Andover Controls

WE'RE BUILDING SMART

CONTINUUM™

SNMP Configuration Guide

Continuum SNMP Configuration Guide, Version: A, January, 2003

Andover Controls part number: 30-3001-855

Andover Controls Corporation
300 Brickstone Square
Andover, MA 01810
(978) 470-0555
fax: (978) 470-0946

Contents

What Is Continuum SNMP Support?

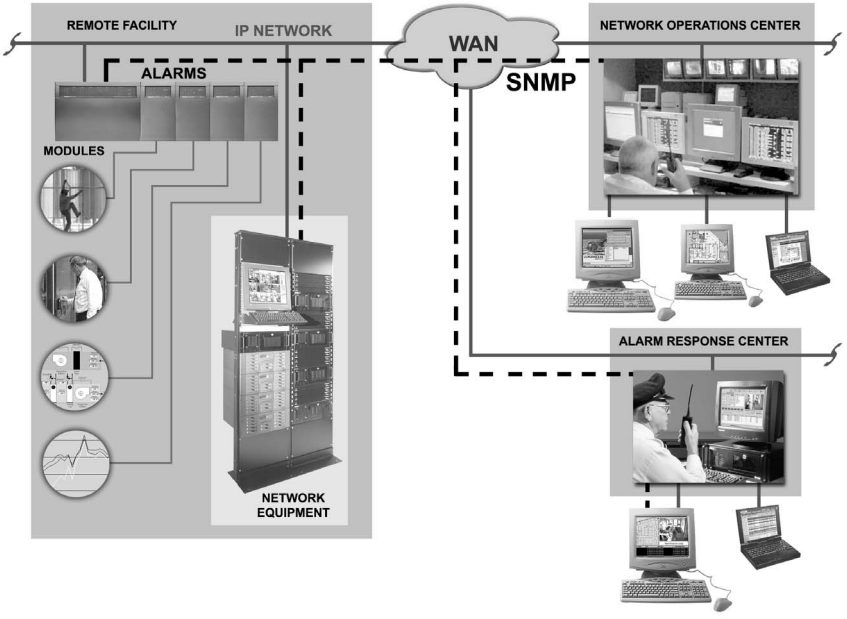
SNMP provides network administrators with a very comprehensive tool for monitoring the health of corporate networks. The more devices on the network that support the SNMP message protocol, the better their ability to manage the system. Previous releases of Continuum controllers did not include this capability.

Version 1.5
As of version 1.5, Continuum CX controllers ((CX99xx, CX94XX, CX9201) can now be located and managed on corporate Ethernet networks with support for SNMP.

Version 1.52
This version enables controllers to allow alarms that have been configured with a CyberStation to be annunciated both to a CyberStation and to an SNMP Network Management software (NMS), such as HP Open View. The CX is an SNMP Client or SNMP Agent. The implementation conforms to SNMP v1 and SNMP v2c.

Our implementation of SNMP resides at the controller level. Many 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 contains the ability to identify itself and to route alarms that it receives to other SNMP devices. There is no single point of failure.

The following diagram graphically depicts our alarming capability:



