Andover Continuum

SNMP Configuration Guide

t.a.c®

This document is produced in the United States of America.

Product Names are trademarks of TAC. All other trademarks are the property of their respective owners.

Title: *Continuum SNMP Configuration Guide*

Revision C

Version 1.73

Date: January, 2006

TAC part number: 30-3001-855

TAC
One High Street
North Andover, MA 01845
(978) 470-0555
Fax: (978) 975-9782
http://www.tac.com

Andover Continuum SNMP Configuration Guide

30-3001-855
Revision C

January, 2006

About this Manual

What's in this Manual

- Continuum SNMP Support
- CX9702 and bCX9640 Controller Configuration
- bCX-40x0 SNMP Alarming Configuration
- Additional CX Controller SNMP Alarm Information
- Additional bCX-40x0 SNMP Alarm Information

Revision History

This is Revision C of this manual.

Table 1 Andover Continuum SNMP Configuration Guide Revision History

Document Revision	Software Version	Date
Revision C	Version 1.73	January, 2006
Revision B	Version 1.7	November, 2004
Revision A	Version 1.52	January, 2003

The following controllers support SNMP on corporate Ethernet networks:

Table 2 Minimum Controller Versions

Controller	Minimum Firmware Required
Continuum	
CX99xx	Version 1.52 or higher
CX94XX	Version 1.52 or higher
CX9201	Version 1.52 or higher
CX9702 SiteController	Version 1.2 or higher
bCX1 controllers 96xx	Version 1.0 or higher
BACnet	
bCX1-40x0	Version 4.3 or higher

Related Documentation

For additional or related information, refer to these documents.

Table 3 Related Documents

Document	Document Number
bCX1 Series Controller Technical Reference	30-3001-890
Command Terminal Configuration Guide	30-3001-843
BACnet Technical Reference	30-3001-862

Symbols Used

The Notes, Warnings and Cautions in this manual follow standard ANSI recommendations.

Note: Notes contain additional information of interest to the user.

CAUTION

Type of hazard

How to avoid hazard.

Failure to observe this precaution can result in injury or equipment damage.

WARNING

Type of hazard

How to avoid hazard.

Failure to observe this precaution can result in severe injury.

DANGER

ELECTRIC SHOCK HAZARD

How to avoid hazard.

Failure to observe these instructions will result in death or serious injury.

Contents

Chapter 1

Continuum SNMP Support

This chapter contains the following topics:

Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a message protocol, which network administrators can use to manage network communication. TAC controller's SNMP Alarming function uses the protocol to route alarms among Continuum controllers and other devices on corporate Ethernet networks. SNMP works by sending messages, called Protocol Data Units (PDUs), to different parts of a network.

Continuum alarms are sent as **SNMP Traps**. These are "Interrupt" signals informing a program that an event has occurred. A software interrupt is called a "Trap" (sometimes an "Exception"). **Continuum SNMP Traps** are fully detailed PDUs defined by a custom TAC Management Information Base (MIB) that is loaded into your Network Management System (NMS). Refer to "SNMP NMS Configuration and Testing" on page 22.

Arriving SNMP alarms are received by an NMS device. An NMS is a device (usually a PC) running the appropriate software to manage SNMP-capable devices across the network via the SNMP protocol. Examples of such software are: **HP OpenView** and **MG-Soft**'s MIB Browser. There can be more than one NMS on the network. Alarms are received, reformatted, and sent from one NMS-configured Andover Continuum (including BACnet) controller to the configured NMSs.

Andover Continuum's implementation of SNMP resides at the controller level. Other control systems rely on the workstation to announce SNMP events. In those cases, if the workstation is down, all SNMP identification and alarm routing stops. In Continuum, the controller has the ability to identify itself and to route alarms that it receives to other SNMP devices. With this configuration, there is no single point of failure.

Note: The more devices on the network that support the SNMP protocol, the better the system can be managed.

Andover Continuum Controllers Supporting SNMP

The following Continuum controllers support SNMP on corporate Ethernet networks: CX controllers CX99xx, CX94XX, CX9201, CX9702 SiteController, bCX1 controllers 96xx and 40x0.

Optionally, if they are configured in Continuum CyberStation, these controllers can also be enabled to deliver alarms via the SNMP protocol, as follows:

- Alarms originating from Infinet controllers can be delivered through all controller models that support SNMP except bCX1 40x0 to an SNMP NMS running SNMP software, such as HP Open View. Controllers can be be the alarm router or the alarm source. The implementation conforms to SNMP v1 and SNMP v2c. See Chapter 2.
- Alarms originating from BACnet controllers can be delivered through a bCX-40x0 controller that has been configured as an SNMP Alarm Gateway (SAG), which receives alarms from Andover Continuum and third-party BACnet controllers and redirects the alarms to other devices configured in an NMS. See "Configuring an SAG" on page 26 and "Configuring an SAI" on page 27 in Chapter 3.

Figure 1 on page 14 depicts these controllers alarming capability.

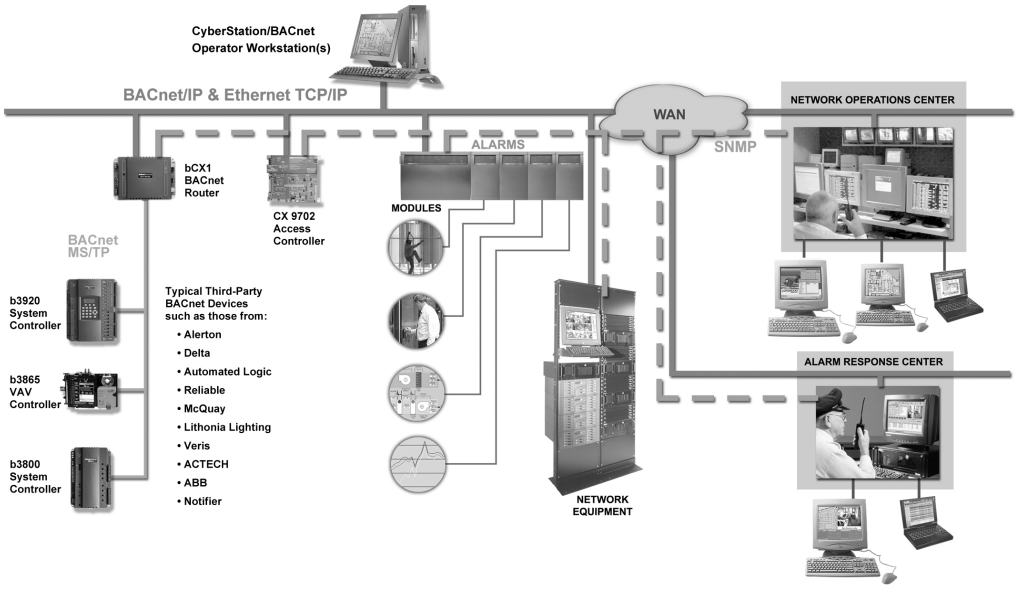

Figure 1 Continuum SNMP Alarming

Making SNMP Work

You must have an SNMP managed network and your controllers must be upgraded to a version that supports SNMP.

