

SNMP Training Manual

Version 10.02

© 2009 ICONICS, Inc. All rights reserved worldwide. This document may not be reproduced or copied in any manner without written authorization from ICONICS, Inc.

The information contained within this document is subject to change without notice. ICONICS, Inc. does not guarantee the accuracy of the information.

GENESIS, GENESIS32, Pocket GENESIS, BizViz and their respective modules, OPC-To-The-Core, and Visualize Your Enterprise are trademarks of ICONICS, Inc.

Windows, Windows XP, Windows 2000, Windows 2003 Server, Windows NT, Windows XP-64, Windows 2003-64, Windows Vista, Windows Server 2008, and Windows CE are registered trademarks of Microsoft Corp. in the United States and other countries.

Other product and company names mentioned herein may be trademarks or registered trademarks of their respective owners.

Document Number: TM-SNMP-1002

ICONICS LICENSE AGREEMENT

YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS!

Opening and using the enclosed software for any purpose indicates your acceptance of the terms and conditions of this license agreement. If you do not agree with them you should return all software, documentation and copy protection keys within seven days of shipment unopened and your money will be refunded.

ICONICS provides this program and licenses its use in the United States, Puerto Rico, or internationally. You assume the responsibility for the selection of the program to achieve your intended results, and for the installation, use and results obtained from this program.

LICENSE

You are granted a personal license to use this program under the terms stated in this Agreement. You may: 1) Install and use the program on a single machine. 2) Make a single archival back-up copy of the program for the sole purpose of supporting your use of the single program on a single machine. 3) You may not use, copy, modify, or transfer the program, or transfer any copy, in whole or in part, except as expressly provided in this license, or with a written contractual agreement with **ICONICS**, Inc.

TERM

The license is effective until terminated. It will terminate if you fail to comply with any term or condition of this Agreement. You agree, upon such termination, to destroy the program and all copies that were made from it and to promptly return any copy protection key(s) to **ICONICS**.

LIMITED WARRANTY

ICONICS WARRANTS THE CD-ROM OR PHYSICAL DISKETTES, ON WHICH THE PROGRAM IS FURNISHED, AND PHYSICAL DOCUMENTATION TO BE FREE OF DEFECTS IN MATERIALS AND WORKMANSHIP UNDER NORMAL USE FOR A PERIOD OF NINETY (90) DAYS FROM THE DATE OF DELIVERY TO YOU AS EVIDENCED BY YOUR RECEIPT. THIS PROGRAM IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR, OR CORRECTION.

ICONICS SPECIFICALLY DISCLAIMS ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, IMPLIED WARRANTIES OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN PARTICULAR, WITH RESPECT TO ANY PARTICULAR APPLICATION, USE OR PURPOSE, IN NO EVENT SHALL **ICONICS** INC. BE LIABLE FOR ANY OTHER COMMERCIAL DAMAGE, INCLUDING BUT NOT LIMITED TO SPECIAL, INCIDENTAL, CONSEQUENTIAL OR OTHER DAMAGES. **ICONICS** DOES NOT WARRANT THAT THE FUNCTIONS CONTAINED IN THE PROGRAM WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE PROGRAM WILL BE UNINTERRUPTED OR ERROR FREE.

LIMITATION OF REMEDIES

ICONICS' entire liability and your exclusive remedy shall be the replacement of any CD-ROM or diskette not meeting **ICONICS'** "Limited Warranty" which is returned to **ICONICS** with a copy of your receipt within the warranty period. The remedy for breach of this warranty shall be limited to replacement and shall not encompass any other damages including but not limited to loss of profit, special, incidental, consequential, or other similar claims arising out of the use or inability to use such program even if **ICONICS** has been advised of the possibility of such damages, or for any claim by any other third party.

GENERAL

This Agreement will be governed by the laws of the Commonwealth of Massachusetts. Should you have any questions concerning this Agreement, you may contact **ICONICS** in writing at:

ICONICS, Inc.
100 Foxborough Boulevard
Foxborough, MA 02035

You acknowledge that you have read this agreement, understand it and agree to be bound by its terms and conditions. You further agree that it is the complete and exclusive statement of the Agreement between you and **ICONICS** which supersedes any proposal or prior Agreement, oral or written, and any other communications between you and **ICONICS** relating to the subject matter of the Agreement.

ICONICS RETURN POLICY

All sales are final (NO RETURNS) unless one of the following conditions is applicable: Program is returned in its original packaging material within 7 days after shipment. In such a case, a full refund is provided, less all incurred shipping and handling costs. Program is returned within 30 days from the original shipment date. In such a case a 20% restocking fee is applicable. No returns are allowed on OPC ToolWorX or ActiveX ToolWorX.

Contents

1. Simple Network Management Protocol

1.1	OBJECTIVES	1-1
1.2	INTRODUCTIONS.....	1-1
1.3	SNMP BASIC COMMANDS.....	1-2
1.4	MANAGEMENT INFORMATION BASE (MIB).....	1-3
1.5	SNMP CONFIGURATION.....	1-5
1.6	TRANSLATION	1-9
1.7	SNMP DATA IN A PROCESS POINT	1-10
1.8	SNMP SERVICE	1-11
	LAB: MACHINE SNMP DATA	L1-1
	REVIEW: SNMP REVIEW	R1-1
	A. Glossary.....	A-1
	B. Answers	B-1

Simple Network Management Protocol 1

1.1 Objectives

After completing this chapter, you should know how to:

- Setup the SNMP configuration
- Assign an SNMP tag as the Data Source for a process
- Make use of a MIB files
- How to setup SNMP service

1.2 Introductions

SNMP, which stands for Simple Network Management Protocol, is part of the Internet Engineering Task Force (IETF) internet protocol suite. SNMP allows devices to expose useful information to other devices and systems, and in some instances allows this information to be managed and altered. The breadth of information available using SNMP can include: a CPU fan speed, the routing table to be used on a router, the number of pages a printer has printed, and many others depending on the device. Almost every network device that can be managed responds to SNMP requests; the SNMP protocol allows for browsing, auto-discovery, and mapping of devices.