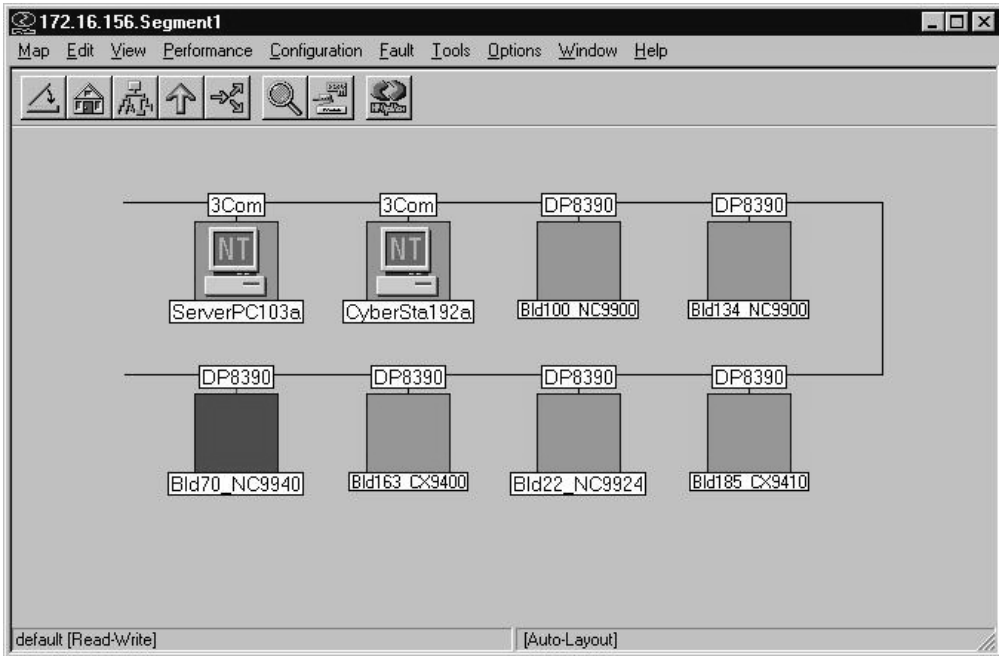
Continuum alarms sent as SNMP traps are fully detailed packets defined by a custom MIB that is loaded into your NMS.

What Do I Need to Make SNMP Work?

Obviously you must have an SNMP managed network.

Your Controllers (CX99xx, CX94xx and CX9201) must be upgraded to version 1.5 or higher.

Continuum CX 1.5 includes SNMP support for identification on the network. With version 1.5 on the controllers, they will show up on the SNMP NMS client. The screen shot below shows Continuum devices that were discovered using the HP OpenView SNMP browser.



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

No configuration of any kind is necessary for version 1.5 Continuum components to be recognized by SNMP management tools.

What Do I Need to Make SNMP Alarming Work?

The following is a simplified overview of the process:

Your Controllers (CX99xx, CX94xx and CX9201) must be upgraded to version **1.52**.

Purchase the SNMP Alarming feature.

Determine if SNMP Alarming is enabled on each CX controller via the Command Terminal Interface.

Determine the community passwords that exist on your SNMP network for GET and SET requests and configure the CX.

Configure each CX controller with the IP addresses of the computers on the network where the alarms are to be sent (NMS address).

Determine the size of the data table within the CX that holds SNMP alarms and configure the CX.

Configure the alarm links (1-8) you want to be echoed as SNMP alarms.

Finally, you must load three Andover Controls-specific MIB files into your network management tool.

The following pages detail each of these steps. Many of them are simple settings made to a single configuration screen viewed via the terminal interface of the CX.

CX Controller Configuration for SNMP Alarming

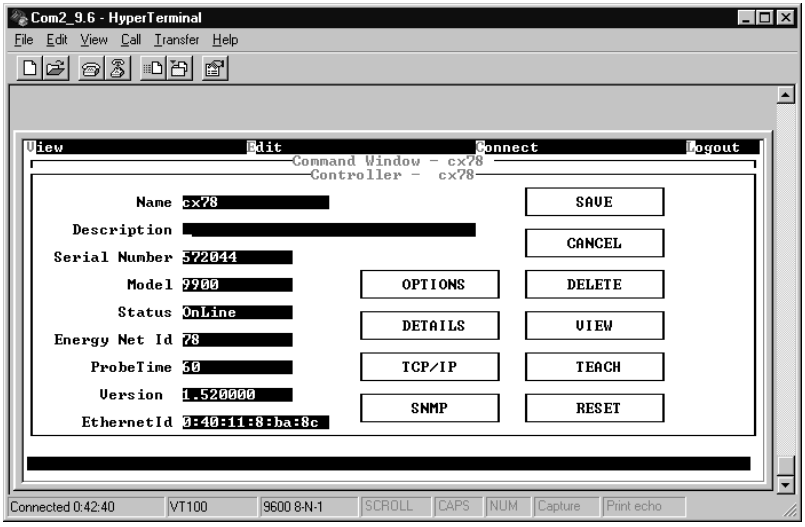
The following steps configure the system to allow echoing of Continuum alarms as SNMP traps.