Continuum includes SNMP support for device identification on the network. Devices and their IDs are shown on the SNMP NMS client. For example, Figure 2 on page 15 illustrates Continuum devices that were discovered using **HP OpenView** SNMP browser:

In this example, a segment of the network is shown. There is a PC dedicated as a server, a PC acting as the Continuum workstation, and six controllers.

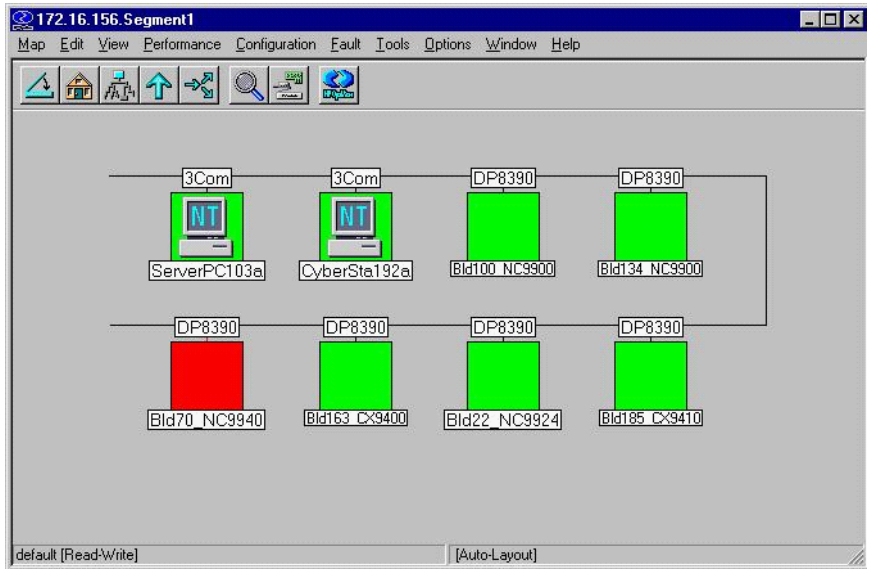

Figure 2 Continuum Devices in HP OpenView SNMP Browser

Note: No configuration of any kind is necessary for compatible Continuum components to be recognized by an SNMP management tool.

Configuring the System for SNMP Alarming

The following is an overview of configuring the system to enable SNMP Alarming:

Note: BACnet devices such as the bCX1 40x0 series have different alarming configurations. See Chapter 3.

You must have purchased the optional **SNMP Alarming Feature**.

1. Upgrade your controllers' firmware to the versions shown in Table 3.

Table 3 Controller Version

Controller	Version
CX99xx, CX94xx, CX9201	Version 1.52 or higher

Table 3 Controller Version (continued)

Controller	Version
CX9702	Version 1.2 or higher
bCX 96xx	Version 1.0 or higher
bCX1-40x0	Version 4.300011 or higher

2. Determine if SNMP Alarming is enabled on each CX controller. See "Determine if SNMP Alarming is enabled." on page 18. The CX99xx, CX94xx and CX9201 can be interrogated via the **Command Terminal Interface**. Other controllers are accessed via internal web-based configuration pages.

   "Controller Configuration for SNMP/NMS Alarming" on page 18 details the steps of this procedure. These are settings that can be made on a single configuration screen viewed via the terminal interface of the CX.

3. Determine the **Community Passwords** that exist on your SNMP network for **GET** and **SET** requests and configure the CX. See "Configure the community passwords for GET and SET requests." on page 19.

4. Configure each CX controller with the IP addresses of the computers on the network where the alarms are to be sent This is the NMS address(es). See "IP Addresses" on page 19.

5. Determine the size of the data table within the CX that holds SNMP alarms and configure the CX. See "Alarm Data Table Set Up" on page 20. See also Appendix A, "Continuum SNMP Alarm Table" on page 30.

6. Configure the alarm links (1-8) you want to be echoed as SNMP alarms. See "Alarm Links Echoes" on page 21.

7. Load three TAC-specific MIB files into your network management tool. Refer to "SNMP NMS Configuration and Testing" on page 22.

   The MIB files can be downloaded from the TAC Tech Support website.

Chapter 2

CX9702 and bCX9640 Controller Configuration

This chapter contains the following topics:

Controller Configuration for SNMP/NMS Alarming

This chapter details procedures for configuring SNMP/NMS alarming for CX9702 and bCX9640 controllers. Refer to Chapter 3, "bCX-40x0 SNMP Alarming Configuration" on page 25 to configure bCX-40x0 controllers.

Access to Configuration Information

Access to the configuration pages within the controller varies from model to model. Older models (CX9201, CX94xx and CX99xx) are configured via their Command Terminal interface. Newer models (CX9702 and bCX9640) allow configuration via internal configuration web pages. It is beyond the scope of this book to explain how to access each configuration area. You must have the appropriate book(s) for an explanation. Table 4 shows the required documents:

Table 4 Documents

Document	Number
Command Terminal Configuration Guide (CX9201, CX94xx, CX99xx)	30-3001-843
BACnet Controller Technical Reference	30-3001-862
bCX1 Series Controller Technical Reference (CX96xx)	30-3001-890

Note: The model CX9702 controller has no technical manual. Instructions for accessing the configuration pages are listed on the front cover plate.

Enable SNMP Alarming

Perform the following steps to enable SNMP alarming.

Step 1: Determine if SNMP Alarming is enabled.

a. Log on to the **Configuration** page.

b. Determine if SNMP Alarming is activated in the controller. If it has been purchased as a controller option, a button labeled SNMP should appear or an SNMP link will be shown. You can also check the Options tab of the controller editor in the Continuum CyberStation to see if the controller is SNMP enabled.

Step 2: Configure the community passwords for GET and SET requests.

Once you are in the SNMP Configuration page you will see an area requesting the following information: **Communities**.

SNMP community is part of the simple security scheme. These entries are passwords. The **GET** action allows the NMS to retrieve information from the Controller. **SET** allows the NMS to write information to the controller.

The default **Get Community** is public, and the default **Set Community** is private.

The Trap community is set to **acctrap**. This setting cannot be changed.

These passwords exist in your NMS management scheme. Check with your network administrator to determine the correct passwords to insert for each entry. Each entry can be a maximum length of 8 characters.

Step 3: Set **Communities**.