The SNMP system is comprised of an Application Layer Protocol implemented in network software, a database schema, and discoverable data objects. The three key components contain:

- **Managed Devices:** a managed device is a device on the network that has a built in SNMP agent, like routers, switches and bridges. Managed devices collect and store management information, which is made available to Network Management Systems (NMS) such as Genesis64.
- **Agents:** an agent is a small network-management software module that resides in a managed device that collects and stores information. An agent

has local knowledge of management information and translates that information into a form compatible with SNMP.

- **Network Management Systems (NMSs):** an NMS executes applications that monitor and control managed devices. NMSs provide the bulk of the processing and memory resources required for network management. One or more NMSs must exist on any managed network.

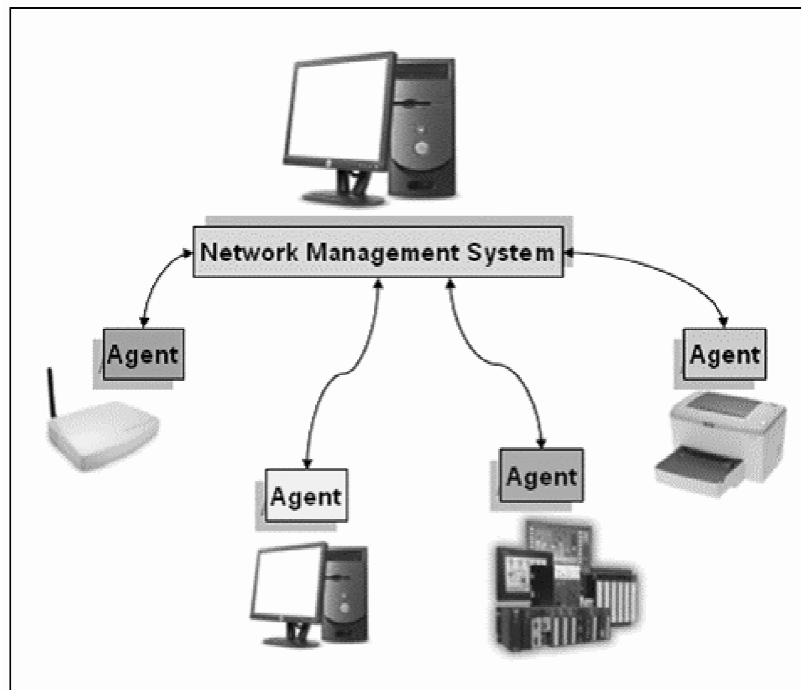


Figure 1.1 - Elements of a Network Management System in SNMP

1.3 SNMP Basic Commands

NMS retrieves information through queries that use the GET, GETNEXT, and GETBULK* commands. The local device agent can also broadcast data using TRAP* or INFORM* operations, which is intercepted by systems that have an SNMP Trap Service running on them. Changes are made to variables using SET commands.

The four basic SNMP operations are read, write, trap, and traversal operations:

- **READ (GET):** The READ command is used by an NMS to monitor managed devices. The NMS examines different variables that are maintained by managed devices.

- **WRITE (SET):** The WRITE command is used by an NMS to control managed devices. The NMS changes the values of variables stored within managed devices.
- **TRAP:** The TRAP command is used by managed devices to asynchronously report events to the NMS. When certain types of events occur, a managed device sends a trap to the NMS.
- **INFORM:** Traversal operations are used by the NMS to determine which variables the managed device supports and to sequentially gather information in variable tables, such as a routing table.

NOTE: Operations marked by asterisk (*) are not supported in current version of GENESIS64

1.4 Management Information Base (MIB)

SNMP does not tell vendors which variables their devices should store; instead, it provides a standard way to translate data into meaningful information stored in the object's template. A Management Information Base (MIB) is used to define a hierarchical namespace with an organized collection of managed objects collected in a virtual information store. SNMP defines a standard hierarchy in a tree structure; the equipment or software vendor determines which objects are stored on its devices.

When SNMP explores a device, the device's hierarchy of objects is returned and displayed in the NMS using object identifiers (OIDs) formatted in a notation defined by ASN.1 (Abstract Syntax Notation One). You can traverse the SNMP tree to **iso.org.dod.internet.mgmt.mib-2.system.sysDescr** where the **sysDescr** variable stores the system description as a number (from the device) that might take the format: **1.3.6.1.2.1.1.1**. The data stored at the device is terse in order to lower the overhead in the system at the device level. Each data object has a unique number. For example, a Cisco router has a different number pattern than an HP printer.

Each device that SNMP monitors has its own hierarchy that is based on the MIB standard. The MIB represents all the data that a device can expose through SNMP. For example, in the MIB of a printer there is: the toner level, the text that displays on the screen, the number of pages printed, and other information that the vendor defines. Each of these pieces of information has its own OID.

In order to make sense of the data stored in OIDs, the device is mapped to a translation table called a MIB file. A MIB file takes the numeric values defined

by SNMP at the devices and translates them from dot format into readable descriptions and attributes from a template. In the example above, the **sysDescr** value is matched to the text string:

A textual description of the entity. This value should include the full name and version identification of the system's hardware type, software operating-system, and networking software. It is mandatory that this only contain printable ASCII characters.

The text is READ-only indicated by a setting on the template.

The standard OIDs are shown in Figure 1.2. Standard OIDs must be the same on all the devices that use the SNMP protocol, and they must have the same organizational structure. ISO maintains the vendor-specific entries for the MIB files. Each vendor implements its own MIB object on each device; for this reason, each device must have the correct MIB files so that non-standard information can be translated.

Two types of managed objects exist: scalar and tabular. Scalar objects define a single object instance. Tabular objects define multiple related object instances that are grouped in MIB tables. SysDescr, for example, is a scalar object.

