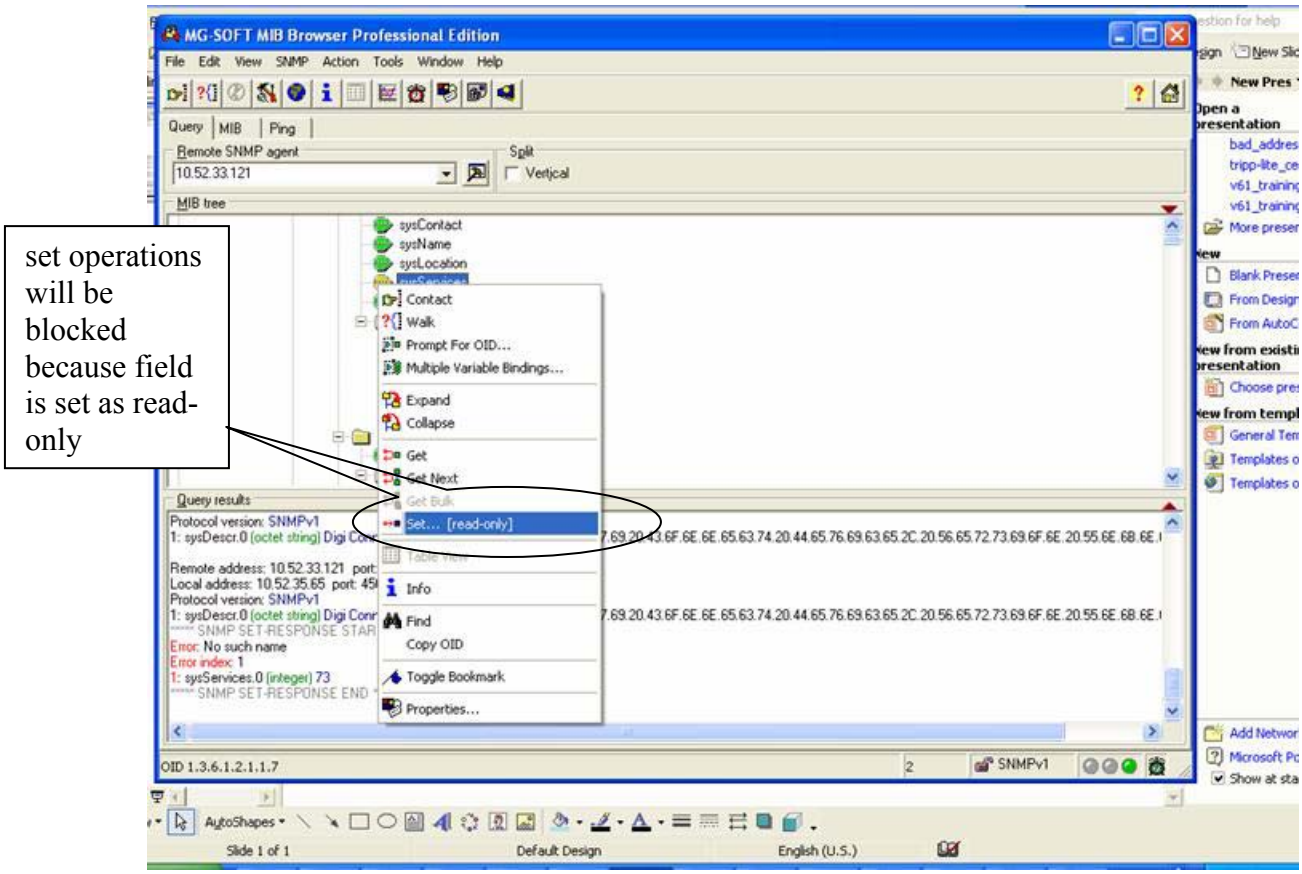
The button to actually perform the set, is the left most iconized button on the top of the sub-menu. Placing your mouse on top of the button will cause its function to be displayed. Click on the set button to cause the set operation to be performed.



There are two places to confirm the success of your set operation. First is the word success in the middle of the bottom line of the submenu. Second, in the main display, there is a line beginning with sysName.0 [Octet String] and the updated contents of sysName. Your operation set was successful.

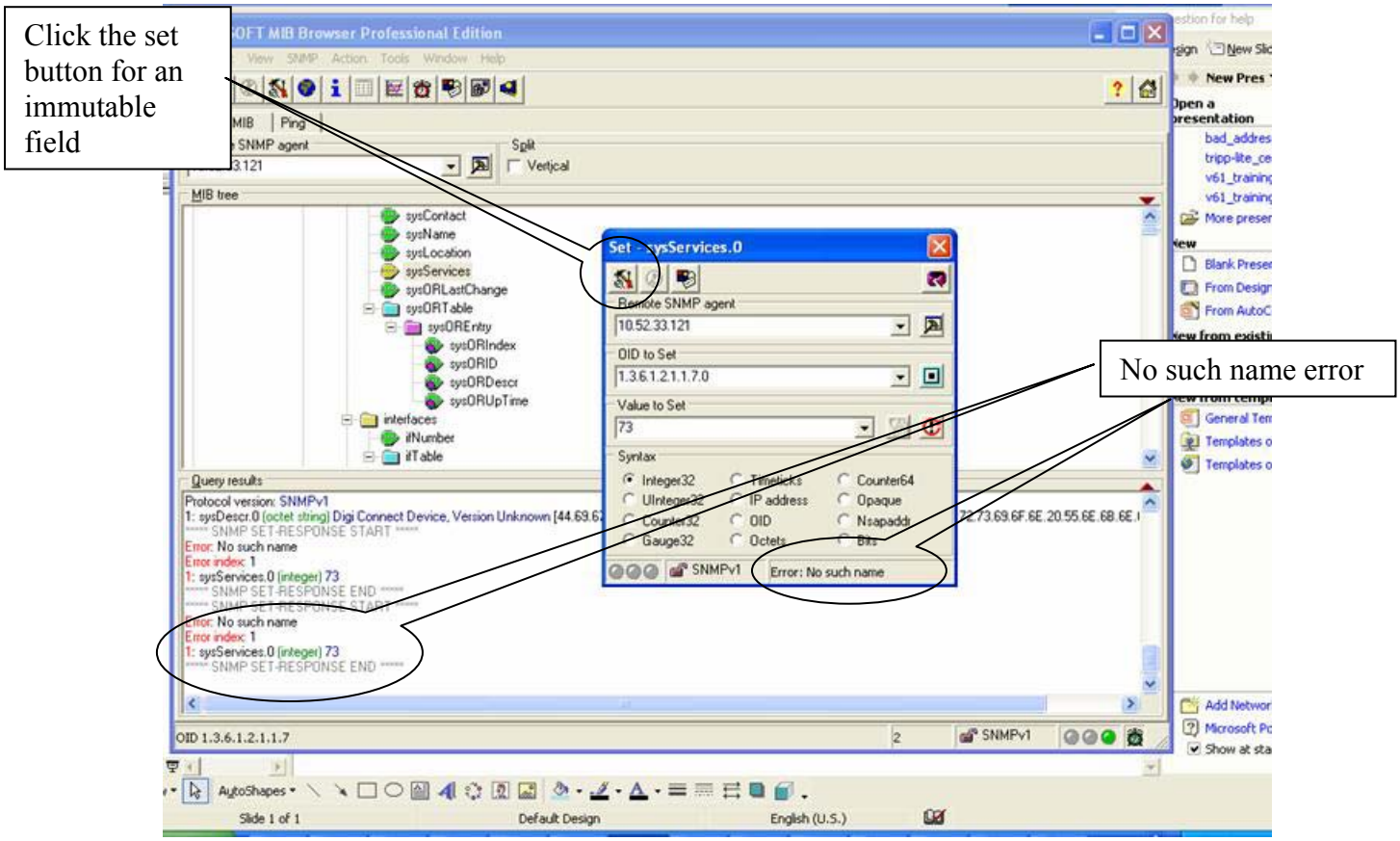


In this case, we did not change the community name from public to private. Therefore we do not have the privileges to update this field. There are two pieces of information that tell us that the set operation failed. The timed out message at the bottom of the sub-menu and the fact that the updated contents of sysName are NOT displayed in the Query results window of the main screen.