Note: The communities set for a controller apply to that controller only. Different Controllers can have different communities.

Note: This information can be changed at any time without having to reset your controller after configuration.

IP Addresses

Perform the following steps to set the (12) IP Addresses.

Step 1: Log on to the **Configuration** page.

Step 2: Configure two IP addresses of the computers on the network where the alarms are to be sent.

SNMP alarms can be sent to no more than 12 SNMP NMS devices. The first two addresses entered on this page are saved in the controller's non-volatile RAM, *and will not be lost even if the Controller is reset*. The other 10 possible notification target IP addresses are stored in volatile RAM. If the controller is reset, their IP addresses will be initialized to 0.0.0.0, and the notification types will be initialized to **None**.

a. Enter the IP addresses of the first two targets into the area provided.

b. Select the **Notification Type** for each IP address.
Two notification types are supported:

- **None** - Alarms will not be automatically delivered to the notification target.

Note: Any NMS device with the ACC MIB files loaded can retrieve alarms from the controller using the GET command.

- **Trap** - Alarms will be automatically delivered to the notification target via SNMP v2c trap.

Note: This information can be changed at any time without having to reset your controller after configuration.

Step 3: Configure the 10 remaining IP addresses.

The 10 remaining device IP addresses must be entered using the **SNMP SET** command. This operation requires knowledge of your particular NMS software package. Refer to Appendix A, "accNotifyTable (Target IP Addresses)" on page 33 for details about the locations where these IP addresses can be entered.

Please refer to the documentation of your NMSs for how to read and set MIB entries.

Alarm Data Table Set Up

Set up the **Alarm Data Table** following the procedure below.

Step 1: Log on to the **Configuration** page.

Step 2: Determine the size of the alarm data table within the CX that will hold SNMP alarms.

The **Table Size** field is used to specify the size of the SNMP Alarm Table. The Controller maintains an internal table for SNMP alarms. One SNMP alarm occupies one entry of the table. You can set the number of entries you want for the table. The Alarm Table occupies RAM memory within the controller and is lost when power is lost.

The following are memory use guidelines for determining your table size:

- The overall table structure requires 32 bytes of overhead.

- There are 18 bytes of overhead memory for each entry. If you allocate more entries than necessary, 18 bytes are still used per entry.
- Each SNMP alarm entry that is used consumes another 114 bytes for the data.

  To determine a safe estimate, find how many points can go into alarm at any given time and double that number.

Example:

On a system with 1000 points, where at any given time 20 points may go into alarm, setting the table to 40 would be a safe recommendation.

Refer to Appendix A, "Continuum SNMP Alarm Table" on page 30 for detailed information about how the alarm table works and its structure.

Step 3: Enter the desired table size into the area provided.

Note: The table size can be changed at any time without having to reset your controller after configuration.

Alarm Links Echoes

Perform the following steps to set up the alarm link echoes (if desired).

Step 1: Log on to the **Configuration** page.

Step 2: Determine which alarm links (1-8) you want to be echoed as SNMP alarms.

The **Alarm Links** field is used to specify which Continuum alarms are to be echoed as SNMP alarms.

Step 3: Select the alarm links to echo as SNMP alarms in the area provided.

Any of the specified alarm links that are attached to points or system variables will become SNMP alarms, and will be sent to both the CyberStation and the SNMP NMS. Alarms that attach to points or system variables other than those selected are not SNMP alarms. They will be sent to CyberStation; however, they will not be sent to the specified NMS.

Note: The alarm links selection can be changed at any time without having to reset your controller after configuration.

Step 4: Upon Completion, **Save** the configuration.

CX9702 and bCX9640 Controller Configuration

As stated in "Access to Configuration Information" on page 18, use the internal configuration web pages for the CX9702 and bCX9640 controllers to verify their configurations.

The **Options** tab of InfinityController Editor shows SNMP configuration information for each type of controller. The type of information shown varies depending on the controller. For security reasons, SNMP Communities are not shown on this page.

SNMP NMS Configuration and Testing

For the software that manages your network to understand the controller's alarm table structure, you must load and compile the three Andover Continuum-specific MIB files into your network management tool.

The three necessary MIB files can be downloaded from the TAC Tech support website. See Table 5.

Table 5 TAC MIB Files

MIB	Action
ANDOVER-CONTROLS-MIB.my	Must be installed first. Provides module-specific information.
ACC-NOTIFICATION-MIB.my	Defines the SNMP notification table
ACC-NC-ALARM-MIB.my	Defines the SNMP alarm table

Perform the following steps:

Step 1: Import the files using your NMS software and compile them.

Step 2: Issue an SNMP Query on each sub-level to verify installation of the MIBs.

An example of the feedback from this query is shown in Figure 3.

Test SNMP Alarms

Perform the following test to check your alarms:

1. Create an Expression alarm and attach it to a test Numeric point.

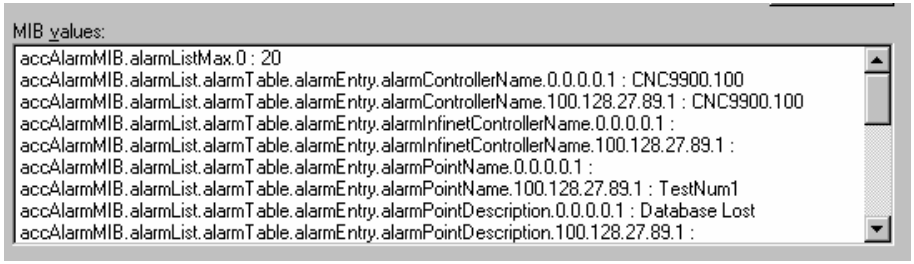

Figure 3 Example: MIB Values

2. Put the point in alarm.
3. Open the alarm browser in your NMS tool.
4. Figure 4 on page 23 shows the following error posting (**MG-Soft** tool shown).

