

Description: Guide to apply SNMP in a segmented network environment.

OS Requirement: Win 2000, XP Pro, Server 2003, Vista, Server 2008, Windows 7

General Requirement: SNMP device/computer with SNMP service enabled

Introduction

SNMP stands for Simple Network Management Protocol and is a simple protocol that allows devices to expose useful information to other devices. This information can be the CPU fan speed of a computer or the routing table of a router or temperature from a sensor. Almost every network device answers to SNMP requests. SNMP gives Network Managers access to information from nearly every device connected to the Network.

Simple Network Management Protocol (SNMP) is a communication standard that facilitates the exchange of network information between SNMP enabled devices. An SNMP network consists of a Network Management System (NMS), Managed Devices, and Agents. An NMS would monitor or control managed devices that provide SNMP information through the agents.

The SNMP Protocol is based on the communication between an Agent and a Manager.

The **Agent** is software installed on a device (a router, a printer a PC, etc) and it simply answers to the messages of the Manager. These messages can be

- Read – manager wants to retrieve data
- Write – manager wants to set data
- Traps – alarms (e.g. "the CPU Temperature is high!")

The **Manager** is software (for example the ICONICS SNMP Connector) that collects data from the devices, organizes it and provides it to users/clients.

Here is how SNMP works with GENESIS32. You can consider ICONICS GENESIS32 V9 as an NMS. The Managed Devices are your routers, printers, servers, etc. The Agents are software which resides in the managed devices that provide management information.

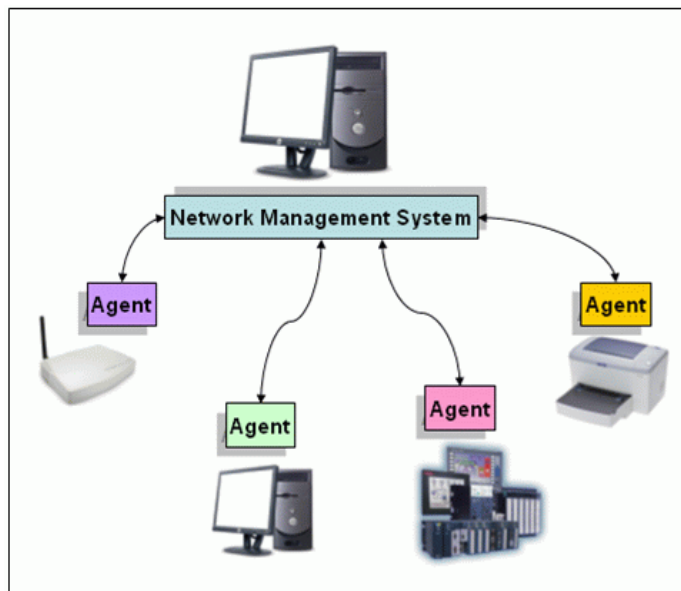


Figure 1 - Network Management System

SNMP Supports Segmented Network Environment

In Genesis32 9.20 version, an enhanced function for SNMP application has been implemented which supports segmented network for device explore. To do this, follow the below steps:

1. Launch SNMP Configurator from Programs → ICONICS Tools, right click SNMP and select new → network. A new network container is created for device searching.

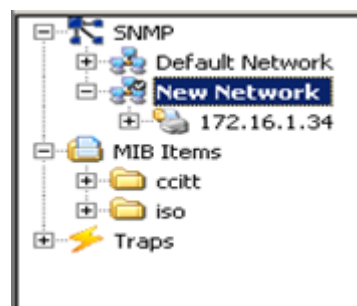


Figure 2 - Network Container

2. On the right side of the screen, an interface for segmented network explore is shown for the configuration as you can see from Figure 3. Here you can pick up a single IP, or some ranges of IP addresses, or a subnet you can setup with Network address and Subnet Mask. Discovery is a very powerful SNMP tool that allows you to search for SNMP devices and import their tags in the database.

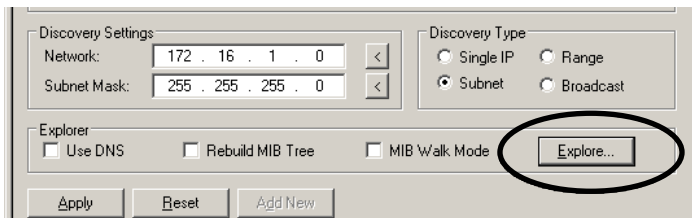


Figure 3 - Segment Network Setup

3. Click Explore button to let SNMP exploring segmented network you setup in step 2. The Unified Data Browser pops up with any device information that response to the request from ICONICS SNMP connector. See figure 4 as an example.

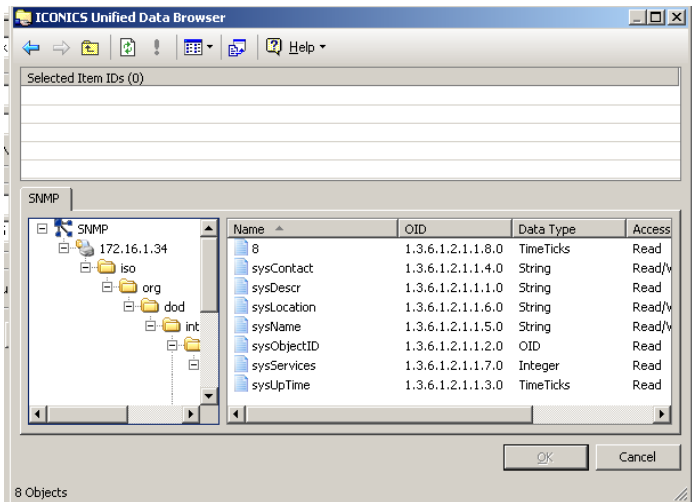


Figure 4 - UDB Exploring Subnet Devices

4. Once you have devices in Unified Data Browser, you can select SNMP OIDs you are interested and add them in the database. Click OK button when you make the selection.
5. Any change that has been made in the above steps, you need to click Apply button to confirm the change.

Please note you can create as many networks as you want. Networks under SNMP setup here are only “containers” of devices under specific IP Address or Segmented network. There is no relationship between networks in the database and your real networks. It is helpful and useful to help you customize and organize your network devices. (Compared with previous version that they are all put under the root level)

Another new feature is the possibility to receive traps from all devices you explore from segmented network environment. To do this, check the box “Receive All Traps from this network” and repeat the steps mentioned above.

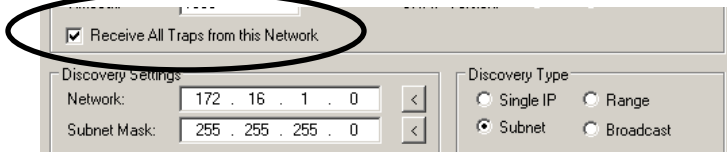


Figure 5 - Receive Trap Information from Devices