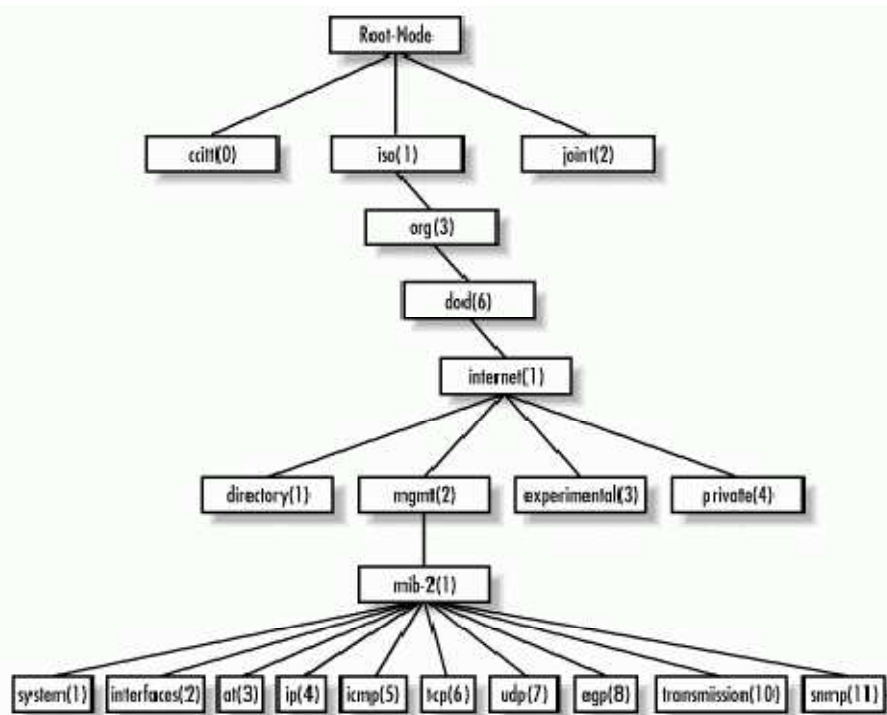


Figure 1.2 - The Root Structure of a Standard MIB Tree

NOTE: Tabular SNMP objects are not supported in current version of GENESIS64

1.5 SNMP Configuration

When you install GENESIS64, you install an SNMP service that you configure by using the SNMP Configurator in the Workbench application. Using the SNMP Configurator, you can explore devices in the SNMP namespace, starting at the network address you specify and browsing any device that is available to that server in its network neighborhood. You can use the SNMP Configurator to manage the network (through SNMP), perform Supervisory Control and Data Acquisition (SCADA through OPC), and even access PLC controls over Ethernet, as shown in Figure 1.3 below.

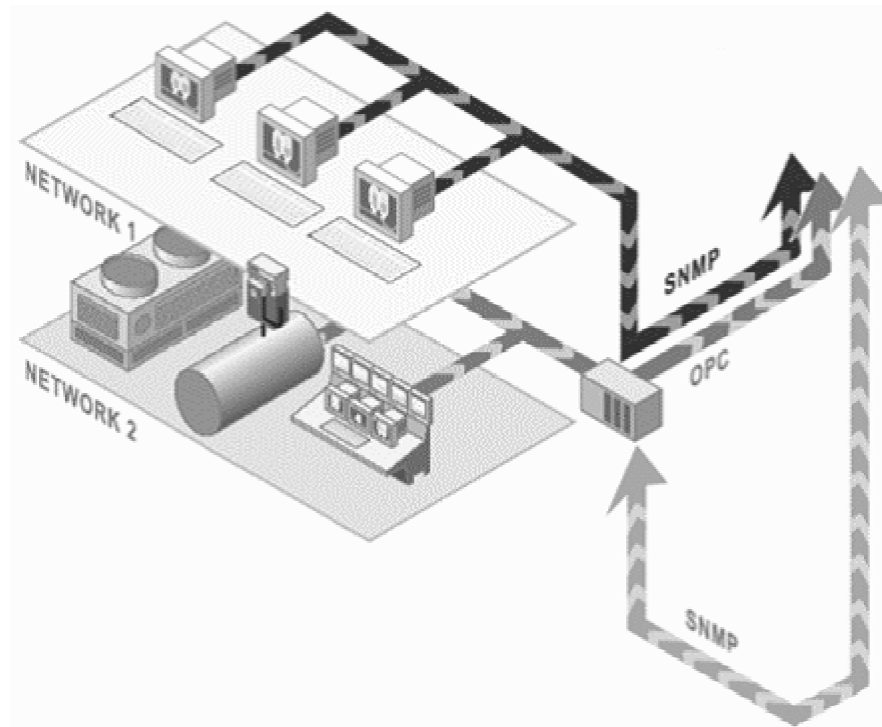


Figure 1.3 - Network Management Using SNMP Service

In the Workbench, you can open the SNMP Configurator by clicking on the SNMP  button. When the SNMP database is Active, two nodes are visible in the Project Explorer:

- One for SNMP devices, which display SNMP tags that you select
- One for the MIB files that provide device translation, which is essentially a dictionary function

If you double-click on the SNMP node, the Network Explorer appears, as shown in Figure 1.4. The Network Explorer allows you to perform the discovery

operation that lets you select from devices that respond to PINGs and return SNMP data.

Figure 1.4 - The Network Explorer Configuration Form

The Network Explorer's **Discovery Settings** allow you to search a subnet, a single address, or a range of addresses for discoverable devices. In addition to timeouts and port settings in the **SNMP Data** section, notice that the **Read Community** setting is set to **public**; **public** is essentially a password setting that provides access to devices set to this type. GENESIS64 supports SNMP versions 1 and 2 (version 3 is not supported). You can use DNS in your discovery in order to resolve computer names.

When you click on the **Explore** button in the Network Explorer configuration form, you open the SNMP Explorer dialog box where you can browse for SNMP devices. In Figure 1.5, the Network Explorer found two devices: 192.168.2.146, a computer; and 192.168.2.94, which is a network switch.

You can explore the information stored in every device by expanding the device tree. It may seem like every device tree is the same as the MIB items tree loaded before, but unlike the MIB items tree, in the device tree we also have real-time information coming from the device. While the MIB items tree organizes the data, the device itself provides the data.