Another error that can happen is attempting to set (update) a field that is NOT modifiable (immutable). Now in this case, I have set my community name back to private. Thus I have the privileges to set fields that are settable. On the other hand, I am going to attempt to set a field that the SNMP agent does not allow to be set.

The first clue to a problem is that the set menu item in the sub-menu shows [read-only] for this field. If you look back at this stage of the operation for sysName, set is displayed for the menu item but [read-only] does NOT appear.

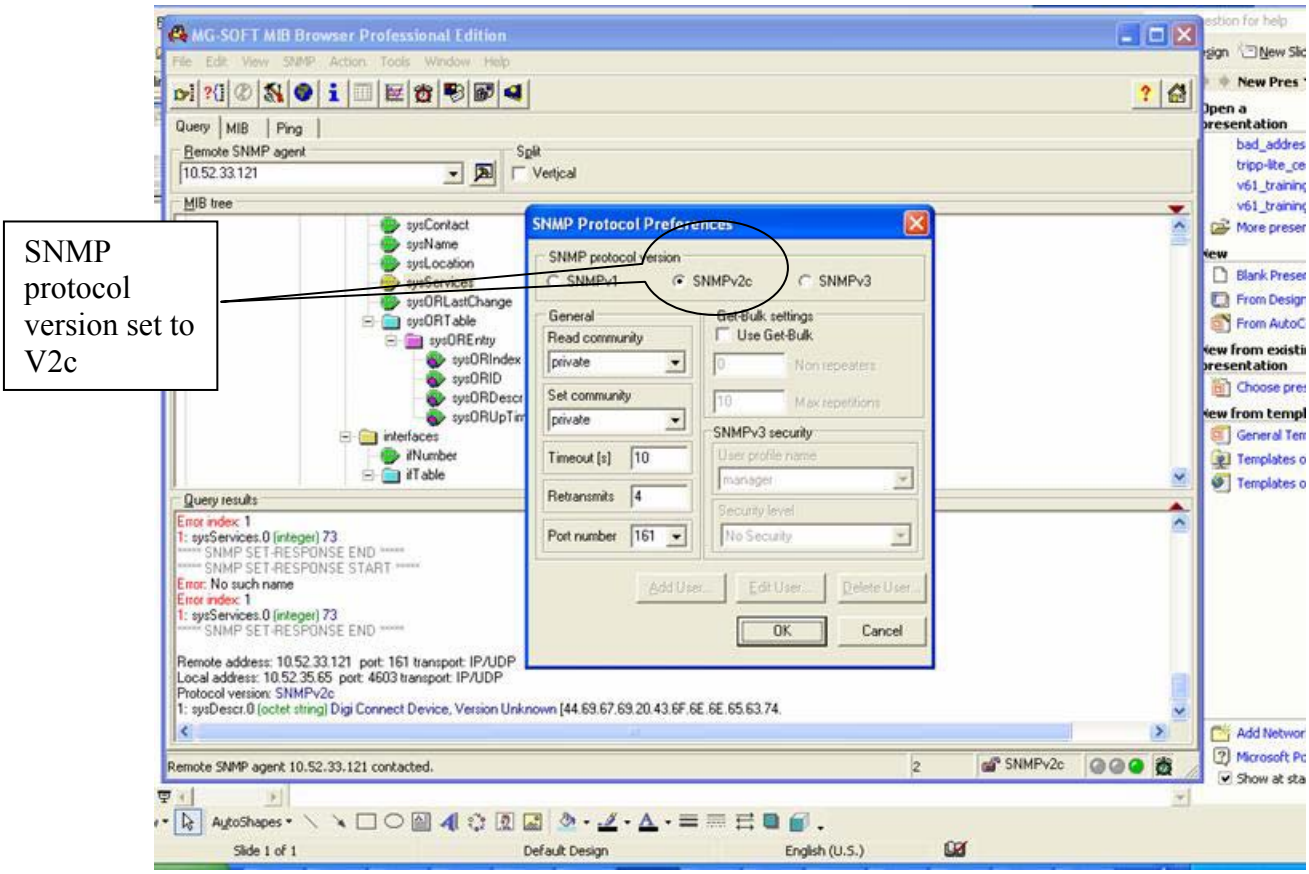


If we continue and actually try and set the field, we get a No such name error both in our set sub-menu and in the Query results window of the main MG-Soft window.