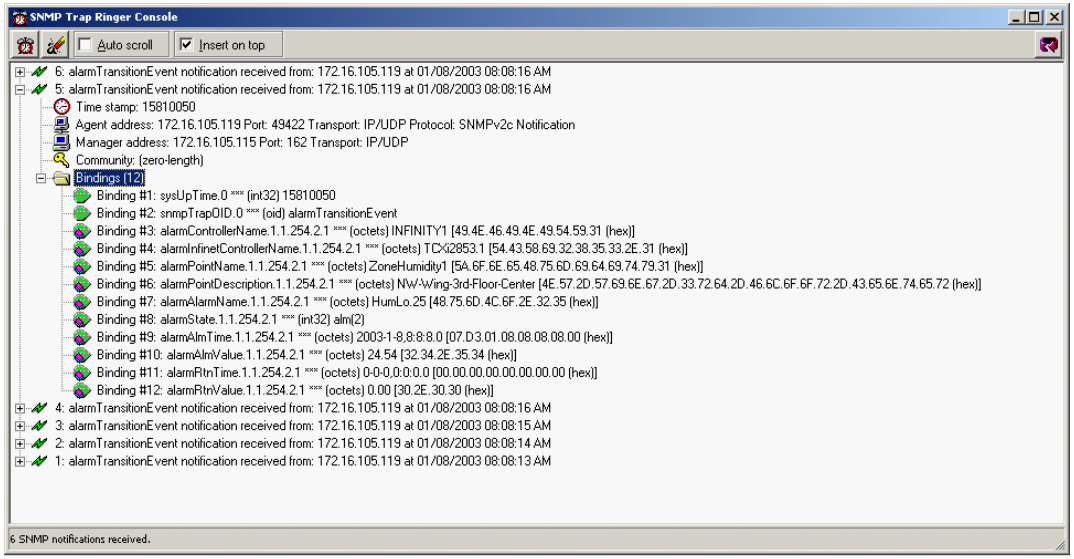

Figure 4 SNMP Alarm Test (1 of 2) (MG-Soft tool shown)

5. Take the point out of alarm, and observe another entry into the alarm browser. See Figure 5 on page 24.
6. Observe that alarm posting is working successfully.

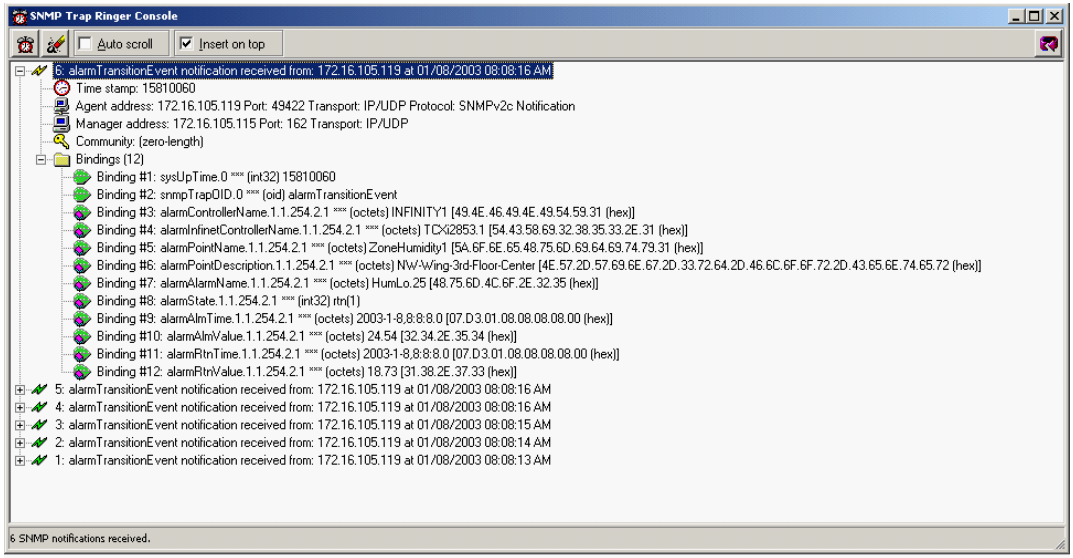

Figure 5 SNMP Alarm Test (2 of 2) (MG-Soft tool shown)

Chapter 3

bCX-40x0 SNMP Alarming Configuration

This chapter contains the following topics:

Configuring a bCX-40x0 Controller for SNMP Alarming

The routing of SNMP protocol is supported in Andover Continuum bCX-40x0 controllers. Additionally, Andover Continuum and third-party BACnet controllers can deliver alarms, via a bCX-40x0 "gateway" controller to NMSs. See also Appendix B.

- A bCX-40x0 controller can serve as an SNMP Alarm Gateway (SAG) controller, through which SNMP alarms are received from multiple BACnet devices (also not configured in an NMS) and deliver them to NMS devices (usually PCs). See "Configuring an SAG", below.
- An Andover Continuum or third-party BACnet controller can be configured as an SNMP Alarm Initiator (SAI), so any SNMP alarms it receives are automatically routed to the SAG for delivery. See "Configuring an SAI" on page 27.

Configuring an SAG

If a bCX-40x0 controller is configured as an SAG, SNMP alarms are received from Andover Continuum and third-party SAI controllers and delivered to other devices (PCs) that are configured with one or more NMS(s). When the SAG receives the alarm notification, it verifies that it is an SNMP alarm and sends it to the configured NMSs with SNMP Trap messages. The SAG also records the alarm in its internal database. Any NMS can poll this database at any time using the SNMP management tool.

Configure a 40x0 controller as an SAG in the controller's **SNMP Configuration Internal Commissioning** web page. In the **Notifications** section, in the **First** and **Second** fields, enter the address of the devices (PCs) to which these SNMP alarms should be routed. Please refer to the *bCX1 Series Controller Technical Reference, 30-3001-890*, for more information on bCX-40x0 commisioning.

Configuring an SAI

An Andover Continuum or third-party BACnet controller can be configured as an SAI using the Continuum **EventEnrollment** and **EventNotification** editors. When an SAI initiates a BACnet alarm, it labels it (See step 3.) as an SNMP alarm and sends it to the configured SAG, which in turn delivers it to the NMS device(s), with a BACnet confirmed or un-confirmed event notification, using the SNMP protocol.. SAIs do not need the SNMP alarming software, and usually do not have it. There can be many SAIs on the network.

Note: An SAG controller (bCX-40x0) can also be an SAI, because if it is also configured as an SAI, it can initiate alarms to itself.

To configure a BACnet controller as an SAI, follow this procedure:

1. Create one or more **EventNotification** objects and, on the **Delivery** tab, add the SAG (in this case a bCX1 model 40x0) as the recipient. Click the **Add Recipient** button to display the **Recipients Configuration** dialog. See Figure 6.

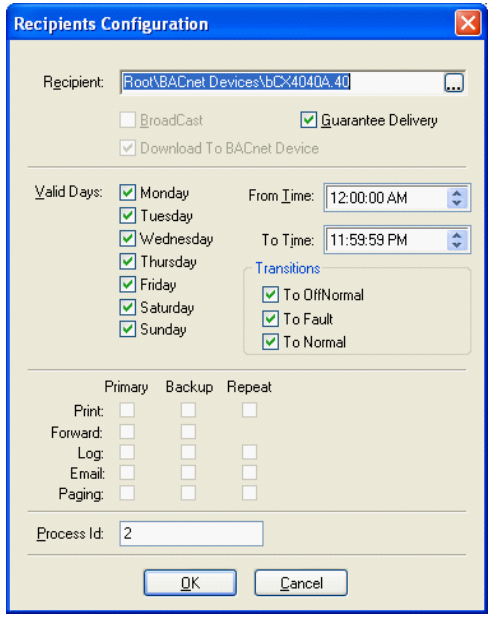

Figure 6 Recipients Configuration Dialog

2. In the **Recipient** field, browse for and select the SAG (40x0) controller that will receive and route the alarm.
3. In the **Process Id** field, enter **2**. (This is the alarm label.)
4. Create an **EventEnrollment** object to be associated with the EventNotification.
   a. If **Event Enrollment** object is used, set the **processidentifier** to the **SNMP Alarming process identifier**.