Initial configuration of the controller is done via the built-in command terminal interface. This interface requires a separate personal computer running a terminal emulator program or a dedicated ASCII terminal. Communications with the Command Terminal firmware are carried out over an RS232 link through any CX Comm port configured as AutoSet.

For more information on the use of this interface and how to connect to the controller to access the command terminal please refer to the Continuum Command Terminal Reference ACC part number 30-3001-843.

Determine if SNMP Alarming is enabled on each CX controller via the Command Terminal Interface.

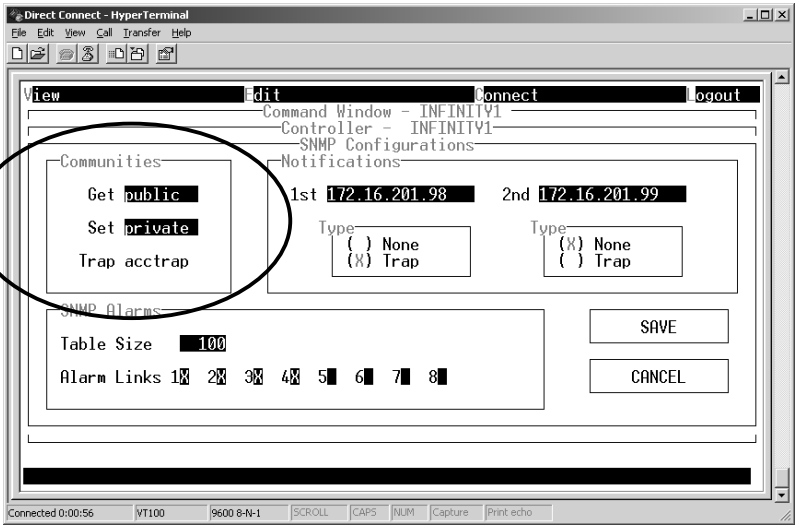
1. Log on to the Command Terminal with administrative privilege
2. Open the Controller's Editor page as shown below.
   If SNMP Alarming is activated in the Controller (it has been purchased), a new button labeled SNMP should appear in the button list.



Another method for checking if the controller is SNMP enabled is to examine the Options tab of the Controller editor in the Continuum CyberStation or in the Command Terminal.

Determine the community passwords that exist on your SNMP network for GET and SET requests and configure the CX

Select the SNMP button to go to the SNMP Configuration page, as shown below.



Configure as follows:

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. These passwords exist in your NMS management scheme. Find out the correct passwords to insert for each entry. Each has maximum length of 8 characters. The default Get Community is *public*, and the default Set community is *private*.

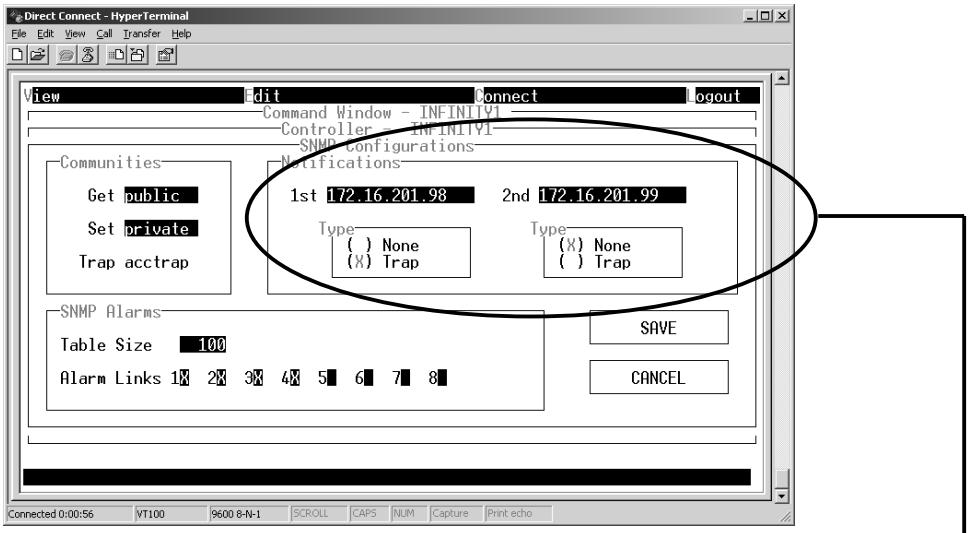
The Trap community is set to *acctrap*. This setting cannot be changed.