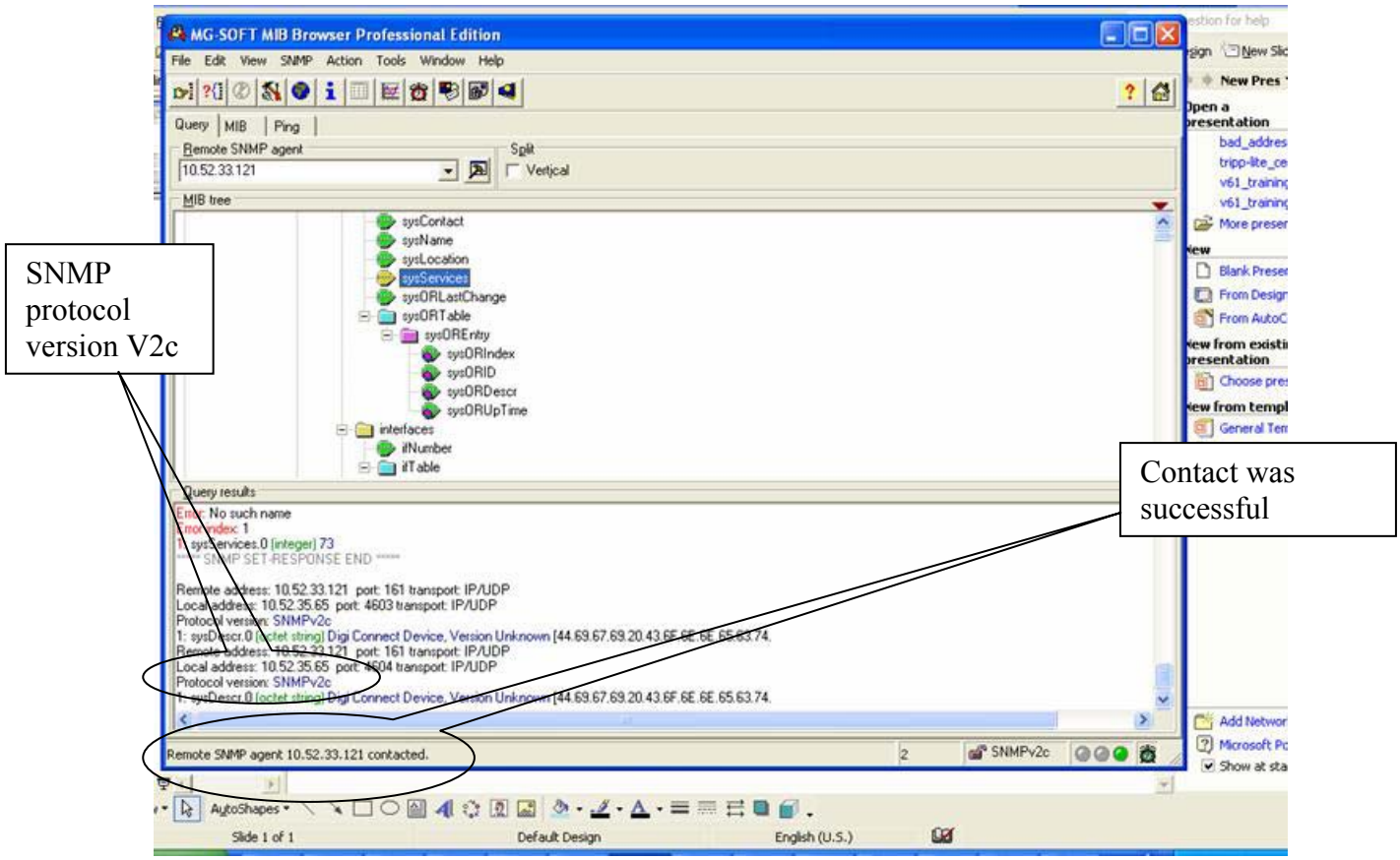
5. SNMP V2c Access

a. Introduction

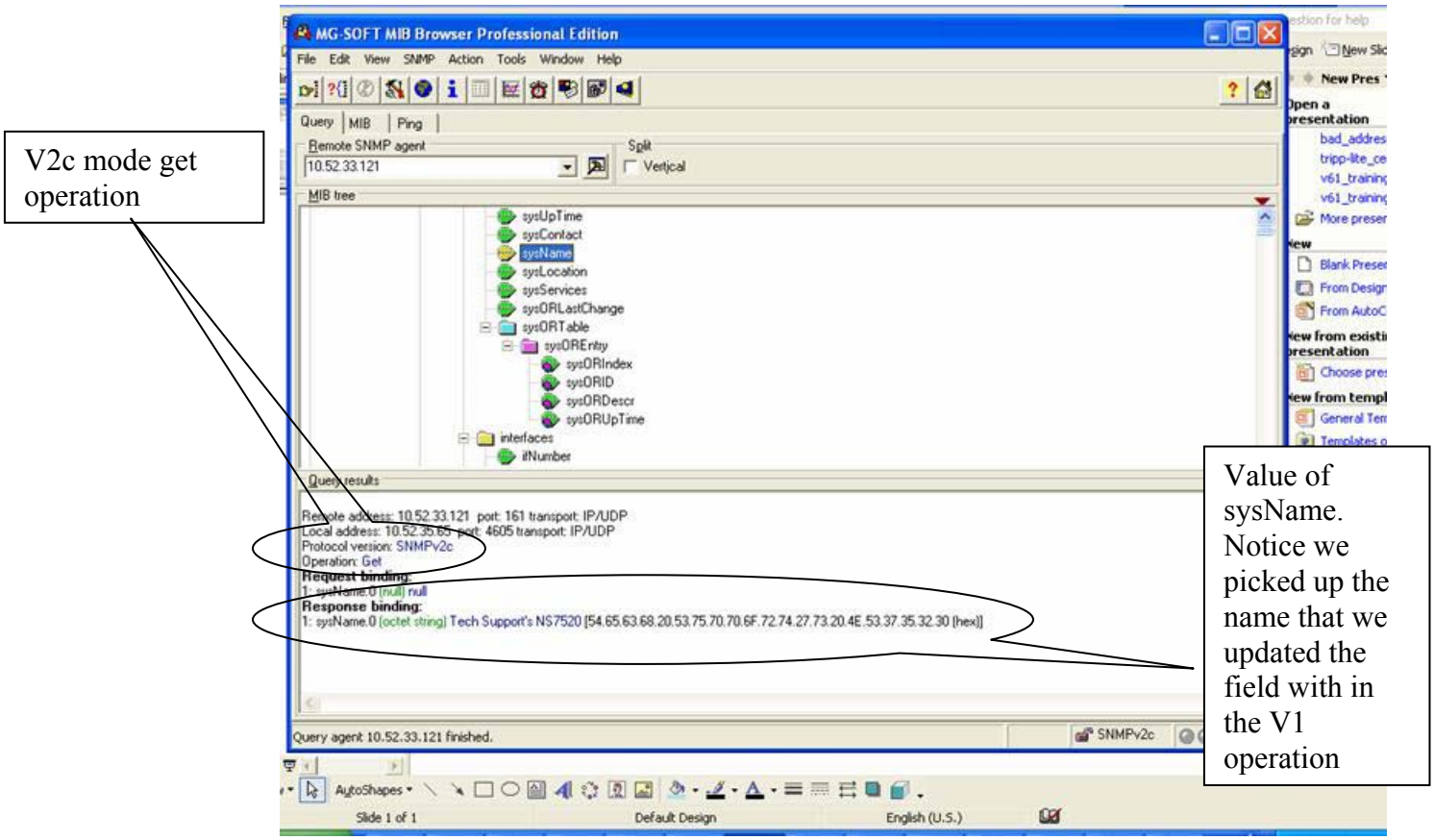
This section uses screen shots to demonstrate accessing NET+OS SNMP agent using MG-Soft's SNMP management software. Since SNMP V1 and SNMP V2c are quite similar at this level, this section only demonstrates the differences between SNMP V1 and SNMP V2c.



In this case we have set the SNMP protocol version to V2c. I am leaving the read and write community names as private, as we went through all of the cases for get and set using SNMP V1. As stated in V1, use your mouse to set the radio button to V2c. Click OK when you are done.



After clicking the OK button, we have again accessed the device, using SNMP, but this time as an SNMP V2c user. You'll notice that in the Query results window, the protocol version is now listed as V2c. If you go back and look at the V1 instances, the protocol version was listed as V1. Also notice that at the bottom of the screen that we successfully contacted the device.