Note: If the SNMP alarms are labled, any NMS can poll the SAI database at any time using the SNMP protocol.

   b. If you use a BACnet **NotificationClass** object, instead of an **EventEnrollment**, specify the SAG (bCX1 model 40x0) in the **Recipient_List**. Likewise, if you are using **NotificationClass**, set the **processidentifier** of the recipient (targeted to the SAG in the **Recipient_List**) to 2.
5. On the **General** tab of the EventEnrollment editor, in the **EventNotification** field, browse for and select the EventNotification object that had specified the SAG (bCX1 model 40x0) in its **Recipients Configuration** dialog. (See Step 2.) This automatically designates the SAG as the recipient as well as designates **2** as the **Process ID**.

   As an alternative to using the **EventNotification** field, on the bottom of the **General** tab, in the **Recipient** field, browse for and select the same SAG (40x0) that was specified in the EventNotification's **Recipients Configuration** dialog. (See Step 2.) The **Process Id** field displays **2**.

Note: The BACnet properties **Recipient, Process Id, Priority, and Confirmed Notifications,** are unselectable if the **EventEnrollment** object resides on a device that does not support these properties.

6. Configure the remainder of the **EventNotification** and **EventEnrollment** objects as you normally would. (See the Continuum online help for those editors.)

Appendix A

Additional CX Controller SNMP Alarm Information

This appendix contains the following topics:

Note: Appendix A applies only to controller models other than bCX-40x0. Refer to "bCX-40x0 SNMP Alarming Configuration" on page 25 and Appendix B, "Additional bCX-40x0 SNMP Alarm Information" on page 37 for information about bCX-40x0 SNMP Alarming.

CX Controller SNMP Alarms

An SNMP alarm is defined as any Continuum alarm that occupies an alarm link that has been selected on the **SNMP Configuration** page of the CX controller.

Continuum SNMP Alarm Table

The CX controller maintains an internal table for storing SNMP alarm occurrences. One SNMP alarm occupies one entry of the table.

The table entries consist of the information shown in Table 6.

Table 6 CX Controller's Internal Table

Entry	Description
bX Controller Name	CX Controller Name
BACnet Controller	Blank if it is a CX point
Point Name	Continuum Point Name
Point Description	Point's description attribute
Alarm Name	Continuum alarm name linked to the point
State	There are three potential values: **ALM** = 2 for in alarm **RTN** = 1 for returned to normal **Null** = if no ALM or RTN
ALMTime	Time stamp or null if no ALM
ALMValue	Value at timestamp or null if no ALM
RTNTime	Time stamp or null if no RTN
RTNValue	Value at timestamp or null if no RTN
IENAD	IENAD that identifies point in IE table; 0 for internal alarm
Alarm Link	Number identifying which Continuum alarm link, 1-8 0 for internal alarm

New Alarms

As new alarms are encountered, they are entered into the table as a new item under the last alarm, occupying another entry in the table. If **Trap Notification** is enabled, a Trap is then sent to the NMS(s).

If the table is full and a new alarm is encountered, the oldest item in the table is erased to make room for the new entry. An internal alarm, notifying the NMS that an overflow has occurred, is generated and sent with the normal notification of the alarm.

Existing Alarms

If an alarm is encountered and an existing alarm entry is found in the table for that point, a new entry will not be created. The existing alarm listing will be updated with the new information and a notification will then be sent, if **Trap Notification** is enabled.

Continuum SNMP Intrinsic Alarms

There are two intrinsic alarm conditions that the CX generates:

- "Controller Reset Alarm", detailed below
- "SNMP Alarm Table Overflow Alarm" on page 32.

Note: Intrinsic alarms will not be sent if the **Notification** is set to "**None**". These alarms are sent only to the SNMP target(s) and not to CyberStations.

Controller Reset Alarm

The Controller Reset Alarm enters the alarm-state when the controller resets. It changes to return-to-normal state when the user reloads it from CyberStation or the clock of the controller gets synchronized. Table 7 describes the fields of the alarm.

Table 7 Reset Alarm Fields

Alarm	Field
Alarm IENAD	00.00.00.00
Alarm Link	1
Controller Name	When in alarm-state, the controller name is the TAC default name, which is INFINITYXXX, where XXX is the Energy Net ID of the controller. After the user reloads the controller from CyberStation, the alarm goes to return-to-normal state, and the controller name is the user-defined name in CyberStation
Infinet Controller Name	Null
Point Name	Null

Table 7 Reset Alarm Fields (continued)

Alarm	Field
Point Description	Database Lost
Alarm Name	Controller Reset
Alarm State	State of the alarm: **RTN** = 1 **Alm** = 2
Alarm Value	0.00
Alarm Time	When the controller resets, it loses its clock, the time is zero
RTN Value	0.00
RTN Time	Time when the controller is reloaded from CyberStation or when its clock was synchronized

SNMP Alarm Table Overflow Alarm

When the controller has to delete used entries in the SNMP alarm table, this intrinsic alarm goes to alarm state. This can happen in one of two scenarios:

- If an SNMP alarm comes in, the controller cannot find an entry for the alarm in its SNMP alarm table, and all the entries of the table are used. The controller will delete the oldest updated SNMP alarm entry.
- If the user manually decreases the size of the SNMP alarm table in the SNMP alarming configuration form and older SNMP alarms entries have to be deleted to conform to the smaller table size

The SNMP Alarm Table Overflow alarm returns to normal state when the user manually increases the size of the SNMP alarm table size. See “Alarm Data Table Set Up” on page 20 for details of how to change SNMP alarm table size.

Table 8 gives the descriptions of the fields of the alarm.