When you expand the SNMP device tree you can drill down to the attributes you want to monitor, and you can add the tags to your display by double-clicking on each one. In Figure 1.5, three tags were chosen: one for the sysDescr, another for

sysUpTime, and the third for the sysName. If you hold the mouse cursor over an attribute, you will see a text description of what the attribute stores.

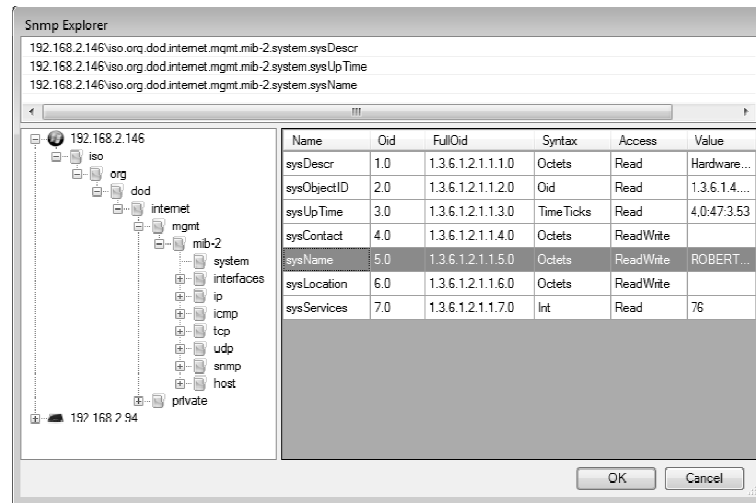


Figure 1.5 - The Network Explorer with Three Selected Tags

Once you select your tags and close the Network Explorer, you may be prompted to refresh the SNMP tree, which will provide the operation necessary to bring the correct MIB file into the Project Explorer. The added tags appear under the node for the device you just added.

If you double-click the Device node, you will see the Device configuration form, as shown in Figure 1.6. The Device form displays attributes such as the Read and Write communities, Polling rate, Device data that can be parameterized, etc.

Device
Name: 192.168.2.146

Read Community: public
Write Community: private
Receive Traps: Disabled Getbulk Count: 30

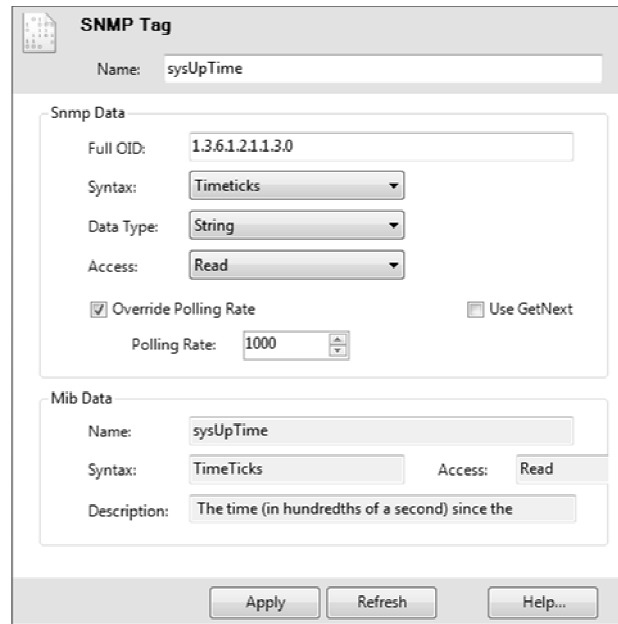
Timing
Polling Rate: 10000
Timeout: 1000
Retry Count: 3

Device Data
Parameters: None Device Type: Printer
Host: 192.168.2.146
Port: 161

Snmp Explorer - Add tags directly in this device
☐ Cache Mib ☐ Rebuild Mib Tree

Figure 1.6 - The Device Form

If you double-click on the tag name in the Project Explorer, you expose the SNMP Tag configuration form. An example for the sysUpTime is shown in Figure 1.7. This form exposes the OID, the various properties of the tag, and the matching MIB description of what the tag data exposes. It does not expose the actual value of the tag, which in this case would be a readable and writeable string. To display the tag you can assign a process point to use the tag as a data source.



The figure shows a window titled "SNMP Tag" with a tabbed interface. The "Snm Data" tab is active, showing the following fields: "Name" (sysUpTime), "Full OID" (1.3.6.1.2.1.1.3.0), "Syntax" (TimeTicks), "Data Type" (String), "Access" (Read), "Override Polling Rate" (checked), "Polling Rate" (1000), and "Use GetNext" (unchecked). The "Mib Data" tab is also visible, showing "Name" (sysUpTime), "Syntax" (TimeTicks), "Access" (Read), and "Description" (The time (in hundredths of a second) since the). At the bottom are "Apply", "Refresh", and "Help..." buttons.

Figure 1.7 - SNMP Tag Configuration Form

There are a couple of settings to take note of here. First, the Polling Rate determines how often the data refreshes at runtime. The default polling rate is 1000 milliseconds. When you check the Override Polling Rate option, it enforces clients, such as GraphWorX64, to use the specified polling rate instead of the one selected in the GraphWorX64 process point.

Also, note that each of the three tags appears alone under the device node (192.168.2.146) in the SNMP tree as shown in Figure 1.6. If you would like to reorganize your tags, you can create a folder structure and organize your selected SNMP tags as you wish.

You can create a new folder by right-clicking on the parent item (the device node, or folder) to which you want to create a folder under and select the Add Folder option in the right-click menu that comes up. This opens the SNMP Folder for on the right-hand side. You can type in the name of the folder and click on the Apply button to save the settings. From here, you can right-click on the folder, and select Add Tag to add your SNMP tags.

If you would like to import a tag into the form of the MIB tree with the folder hierarchy showing, you can go to the Device configuration form. In the form, check on the **Rebuild Mib Tree** option in the Snmp Explorer – Add tags directly in this device section at the bottom of the form and then click on the **Explore** button to open the SNMP Explorer. From here, you can navigate to the desired tag to add and click on the OK button when you are done. When it prompts you to refresh the tree, click on Yes to let it update.