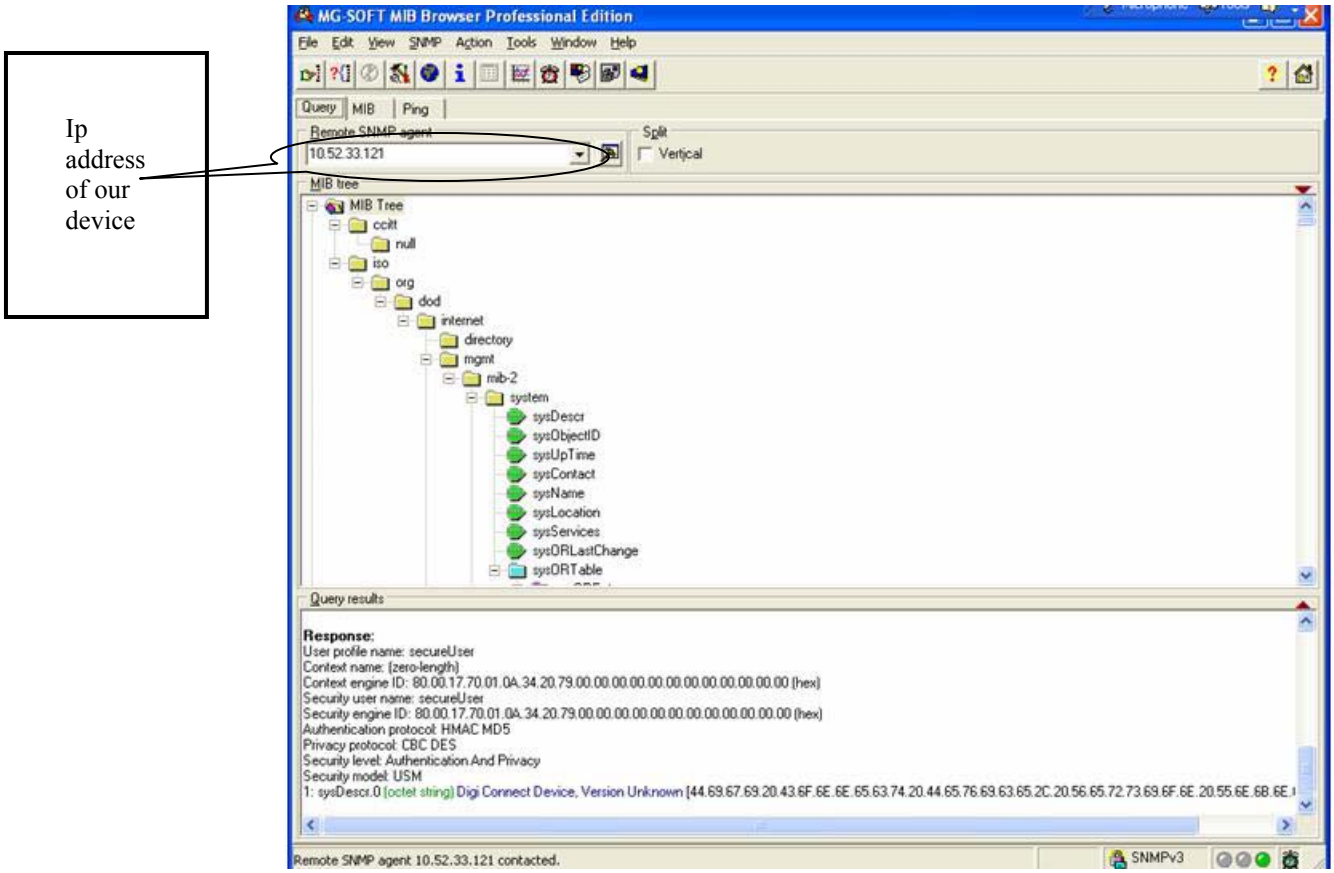
In this picture, we access the device's sysName in V2c mode.

6. SNMP V3 Access

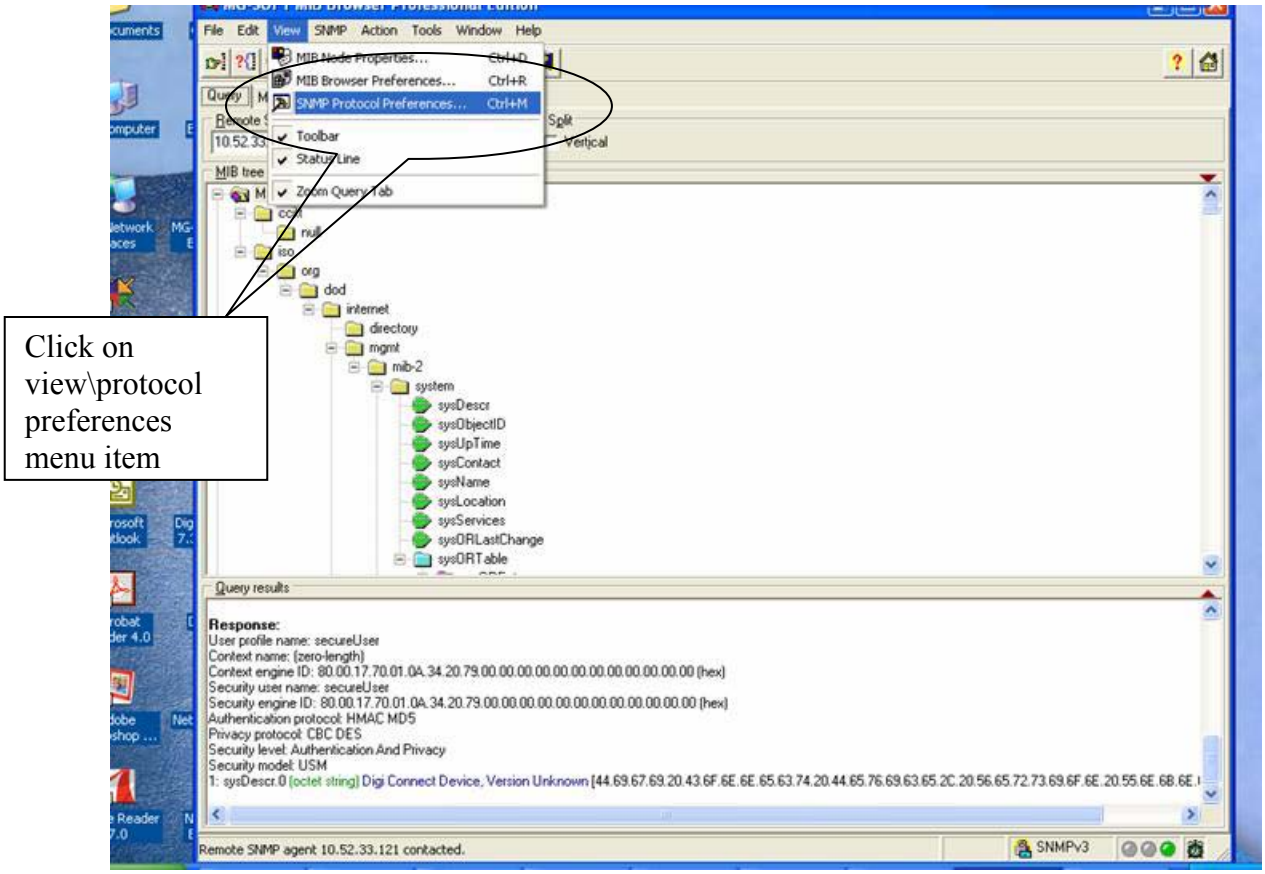
a. Introduction

This section demonstrates setting up the user as a V3 user. Once your V3 users are set up, the acts of get, set and walk are virtually the same as doing gets, sets and walks in SNMP V1 and SNMP V2c. Therefore, I will ask you to refer to get and set examples in the SNMP V1 and SNMP V2c sections.