Table 8 Intrinsic Alarm Fields

Alarm	Field
Alarm IENAD	00.00.00.00
Alarm Link	2
Controller Name	Name of the Ethernet Controller
Infinet Controller Name	Null

Table 8 Intrinsic Alarm Fields (continued)

Alarm	Field
Point Name	Null
Point Description	SNMP Alarm Table Overflowed
Alarm Name	Alarm Overflow
Alarm State	State of the alarm: **RTN** = 1 **Alm** = 2
Alarm Value	The SNMP alarm table size when the transition into the alarm state occurred
Alarm Time	Time when the table overflowed
RTN Value	The SNMP alarm table size when the user increased the size of the SNMP alarm table
RTN Time	Time when the user increased the SNMP alarm table size

Configuring Other NMS Device Notifications

Continuum supports up to 12 SNMP notification targets. The first two of them are non-volatile. Their IP addresses and notification types are saved in the CX Controller's non-volatile RAM, *and will not be lost even if the Controller resets*. The other 10 notifications are volatile. Their information is saved in volatile RAM. If the Controller resets, their IP addresses will be initialized to 0.0.0.0, and the notification types will be initialized to **None**.

accNotifyTable (Target IP Addresses)

This section describes the **accNotifyTable** from which the NMS can change the 10 additional target IP addresses.

All the notification targets, even the two non-volatile addresses, can be set from NMSs. Figure 7 on page 34 shows a columnar view of the notification settings using the **MG-Soft MIB** Browser, V7.10.

Please refer to the documentation of your NMSs for how to read and set MIB entries.

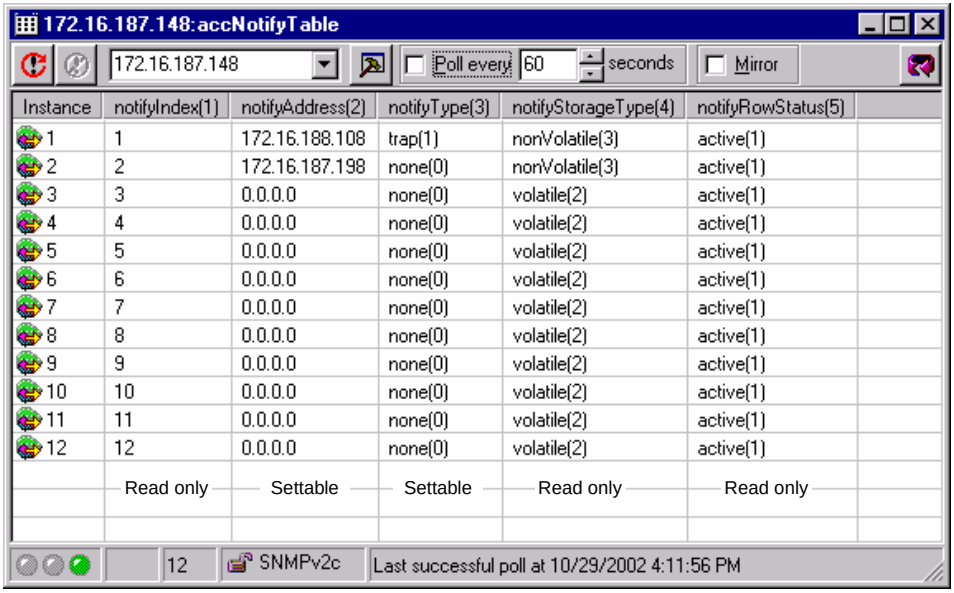

Figure 7 MG-Soft MIB Browser - accNotifyTable

In this view you can see all the notification settings. The first two columns, **Instance** and **notifyIndex**(1) show the previously entered settings from the CX controller SNMP configuration form. Rows 3 through 12 are where the remaining 10 devices are configured.

The second column shown, **notifyIndex**, is the index of the SNMP notifications from 1 to 12. This field is read only.

The third column, **notifyAddress**, is the IP address of notification, it is settable.

The fourth column, **notifyType**, is the type of the notification. Valid notification types are Trap (1) and none (0). This field is settable.

The fifth column, **notifyStorageType**, shows the storage type of the notifications. As shown in the image, the first two notifications are non-volatile, and the other ten are volatile. This field is read only.

The last column, **notifyRowStatus**, is read only.

CX Controller SNMP Defaults

Community Strings:

(8 characters max.)

GET	Public
SET	Private

Notifications:

IP:	0.0.0.0
Type:	None

Table Size:

0

The overall table structure requires 32 bytes of overhead.

There are 18 bytes of overhead memory for each entry.

Each SNMP alarm entry that is used, consumes another 114 bytes for the data.

Port Numbers

Port number 161 is used for SNMP, and number 162 is used for SNMP Traps.

Appendix B

Additional bCX-40x0 SNMP Alarm Information

This appendix contains the following topics:

bCX-40x0 SNMP Alarms

This appendix additional SNMP alarming information for the bCX-40x0 controller. Also see Chapter 3.

bCX-40x0 SNMP Alarm Table

The bCX-40x0 controller maintains an internal table for storing SNMP alarm occurrences. One SNMP alarm occupies one entry of the table. The table entries consist of the information shown in Table 9.

ACC-BACNET-ALARM-MIB

The **ACC-BACNET-ALARM-MIB** file defines a node, named **accAlarmMIB**, under **accBACnetEthernetController**. Under this node, an alarm table named **alarmTable** is defined, whose fields are specified in Table 9. The key to this table is Sequence Number. Refer to "Sequence Number" on page 45.

Table 9 Alarm Table Defined in ACC-BACNET-ALARM-MIB

Field	SNMP Syntax[1]	Size[2]	Description
Device Name	DisplayString	16	The name of the device that initiates the alarm
Point Name	DisplayString	16	The name of the point that causes the alarm
Point Description	DisplayString	32	The description of the point that causes the alarm
Property Name	DisplayString	16	The name of the point property whose value change triggers the alarm
Event Originator Name	DisplayString	16	The name of the object that originates the event notification If the alarm point originates the notification, this field repeats the **PointName** field, otherwise it contains the **EventEnrollment** object name
Event Originator Description	DisplayString	32	The description of the object that originates the **eventnotification** If the alarm point originates the notification, this field repeats the **PointDescription** field, otherwise it contains the **EventEnrollment** object description.