Figure 1.8 shows the result, with the updated MIB tree in the device node. As you can see, you can add a tag to the device node multiple times. Sometimes you may want to see the tree, and other times you may want to use your own folder structure.

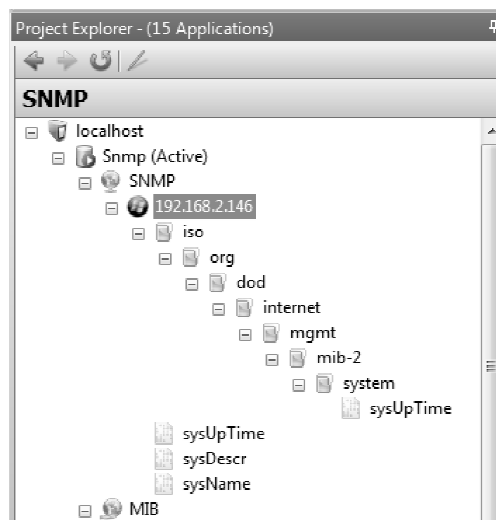


Figure 1.8 - An SNMP Tag with Its Associated MIB tree

1.6 Translation

The Device tree is the instantiation of the MIB items tree. When you browse to a device that responds by returning SNMP data, the first few numbers of the address identify the manufacturer of the device, and the device type. Additional parts of the data provide the type of attribute that is described and data values. Devices do not implement all of the possible SNMP tags that a vendor has in their MIB tree, nor do they have to. Stored within the device and communicated with the data that is returned are the leaves of the MIB tree that are populated by the device. Those leaves appear in the device node when you select specific tags.

If you were to browse the MIB node to the following location: MIB\ISO\ORG\DOD\INTERNET\PRIVATE, you would see that many popular

manufacturers' MIB files appear in the list. Most of these nodes are empty, with the exception of the top-level assignments. As you select devices, you populate the nodes with the leaves supported by the devices.

The ICONICS node, which appears near the bottom of the PRIVATE folder is of interest because it contains a number of SNMP simulator functions that you can use to test the validity of your displays. Figure 1.9 shows the highlighted ICONICS branch of the MIB tree. It contains simulators for devices, signals, traps, and more.

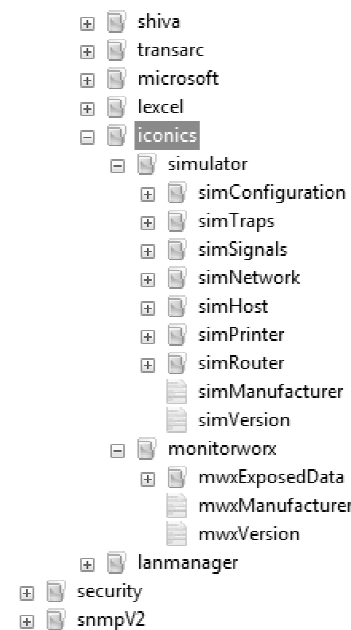


Figure 1.9 - The ICONICS leaf of the MIB tree

NOTE: SNMP simulator is not available in current version of GENESIS64. The MIB record provides you OID translation if you connect to existing GENESIS32 installation.

1.7 SNMP Data in a Process Point

Assigning SNMP data to a GraphWorX64 process point is no different than connecting any other data source. The example below illustrates the placement of the sysUpTime variable to a process point in configuration mode and its display in runtime.

To connect a process point to an SNMP data source, you should first open a GraphWorX64 display and click on the Dynamics tab of the ribbon. In the Text Objects section, select the Process Point button and then click on the design surface to place the process point on to the display.

The Data Browser should now come up for you to select the data source. Navigate to OPC Servers → My Server → SNMP. All of your configured SNMP devices should display on the right-hand side. Double-click on the device desired and then on the SNMP tag of interest. Figure 1.10 illustrates the SysUpTime tag in the Data Browser.

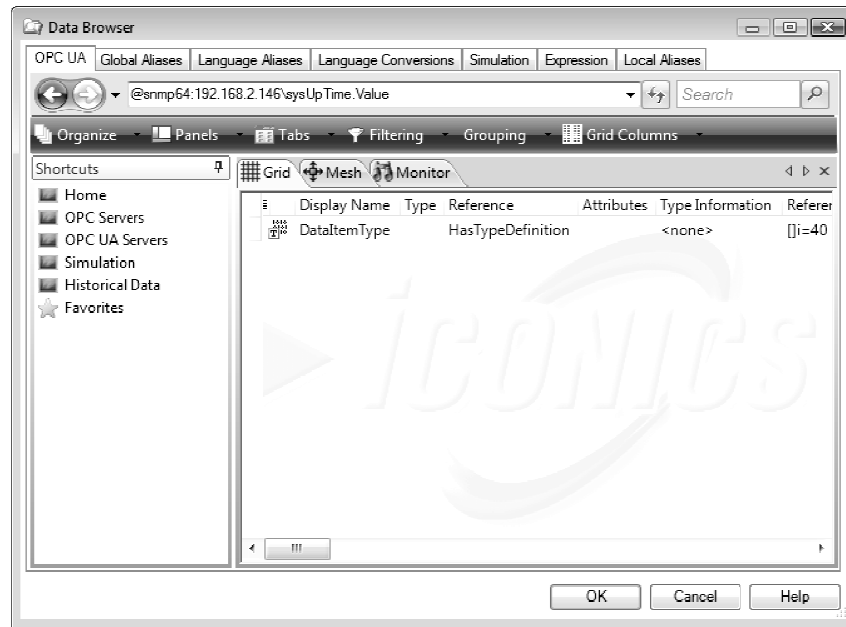


Figure 1.10 - Selecting the SysUpTime SNMP Tag in the Data Browser

Click on OK to select the tag and close the Data Browser. When you switch the GraphWorX64 display into runtime, you will see the SNMP data with values refreshing at the rate of the polling rate that you set. To change the SNMP tag, edit the DataSource property of the process point.