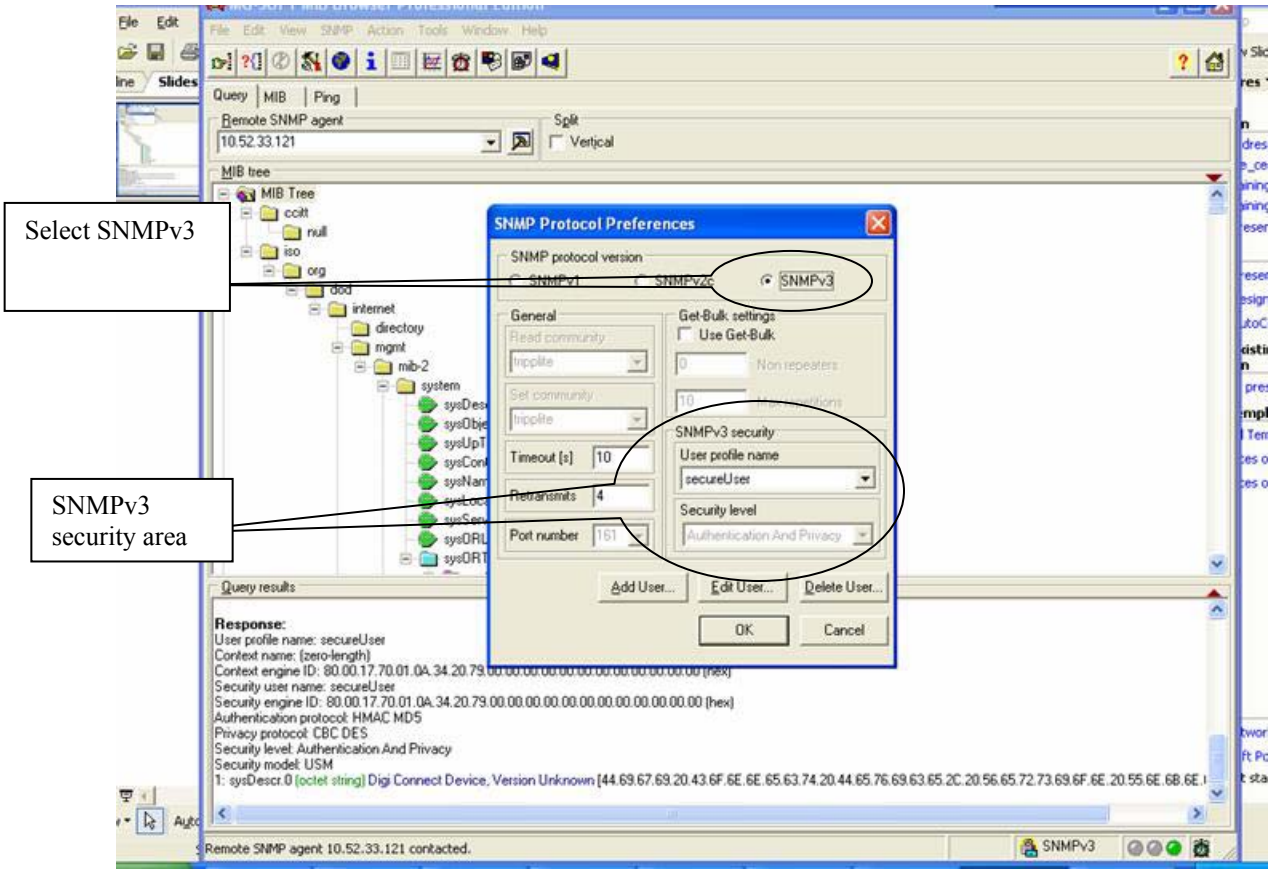
SNMP V3 adds authentication and encryption to the capabilities of SNMP V1 and SNMP V2c. Authentication refers to the ability to log into a service, such as SNMP, using a user name and a password. Encryption refers to the ability to encode data being passed between the client (MIB browser) and the server (SNMP agent).



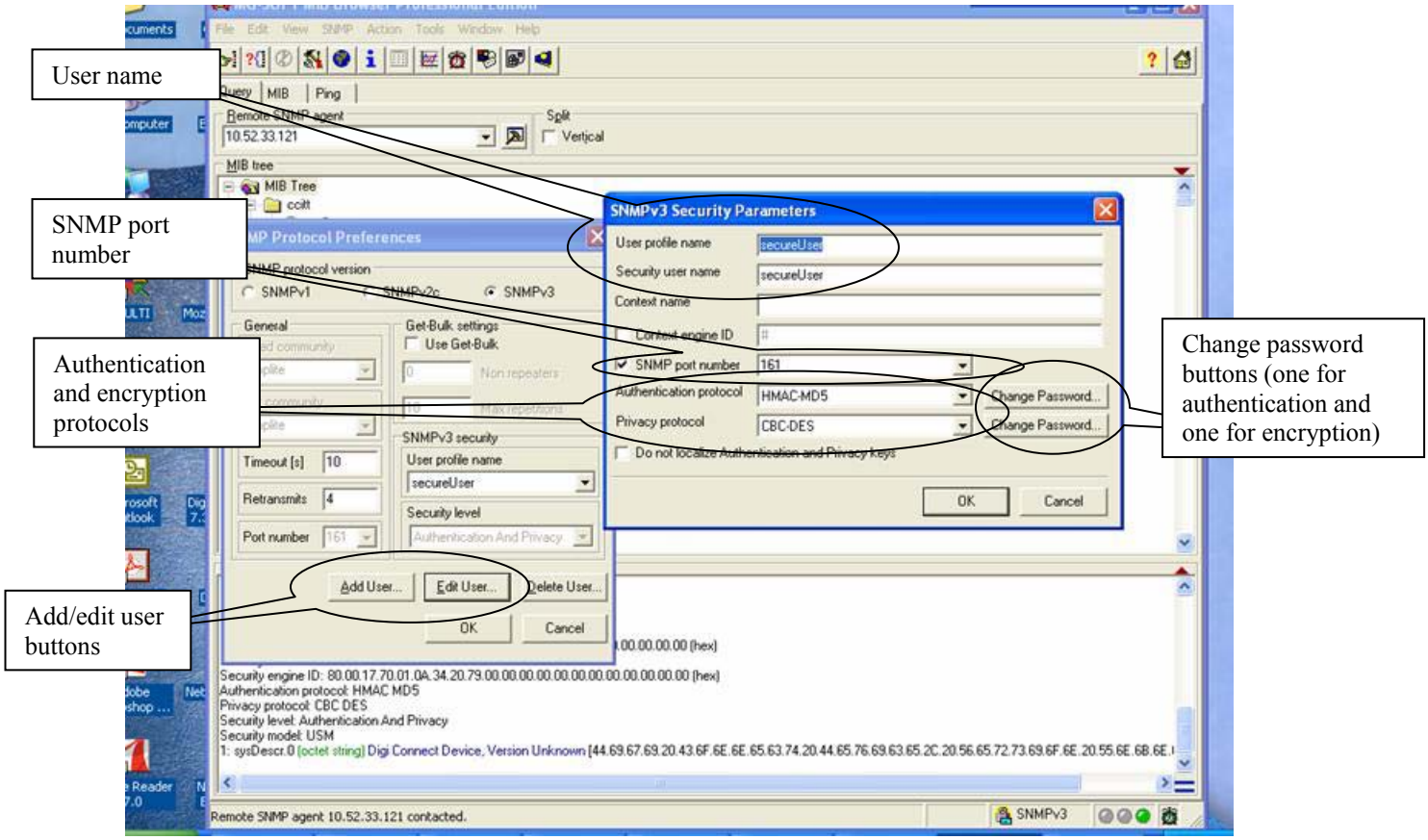
This screen shot looks the same as the beginning screen shots for SNMPV1 and SNMP V2c. The ip address of the device we want to access is displayed in a rectangular block near the top left of the MIB browser screen.