The communities set for a Controller apply to that Controller only. Different Controllers may have different communities.

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

Configure each CX controller with the IP addresses of the computers on the network where the alarms are to be sent

Continuum 1.52 allows SNMP alarms to be sent to up to 12 other devices (SNMP NMS devices). The first two of them are non-volatile. Their IP addresses are entered on this form and are saved in the controller's non-volatile memory, and will not be lost even if the Controller resets. The other 10 possible notification target IP addresses are stored in 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.



1. Enter the IP addresses of the first two targets into the area provided as shown.
2. Select the Notification Type for each IP address

   Two notification types are supported:

   None: Alarms will not be automatically delivered to the notification target. However, any NMS device with the ACC MIB files loaded can retrieve alarms from the controller using the GET command.

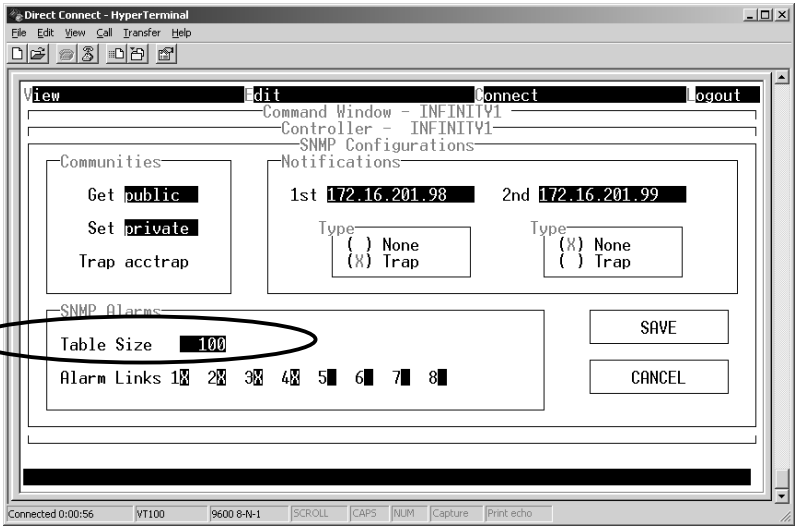
   Trap: Alarms will be automatically delivered to the notification target via SNMPv2c trap.

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

The remaining 10 other device IP addresses must be entered using the SNMP SET command. This operation requires knowledge of your particular NMS software package. Refer to the *Technical Information Appendix* at the end of this document for details on the locations where these IP addresses can be entered.

Determine the size of the alarm data table within the CX that holds SNMP alarms and configure the CX

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. You need to determine how much memory you want to reserve for this table.



Enter the desired table size into the area provided as shown.

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

Some memory use guidelines to use when 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 wasted per entry.