Table 9 Alarm Table Defined in ACC-BACNET-ALARM-MIB (continued)

Field	SNMP Syntax[1]	Size[2]	Description
Transition Type	Integer[3] • To OffNormal = 0 • To Fault = 1 • To Normal = 2		The type of the transition
To State	Integer[4] • Normal = 0 • Fault = 1 • OffNormal = 2 • High Limit = 3 • Low Limit = 4 • Life Safety Alarm = 5		The state that the alarm transits to
From State	Integer[4] • Normal = 0 • Fault = 1 • OffNormal = 2 • High Limit = 3 • Low Limit = 4 • Life Safety Alarm = 5		The state that the alarm transits from
Alarm Type	Integer[5] • Change of Bit String = 0 • Change of State = 1 • Change of Value = 2 • Command Failure = 3 • Floating Limit = 4 • Out of Range = 5 • Change of Life Safety = 7		The **EventType** of this alarm
To-OffNormal Value	DisplayString: The content of this field depends on the Alarm Type. Table 10 on page 41 specifies more details.	32	Value of the most recent To-OffNormal transition

Table 9 Alarm Table Defined in ACC-BACNET-ALARM-MIB (continued)

Field	SNMP Syntax[1]	Size[2]	Description
To-OffNormal Transition Time	DateAndTime		Time when the most recent To-OffNormal transition occurs **Note:** Some devices use a sequence number in their event notifications. If so, the SAG uses the local time when the transition is received. Refer to "Sequence Number" on page 45.
To-OffNormal Status Flags	Integer[6] • Bit 0 (LSB) = In Alarm • Bit 1 = Fault • Bit 2 = Overriden • Bit 3 = Out_Of_Service		The status flags contained in the most recent To-OffNormal transition
To-Normal Value	DisplayString: The content of this field depends on the Aarm Type. Table 10 on page 41 specifies more details.	32	Value of the most recent To-Normal transition
To-Normal Transition Time	DateAndTime		Time when the most recent To-Normal transition occurs **Note:** Some devices use a sequence number in their event notifications. If so, the SAG converts it to local time when the transition is received. Refer to "Sequence Number" on page 45.
To-Normal Status Flags	Integer • Bit 0 (LSB) = In Alarm • Bit 1 = Fault • Bit 2 = Overriden • Bit 3 = Out_Of_Service		The status flags contained in the most recent To-Normal transition
Message	DisplayString	32	The message text of the event notification
Sequence Number	Unsigned Integer		The sequence number of the record. "Sequence Number" is the key to this table.

1. SNMP Syntax can be thought of as the data type used in SNMP.
2. Apply to string only. If a string's size is larger than that specified, it will be truncated.
3. Same as the bit number of the BACnetEventTransitionBits in the BACnet Specification (ANSI/ASHRAE Standard 135-2001).
4. Same as the BACnetEventState in the BACnet Specification (ANSI/ASHRAE Standard 135-2001).

5. Same as the BACnetEventType in the BACnet Specification (ANSI/ASHRAE Standard 135-2001). Buffer Ready is excluded.
6. Same as the BACnetStatusFlags in the BACnet Specification (ANSI/ASHRAE Standard 135-2001).

alarmTable Value Fields

The **To-OffNormal Value** or **To-Normal Value** fields of the **alarmTable** (Refer to Table 9 on page 38) are chosen from the value list reported in the **Event Values** of the most recent To-OffNormal or To-Normal EventNotification. The item chosen depends on the alarm type, as specified in Table 10. When reported to NMS(s), the value is rendered as a string. The format is specified in the table.

Table 10 Data and Rendering Format of SNMP Alarm Values

Alarm Type	Data	Rendering Format
CHANGE_OF_BITSTRING	Referenced_Bitstring	**Binary string** For each bit, "1" means set, and "0" means clear
CHANGE_OF_STATE	New_State	If the **ObjectType** is Binary Input, or Binary Value: "Inactive" if new state is 0, "Active" if 1 If the **ObjectType** is Multi-State Input or Multi-State Value, the value is rendered in decimal
CHANGE_OF_VALUE	New_Value	If the **ObjectType** is Binary Input, Binary Output, or Binary Value: the value is rendered as "Active" or "Inactive" If the **ObjectType** is Multi-state Input, the value is rendered in decimal If the **ObjectType** is Analog Input: **AnalogOutput**, or **AnalogValue**, the value is rendered as a float number For all other object types, the value is rendered as a hexadecimal number.
COMMAND_FAILURE	Command_Value	If the object type is **BinaryOutput**: "Inactive" if new state is 0, "Active" if 1 If the **ObjectType** is Multi-State Output, the value is rendered in decimal.
FLOATING_LIMIT	Referenced_Value	Same as CHANGE_OF_VALUE
OUT_OF_RANGE	Exceeding_Value	Float

Table 10 Data and Rendering Format of SNMP Alarm Values (continued)

Alarm Type	Data	Rendering Format
CHANGE_OF_LIFE_SAFETY	New_State	Decimal

If the Controller is Off-Line

Data of some fields in Table 9 on page 38 are contained in the **EventNotification** packet. Such fields need no further resolution. Other fields, however, require one or more rounds of data inquiries from the SAG to the initiating device to resolve them. If the inquiry communication in whole or part fails, the SAG reports offline values to the NMS(s) for those fields that are not resolved. Table 11 defines the offline values. "Resolved" means the data requires no further resolution.

Table 11 Offline Values for the SNMP Alarm Table

Field	Offline Value
Device Name	`<Device identifier in hexadecimal>`

Point Name	If the event is initiated from a point:
	
	`<Object identifier in hexadecimal>`
	
	If the event is initiated from an **EventEnrollment** object, and the **Object_Property_Reference** has been resolved:
	
	`<Referenced object identifier in hexadecimal>`
	
	If the event is initiated from an **EventEnrollment** object, and the **Object_Property_Reference** has not been resolved:
	
	"`Device Offline`" is returned

Point Description	"Device offline"
Property Name	"Device offline"
Event Originator Name	`<Object identifier in hexadecimal>`
Event Originator Description	"Device offline"

Table 11 Offline Values for the SNMP Alarm Table (continued)

Field	Offline Value
Transition Type	Resolved
To State	Resolved
From State	Resolved
Alarm Type	Resolved
To-OffNormal Value	If the object type is Multi-state Input, Multi-state Output, or Multi-state Value, the SAG will try to get the decimal number. If the controller is offline, the value is rendered as a decimal number. For other points, it will be resolved from the **EventNotification** packet
To-OffNormal Transition Time	Resolved
To-OffNormal Status Flags	Resolved
To-Normal Value	Resolved
To-Normal Transition Time	Resolved
To-Normal Status Flags	Resolved
Message	Resolved
Sequence Number	Resolved

bCX-40x0 SNMP Internal Alarms

Note: In BACnet, “Intrinsic” has a different meaning than it does in Continuum. Therefore, in BACnet, intrinsic alarms are called “Internal” alarms.

In addition to normal SNMP alarms, there are two internal alarms:

1. Controller Reset
2. SNMP Alarm Table Overflow

Table 12 specifies their transitions.

Table 12 SNMP Internal Alarm Transitions

Alarm	Transition To OffNormal	Transition To Normal
Controller Reset	The controller starts up	The controller gets reloaded if it is in the **OffNormal** state[1]
SNMP Alarm Table Overflow	When an alarm from a new source arrives and the database is full. *OR:* When the user decreases the database size and some alarm records will be deleted	The User increases the alarm table size if it is in the **OffNormal** state[1]

1. See Table 9 on page 38.

Table 13 specifies the data of the two internal alarms.