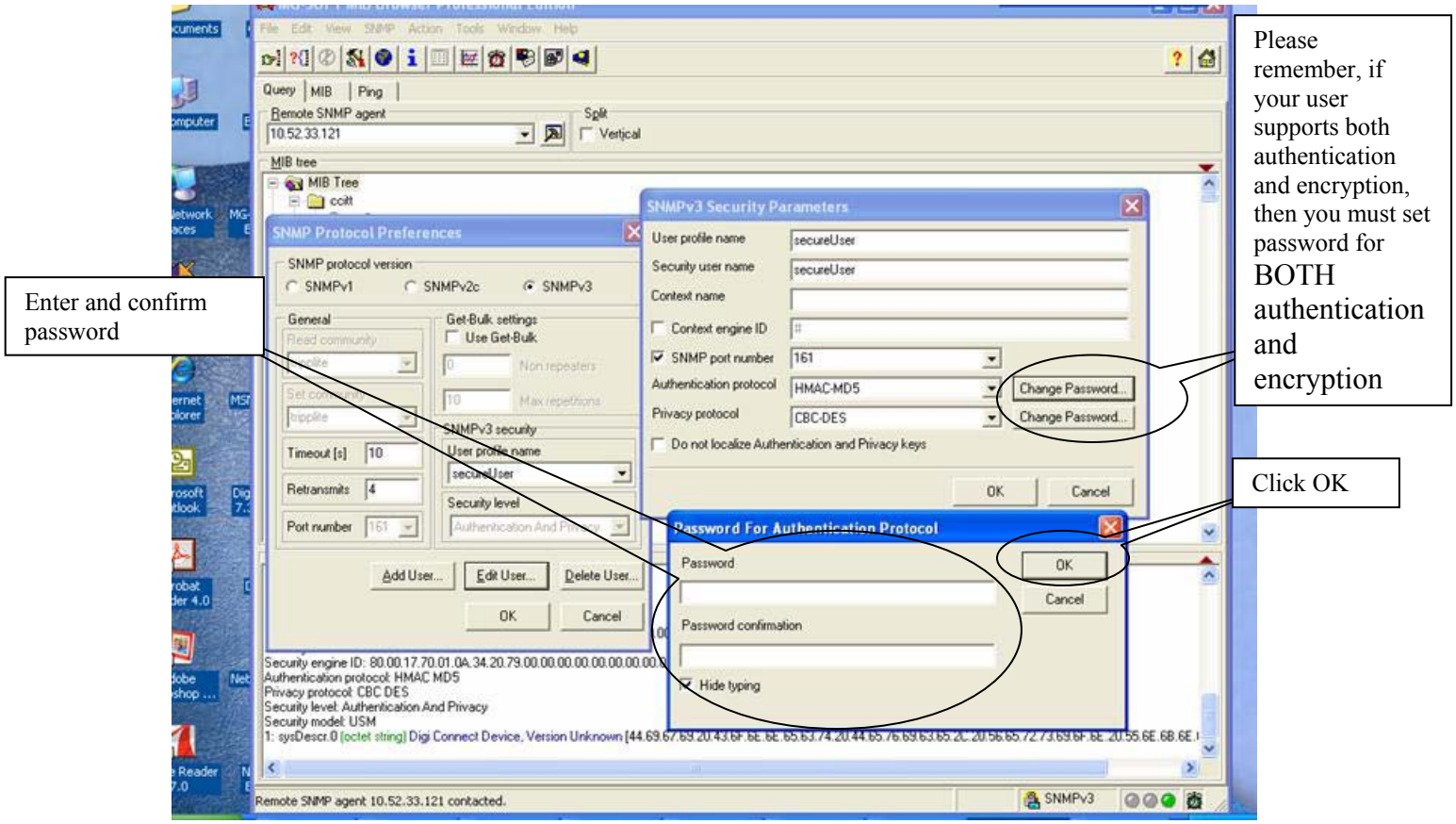
As with SNMP V1 and SNMP V2c we need to set the SNMP version that MG-Soft will use for accessing the device. So first click view and within view click SNMP Protocol Preferences



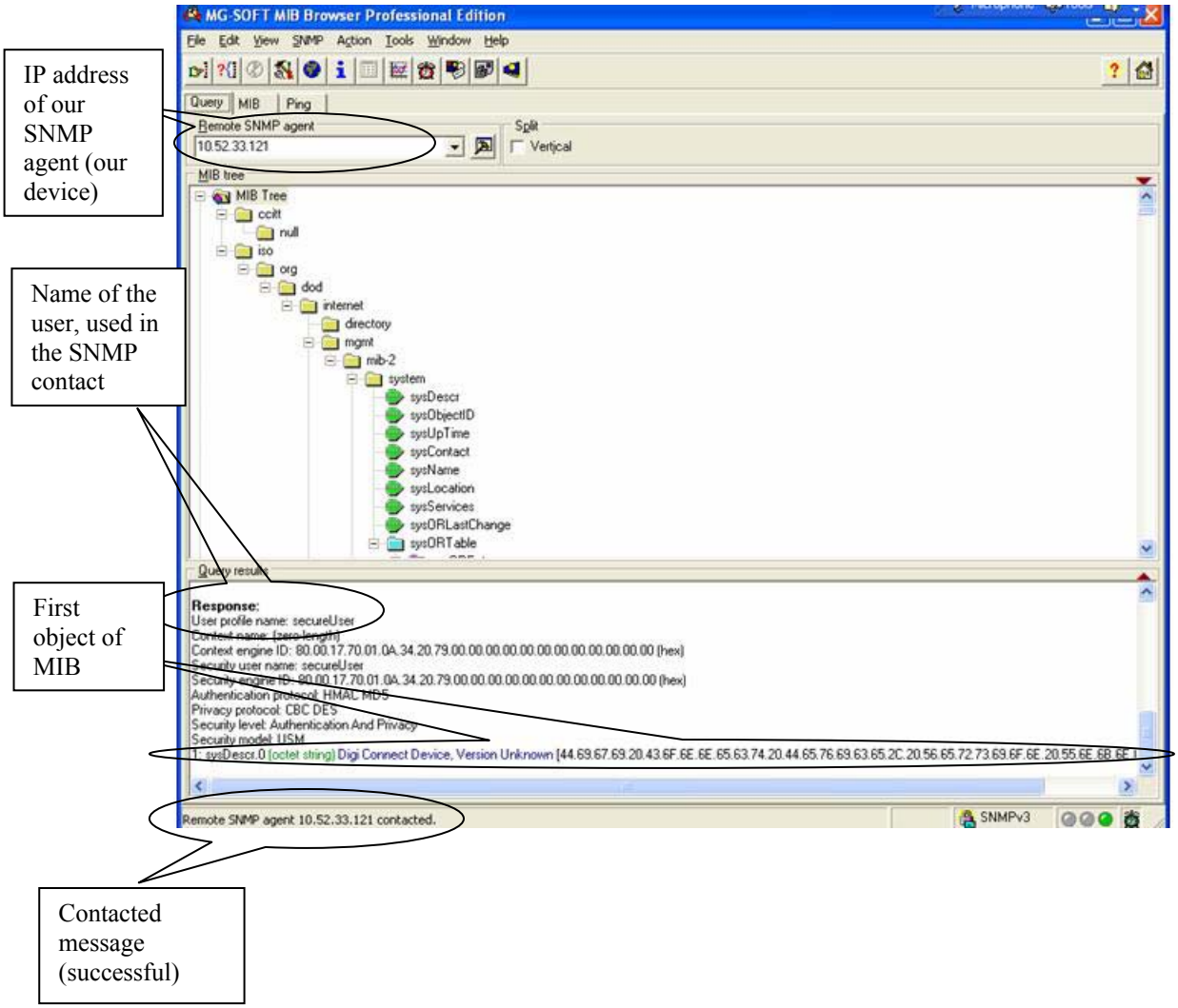
When the SNMP protocol Preferences screen appears, click the SNMPv3 radio button. When you do that you'll notice that in the bottom right, the SNMPv3 security area of the window is no longer grayed out. We'll deal with that shortly.