1.8 SNMP Service

Microsoft provides an **SNMP Service** on Windows Operating system (XP and later versions). This service enables SNMP messages and is the sending service. In order to use this service, you should first make sure that it is installed. If the service is installed, you should see the SNMP service in the services manager. If you do not see it in the services manager, you can add the service by going to the Control Panel → Programs and Features window, and click on the Turn Windows Features on or off link. Depending on your operating system, what you will see next will be different. Regardless of the operating system, in the end, you want to make sure that in the features list, you place a checkmark next to the SNMP

feature or SNMP Server option. You should do this for every machine you expect to provide you with SNMP data.

Once you have installed the service, you should check in the service manager to make sure that the service is turned ON properly. In the services manager, bring up the properties of the SNMP Service. On the **Security** tab of the service properties, shown in Figure 1.11, set the community allowed to request SNMP data from this SNMP host and list the SNMP hosts and SNMP management systems that can send SNMP requests to this SNMP host. For demonstrations purposes, you can set the community to *public* and then allow incoming packets from either any host or the hosts you specify.

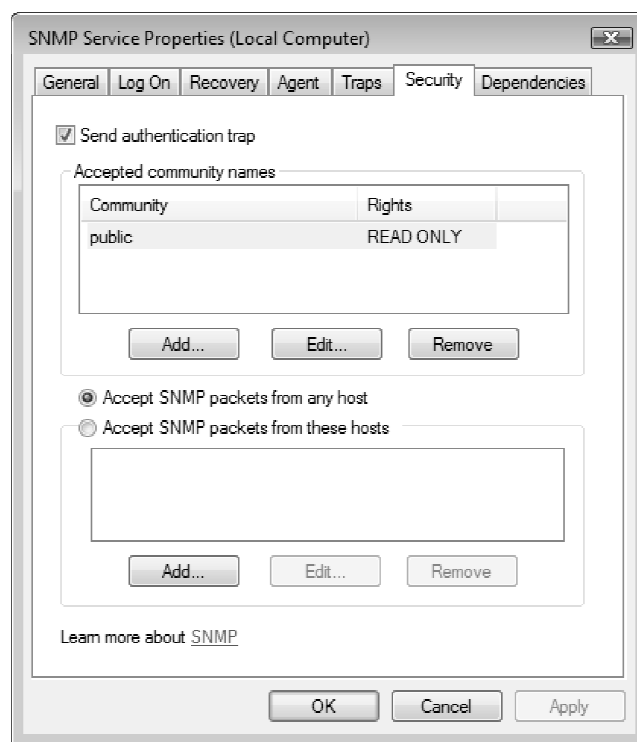


Figure 1.11 - The Security tab of the SNMP Service

Lab: Machine SNMP Data

1

1.1 Lab Overview

icTonics would like to take advantage of SNMP to monitor the computers that they are using to run their plants. This will allow them to see immediately if the monitoring computers are malfunctioning. In this section, we will setup the Windows SNMP Service to allow icTonics to monitor their computer status. Furthermore, we will create a display for them to show the SNMP data.

Estimated time to complete this lab: 20 minutes

1.1.1 Task Checklist

In this lab, you will complete the following tasks:

- Create a configuration database for SNMP configuration
- Check whether your SNMP service is running and properly configured in order to access your local SNMP objects
- Discover the network neighborhood
- Create SNMP tag out of SNMP object
- Connect to your new SNMP tag via GraphWorX64

1.1.2 Support Files

You do not need any support files to complete this lab.

1.2 SNMP Service

Before we can monitor the machine status, we must turn on and configure the SNMP service. This will allow us to monitor SNMP objects on the local machine.

1. Bring up the Services Manager. You can do this through the Administrative Tools menu or use the Task Manager's Services tab.
2. Find the **SNMP Service** in the list and open its **Properties** window by double-clicking on it.



Figure L1.1 - SNMP Service

3. Select the Security tab in the SNMP Service Properties window.
4. Click on the **Add** button in the Accepted Community names. In the SNMP Service Configuration window, select READ ONLY for the Community rights and type in **public** for the community name.

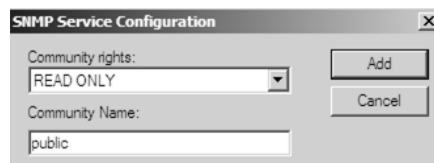


Figure L1.2 - SNMP Service Configuration

5. Click on **Add** when you are done. Select the option to Accept SNMP packets from any host. Your security tab should look similar to Figure L1.3.

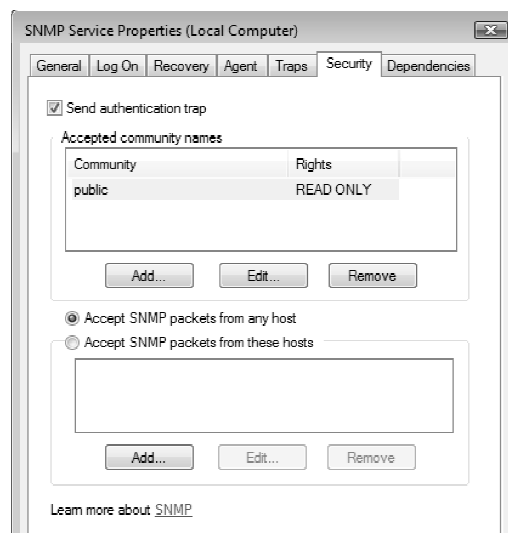


Figure L1.3 - The Security Tab of the SNMP Service

6. Click on **OK** and **Start** the SNMP service when you are done configuring. You should see Started in the Status column of the Services Manager.

1.3 SNMP Configuration

First, you need to open SNMP configuration interface in order to configure your SNMP tags. We will also add SNMP tags to our new configuration database.