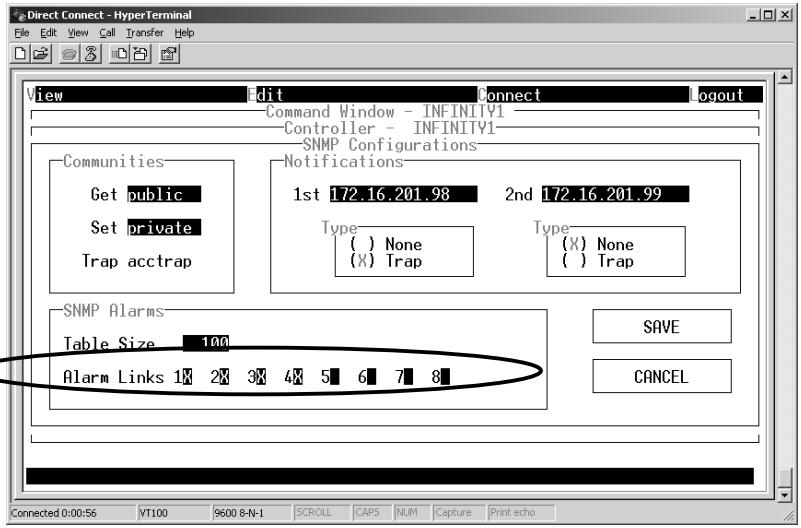
Each SNMP alarm entry that is used, consumes another 114 bytes for the data.

As a safe estimate, determine how many points may 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 the *Technical Information Appendix* for detailed information about how the alarm table works and its structure.

Determine and set 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.



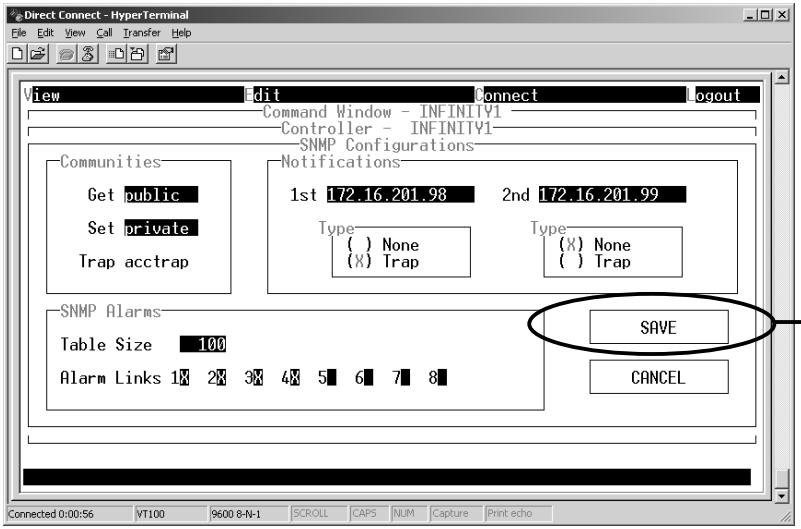
Select the alarm links to echo as SNMP alarms in the area provided as shown.

As the example above shows, alarm links 1 through 4 are selected. In this case, any of the specified alarms (1-4) 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 NMS specified.

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

Upon completion, save the configuration

Once the form is completed you must save the configuration.