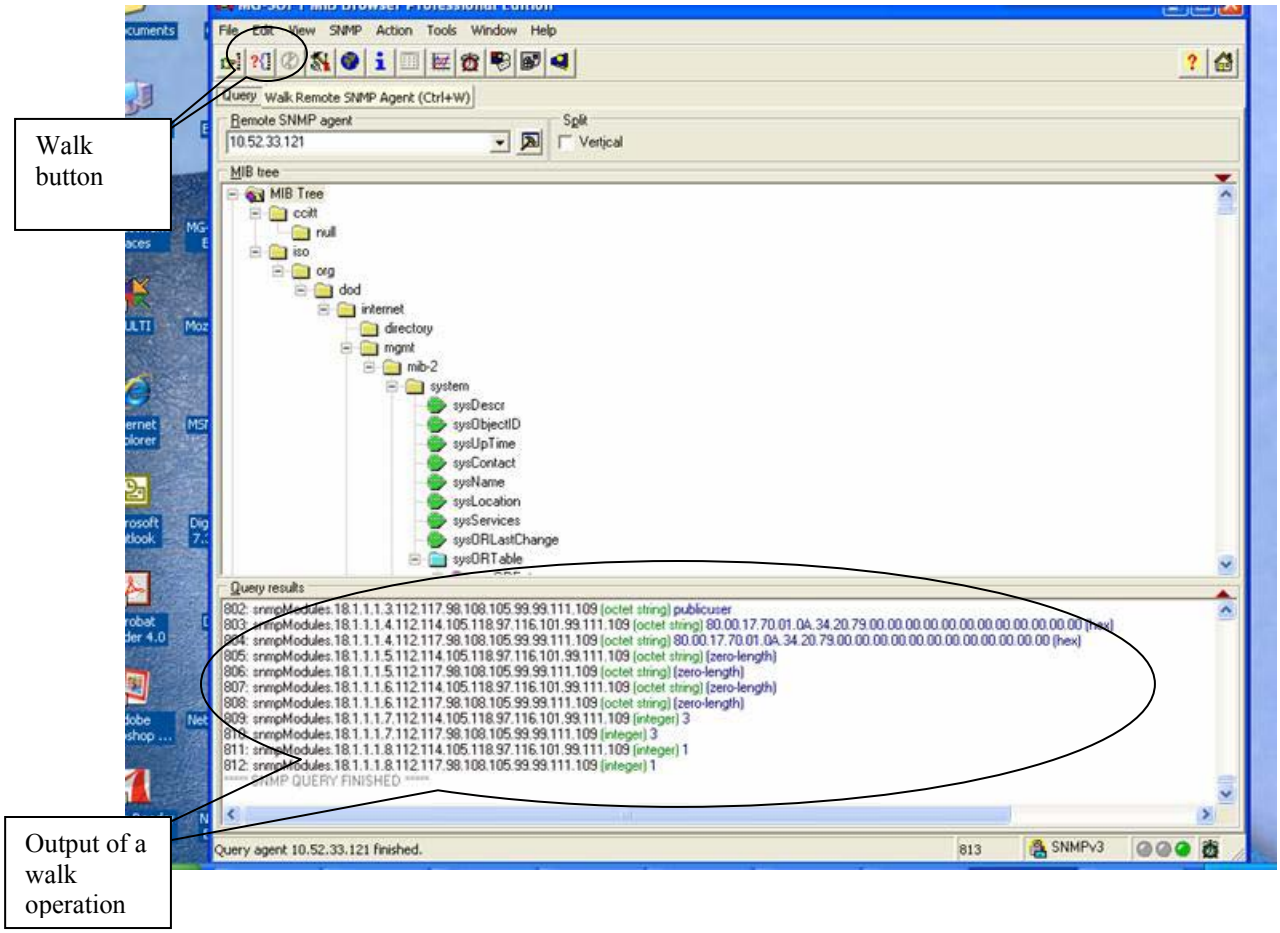
We clicked on the Edit User button. The Add User button functions the same except the fields in the new window are blank. We generally recommend keeping the User profile name and the security user name, the same. The default SNMP port number is 161. If you are using authentication, you'll need to select an authentication protocol and select an authentication password. If you are using privacy (encryption) you need to select an encryption protocol and a password. It goes without saying that for you to be able to successfully connect using authentication/encryption; your application in your Digi Device would have had to set up the user with those attributes. Please see Application Note: Enabling SNMPv3 Security in NET+OS V7.x if you are unfamiliar with setting up SNMPv3 security features and users in NET+OS applications.



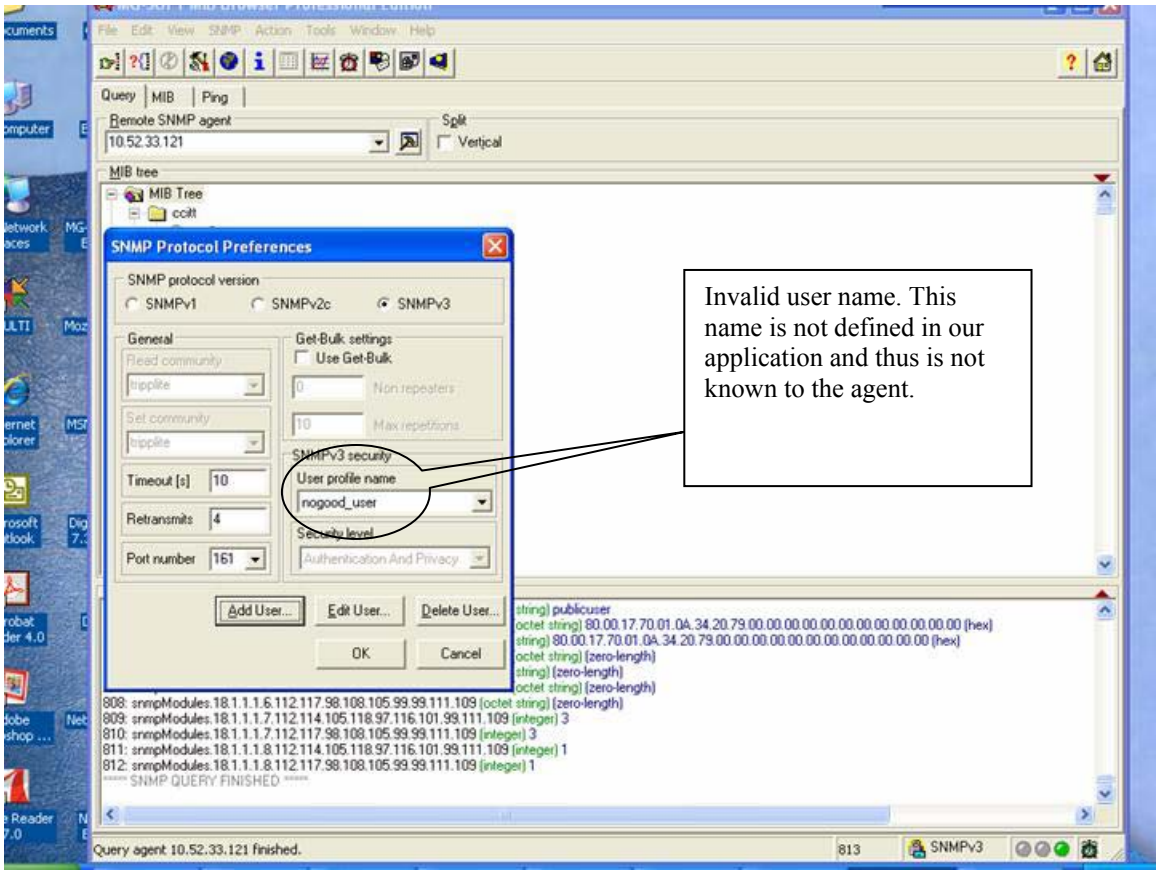
If your user has enabled authentication and/or privacy (encryption), you'll need to set up a password for them. By selecting the Change Password button on the SNMPv3 Security Parameters page you'll see the window displayed above in the lower right. Fill in and confirm the password. If you want to see the password, uncheck the Hide typing checkbox, otherwise your password, as you type, will be obscured. Click ok in this window and all prior windows to get back to the MIB browser.