1. Open Workbench by going to **Start → Programs → ICONICS GENESIS64 → Workbench**.
2. Select the **SNMP**  **button** in the toolbar to open the configuration interface.
3. In the Project Explorer on the left pane, right-click on the **localhost** and select **New Database...**

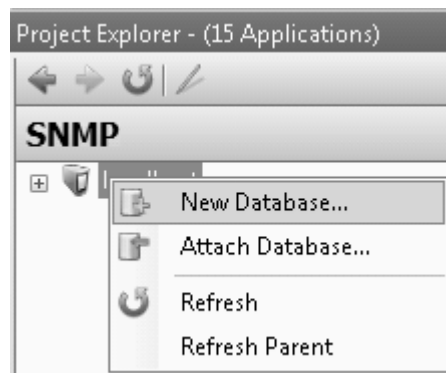


Figure L1.4 - Create New Database

4. Follow the **SNMP – SQL Create Database Wizard**, which opens, and create a new database called *My Database* in the default SQL server without changing any of the predefined settings. When you finish the process, you should have two databases in the Project Explorer.

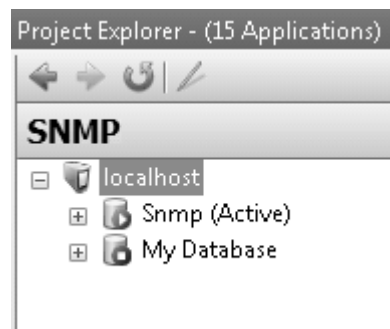


Figure L1.5 - My Database Created

5. Notice the different symbols over the two databases. The green play like symbol means that the database is currently read by the SNMP service as the source of configuration. Make your new configuration active by right-clicking on the database and selecting **Make Active**.
6. Expand **My Database** tree and double click on **SNMP** item. The Network Explorer will open in the right pane similarly to Figure L1.6.

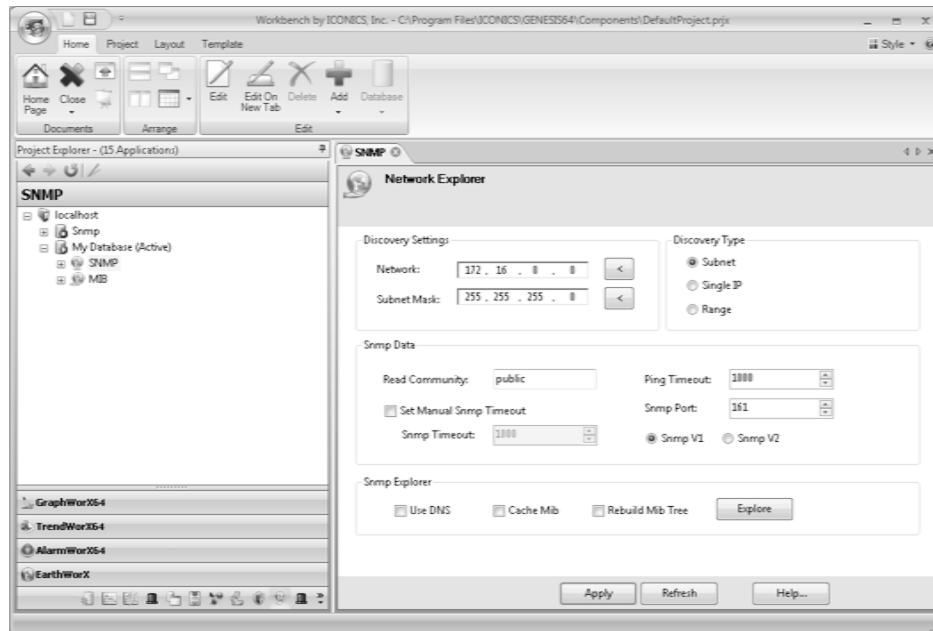


Figure L1.6 - Network Explorer Setting

7. If you know the IP address of your machine you may put it in the Network field and click on the **Explore** button. If you do not know, you should first change the Discovery type to Single IP and set the IP address to 127.0.0.1, which is localhost.
8. The Explore button will open the SNMP Explorer, where you can browse all accessible SNMP objects within the range you specified in Network Explorer setting. We will select our machine's IP address and drill down to **iso** → **org** → **dod** → **internet** → **mgmt** → **mib-2** → **system** to see the SNMP objects exposed by our system as shown in Figure L1.7.

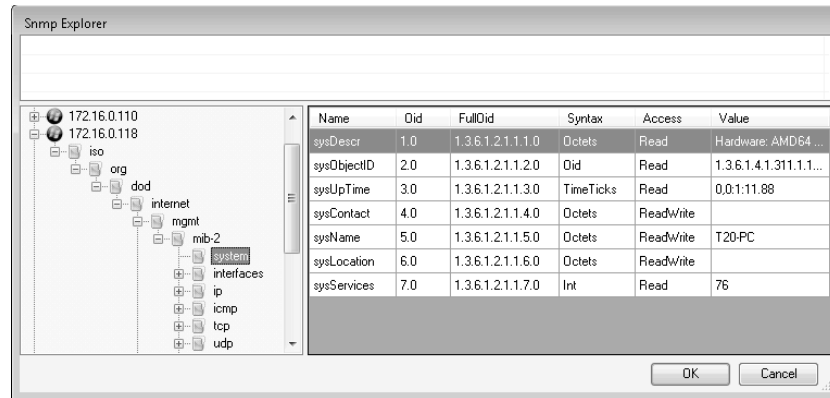


Figure L1.7 - SNMP Objects Exposed by the System in SNMP Explorer

9. **Select** all of the objects by holding down the Shift or Control Key and right-click to select the **Add** option.
10. Once you see all of the tags entered in the upper part of the SNMP Explorer, click on **OK** to add the tags and close the explorer.
11. You will be prompted to refresh the tree because of database change. Select **Yes** to continue.
12. You should now see all your new SNMP tags under SNMP and the name of your node in the Project Explorer.

1.4 SNMP tags in GraphWorX64

When you have configured your SNMP tags, you can access them from ICONICS applications.