Table 13 bCX SNMP Internal Alarms Values

Field	Controller Reset	SNMP Alarm Table Overflow
Device Name	Name of the SAG controller	Name of the SAG controller
Object Name	Controller Reset	“Alarm Overflow”
Object Description	Database Lost	“SNMP Alarm Table Overflow”
Property Name	None	None
Event Originator Name	None	None
Event Originator Description	None	None
Transition Type	To OffNormal = 0 To Normal = 2	To OffNormal = 0 To Normal = 2
To State	Normal = 0 OffNormal = 2	Normal = 0 OffNormal = 2
From State	Normal = 0 OffNormal = 2	Normal = 0 OffNormal = 2
Alarm Type	Change of State = 1	Change of State = 1
To-OffNormal Value	None	Table size when the transition occurs
To-OffNormal Time	Controller local time when the transition occurs	Controller local time when the transition occurs

Table 13 bCX SNMP Internal Alarms Values (continued)

Field	Controller Reset	SNMP Alarm Table Overflow
To-OffNormal Status Flags	1 (Bit 0 = 1, or In Alarm)	1 (Bit 0 = 1, or In Alarm)
To-Normal Value	None	Table size when the transition occurs
To-Normal Time	Controller local time when the transition occurs	Controller local time when the transition occurs
To-Normal Status Flags	0	0
Message	None	None
Sequence Number	1	2

Sequence Number

Unlike SNMP alarms in Continuum, IENAD is not used; in BACnet SNMP protocol, sequence number is used instead.

The sequence number serves two purposes:

1. It is used to log the relative order of the transitions.
2. It is used as the key to identify each transition.

The SAG assigns a unique sequence number to each SNMP alarm transition it receives. When a transition is received, if the record for the alarm source already exists in the database and has a sequence number for the previous transition, the sequence number will be updated to that associated with the new transition. A sequence number is a 32-bit unsigned integer. The algorithm to assign the sequence number is as follows:

- Sequence number of Controller Reset transitions = 1
- Sequence number of SNMP Alarm Table Overflow transitions = 2
- Sequence number of the first alarm transition = 3
- Sequence number of the new alarm transition = Sequence number of the previous transition + 1

Note: In reality, using 32-bit unsigned integers for sequence numbers is sufficient and no wrap-around will occur. About 4.3 billion transitions can be assigned before a wrap-around occurs. If alarms arrive every 10ms, this number can hold for about 497 days. Considering the processing ability of the controller, the time is much longer. If alarms arrive every second, the number can hold for about 136 years.

Record Age

The following is how the the oldest alarm is picked.

The age of a record is determined by the time the SAG receives the record's most recent transition, not by the time when the transition is originated from the originating device. The later such a time is, the younger the record is. This is for programming simplicity because it co-incides with the definition of the sequence number. Without considering the internal alarms, which are processed separately, the smaller the sequence number, the older the record is and vice-a-versa.

Configuring Other NMS Device Notifications

Continuum supports up to 12 SNMP notification targets. The first two of them are non-volatile. Their IP addresses and notification types are saved in the CX Controller's non-volatile RAM, *and will not be lost even if the Controller resets*. The other 10 notifications are volatile. Their information is saved in volatile RAM. If the Controller resets, their IP addresses will be initialized to 0.0.0.0, and the notification types will be initialized to **None**.

accNotifyTable (Target IP Addresses)

This section describes the **accNotifyTable** from which the NMS can change the 10 additional target IP addresses.

All the notification targets, even the two non-volatile addresses, can be set from NMSs. Figure 8 on page 47 shows a columnar view of the notification settings using the **MG-Soft MIB** Browser, V7.10.

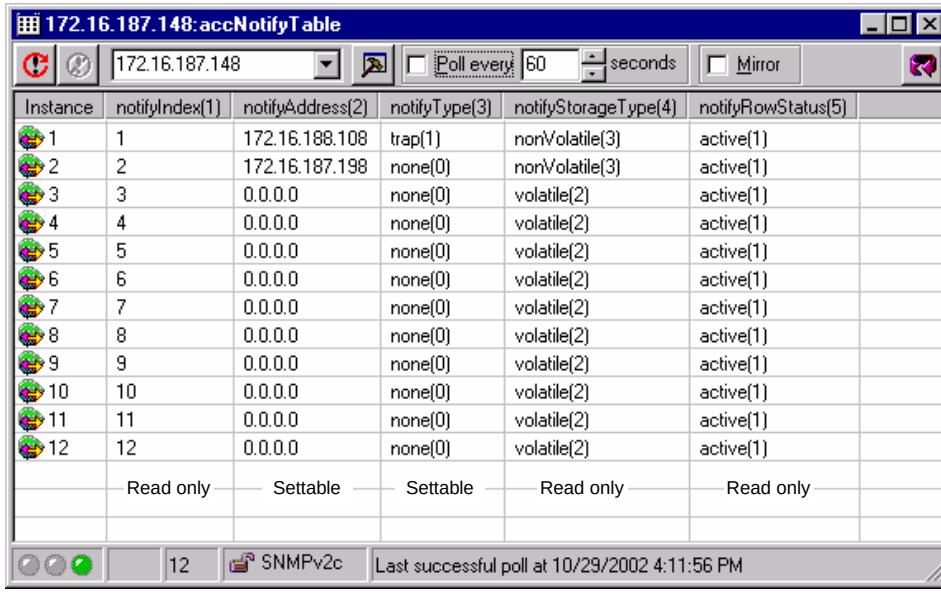

Figure 8 MG-Soft MIB Browser - accNotifyTable

Please refer to the documentation of your NMSs for how to read and set MIB entries.

In this view you can see all the notification settings. The first two columns, **Instance** and **notifyIndex**(1) show the previously entered settings from the CX controller SNMP configuration form. Rows 3 through 12 are where the remaining 10 devices are configured.

The second column shown, **notifyIndex**, is the index of the SNMP notifications from 1 to 12. This field is read only.

The third column, **notifyAddress**, is the IP address of notification, it is settable.

The fourth column, **notifyType**, is the type of the notification. Valid notification types are Trap (1) and none (0). This field is settable.

The fifth column, **notifyStorageType**, shows the storage type of the notifications. As shown in the image, the first two notifications are non-volatile, and the other ten are volatile. This field is read only.

The last column, **notifyRowStatus**, is read only.

bCX-40x0 SNMP Defaults

Community Strings:

(8 characters max.)

GET	Public
SET	Private

Notifications:

IP:	0.0.0.0
Type:	None

Table Size:

20

Port Numbers

Port number 161 is used for SNMP, and number 162 is used for SNMP Traps.

Index

T

Andover Continuum SNMP Configuration Guide
Document Number 30-3001-855
Revision C