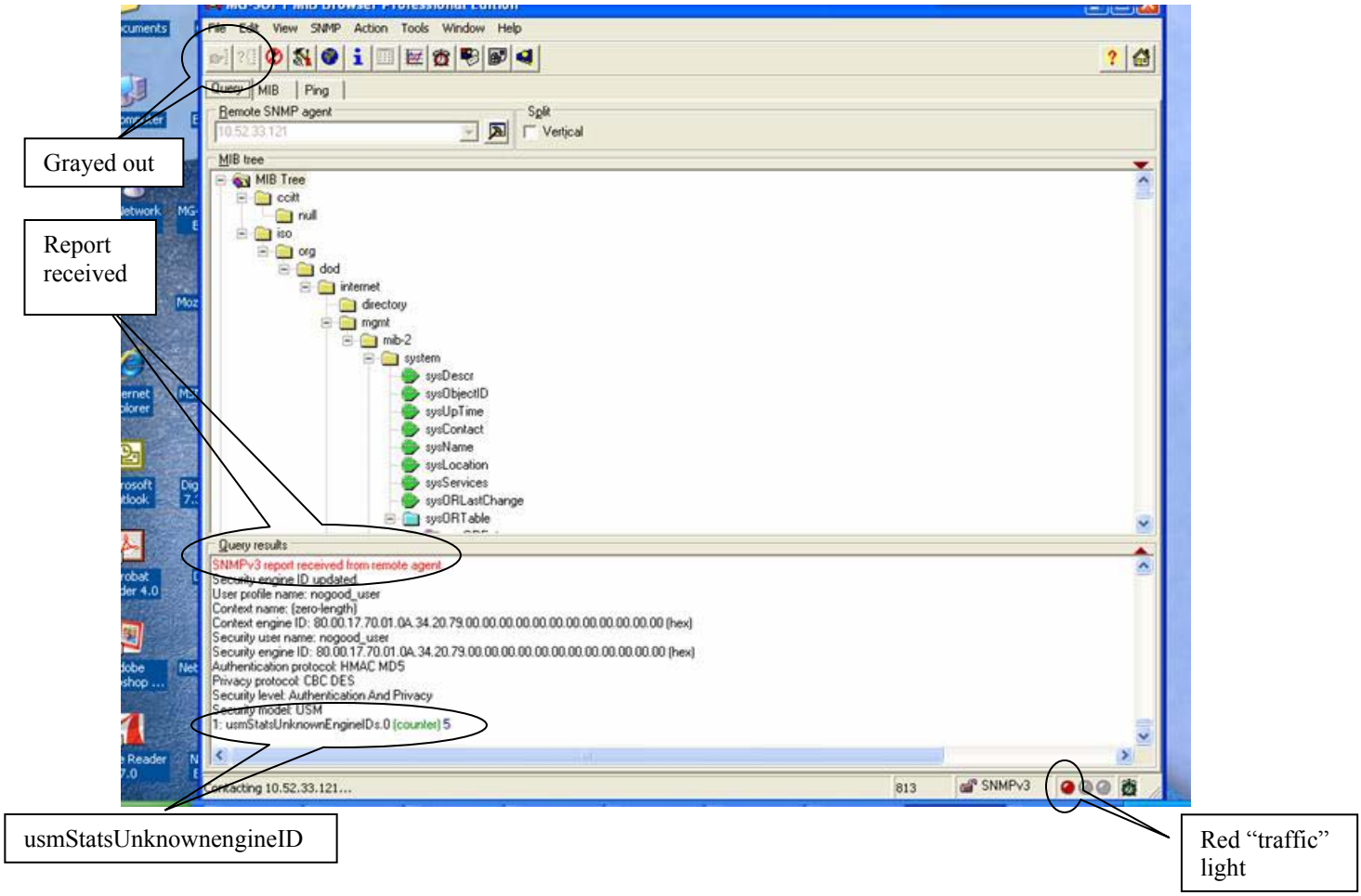
If you have the user, security protocols, passwords, et al correct, you will be able to successfully connect to your device, in SNMPv3 mode. Notice that at the bottom, we see the message that the remote SNMP agent was contacted. Also notice that the user profile name is listed and the first object of the MIB is displayed.



As with SNMPv1 and SNMPv2c, after successfully contacting your device, if your click the walk button, you'll walk the MIB starting from where your MIB browser is located, to the end.



In this screenshot, we are attempting to contact our SNMP agent (device) that we know is not a valid user to show the results.



We received a number of indicators showing that we did not successfully contact our SNMP agent. The contact and walk buttons are grayed out. The first object of the MIB is not shown. We got an usmStatsUnknownEnginID message/count. Also we got a report from the agent. Lastly, the "traffic" light at the bottom right of the SNMP MIB browser screen is red (left hand side light) instead of green (right hand side light).

7 Glossary

- Authentication

An act or action that establishes or confirms that something is true. In this case it is used in a login process. In this way a password (SNMP V1, V2c) or a user name and password are expected to enable an SNMP browser to access and SNMP agent.

- Encryption

A process used to render some information unreadable without the potential reader having access to some other secret information.

- MIB

Management Information Base. A database used in SNMP for the purpose of holding information used to manage some object (printer, router…etc).

- MIB Browser

A piece of software used to access the MIB in an object through that objects SNMP agent.

- MIB Tree

A structured method for displaying the information in an object's MIB. Usually displayed within the context of an SNMP browser.

- MG-Soft

A particular instance of an SNMP browser produced by MG-Soft of Maribor, Slovenia
http://www.mg-soft.si/

- NET+OS

An embedded operating system development environment developed and produced by Digi International.
http://www.digi.com/

- OID

Object identifier. An identifier used to name an object, in this instance an object in an SNMP MIB. Physically the OID is displayed as a successive set of integers, separated by periods. This set of integers describe a tree structure for apportion of a MIB.

- SNMP

Simple Network Management Protocol. A protocol that is a component of the internet suite of protocols as defined by the IETF. It is generally used for managing a device through an SNMP agent.

- SNMP Agent

A component of an SNMP implementation. Generally they represent a layer of software that sits between the tcp/ip stack and the SNMP MIB.

- SNMP V1

The original version of SNMP. The authentication object used in SNMP V1 was the community name.

- SNMP V2c

An update to SNMP V1. Among other things added conceptual tables but left authentication in the SNMP V1 model.

- SNMP V3

A newer version of SNMP that added real authentication and encryption to SNMP.