1. Open a **GraphWorX64 display** and apply the icTonics template to the display.
2. Save the display as "icTonicsMachineStatistics".
3. Click on the Dynamics tab of the ribbon and select the **Process Point** button in the Text Objects section. Click on the design surface to place the process point. The **Data Browser** appears.
4. Navigate to the following node in the Data Browser by going to **OPC Servers** → **My Server** → **SNMP** → **Your Node**.

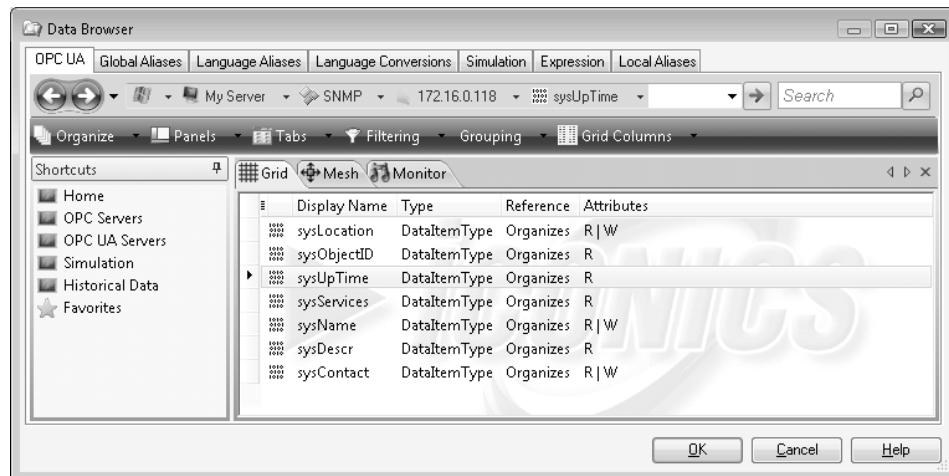


Figure L1.8 - Select SNMP Tag

5. Select the sysName tag and click on **OK**. You should be back in the display now. You may want to resize the process point
6. Add a text label to the left of the process point and type in the text “Machine Name:”
7. Repeat steps 3-6 to add other information. Your display should look like Figure L1.9 when you are done.



Machine Name: ICOTRaining

System has been running for: 1,2:3:17.3

System is running: 76 Services

System description:

Hardware: AMD64 Family 15 Model 75 Stepping 2 AT/AT
COMPATIBLE - Software: Windows Version 6.0 (Build 6001
Multiprocessor Free)

Figure L1.9 - Finished Display in Runtime

8. When you switch the GraphWorX64 display into **runtime**, you will see the SNMP data.

SNMP Review

R1

1.1 Objectives Review

After completing this chapter, you should know how to:

- Setup the SNMP configuration
- Assign an SNMP tag as the Data Source for a process
- Make use of a MIB files
- How to setup SNMP service

1.2 Summary

SNMP (Simple Network Management Protocol) is a system of network broadcasts that provides information on devices and systems. SNMP is an Application Layer Protocol that is comprised of a network management system (NMSs), a database scheme that maps the SNMP data to vendor information, and discoverable data objects with local agents such as systems, routers, disks in storage devices, and many other entities.

The SNMP data from a device comes in a standard form that is created by a vendor as part of a MIB (Management Information Base). SNMP defines a standard hierarchy and it is up to the vendor to implement the data that is exposed on the objects stored on the device. Each device has an object identifier (OID) that uniquely maps to each entry in a specific vendor's MIB.

You can assign SNMP data to process points in GraphWorX64. In order to do this, you must first use the Network Explorer utility to select the SNMP objects that you are interested in from the Device node of the SNMP service. Those tags are then available for assignment to the DataSource property through the Data Browser.

1.3 Terms

Agent	Managed Device	MIB
NMS	OID	Network Explorer
SNMP	Trap	

1.4 Test Your Knowledge

In this chapter, we described how to configure SNMP and display that data in a GraphWorX64 display. You should be able to answer the questions below.

1. Which of the following is *not* an SNMP command?
 - a. TRAP
 - b. READ
 - c. WRITE
 - d. UPDATE
2. When you add an SNMP tag to the Device node in the SNMP configurator, how do you show the position in the MIB file that the tag occupies?
 - a. Use the Device checkbox on the Rebuild form and refresh the view after you select the tag.
 - b. Use the Rebuild MIB Tree checkbox on the Device form and refresh the view after you select the tag.
 - c. Click the MIB button in the Navigation tree.
 - d. None of the above.
3. True or False: You can connect to SNMP tags from other ICONICS applications?
4. For what can you use SNMP?
 - a. Managing the network
 - b. Performing Supervisory Control and Data Acquisition (SCADA through OPC)
 - c. Accessing PLC controls over Ethernet
 - d. All of the above
5. True or False: SNMP Service have to be running to receive SNMP data from other machines?

Glossary

Agent is a small network-management software module that resides in a *Managed Device* that collects and stores information.

Managed Device is a device that responds to SNMP requests and stores data in an *SNMP MIB* format.

MIB stands for Management Information Base, which is a standard schema for organizing SNMP data. Each vendor implements its own MIB.

NMS stands for Network Management System, which is a software that can browse the network for SNMP devices, view SNMP data, and change device parameters using SNMP commands.

Network Explorer is an SNMP browser utility that defines the data being exposed; it is sent by a managed device to an *NMS*.

OID stands for Object Identifier, which is a unique code that defines the SNMP data being exposed. It is sent by a managed device to an *NMS*.

SNMP stands for Simple Network Management Protocol, which is a protocol for viewing and managing device information.

Trap is an alarm or message that is sent by a device via SNMP messages.

Answers

Questions	1	2	3	4	5	6	7	8	9	10
Chapters										
Chapter 1	D	B	True	D	False					

iconics

OPC Automation at your fingertips

100 Foxborough Blvd., Foxborough, MA 02035
508.543.8600 • FAX 508.543.1503 • BBS 508.543.3881
www.iconics.com • E-mail info@iconics.com

© 2009 ICONICS, Inc. All Rights Reserved.
Specifications subject to change without notice.