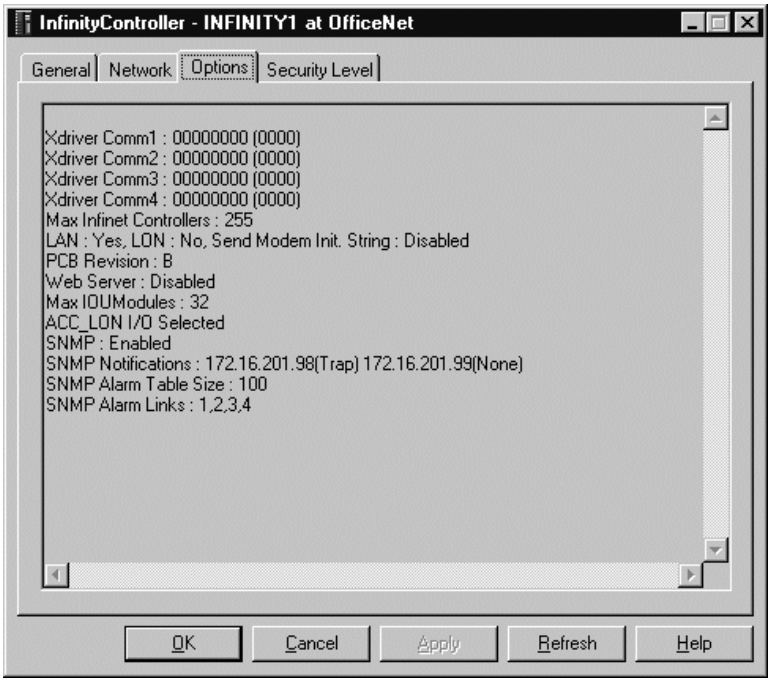


Select the SAVE button.

Checking the CX Configuration

Once the configuration has been saved you can check the options that were selected by observing the Options form of the Terminal Interface.

The page indicates the IP addresses and notification types of the first two notification targets, SNMP alarm table size, and SNMP alarm links. For security reasons, SNMP Communities are not shown on this page.



SNMP NMS Configuration and Testing

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

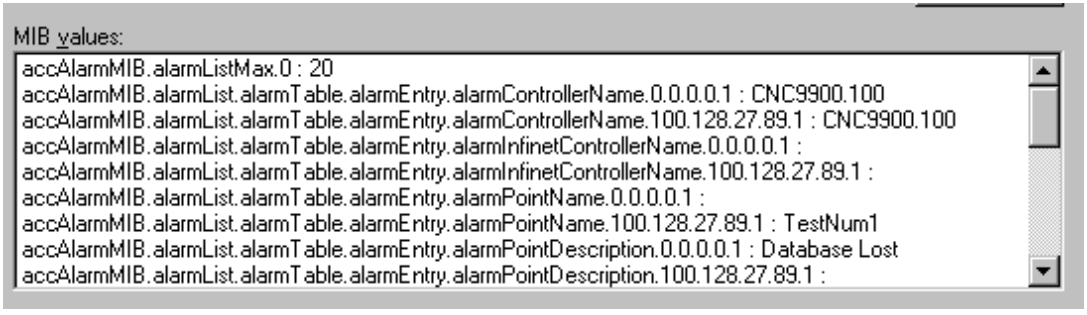
The three necessary MIB files can be downloaded from the Andover Controls website. The file names are:

ANDOVER-CONTROLS-MIB.my	To 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

1. Import them using your NMS software and compile them.

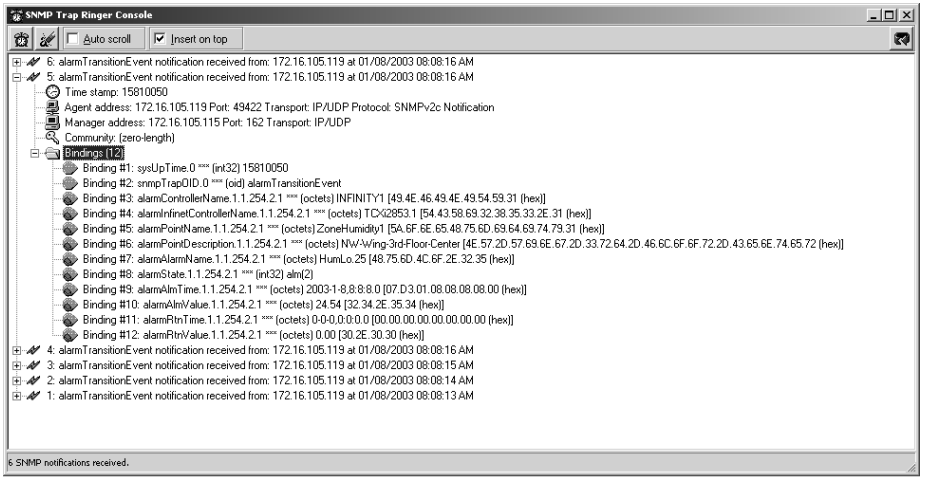
2. Issue a SNMP Query on each sub-level to verify installation of Andover's MIB

   An example of the feedback from this query is shown below:

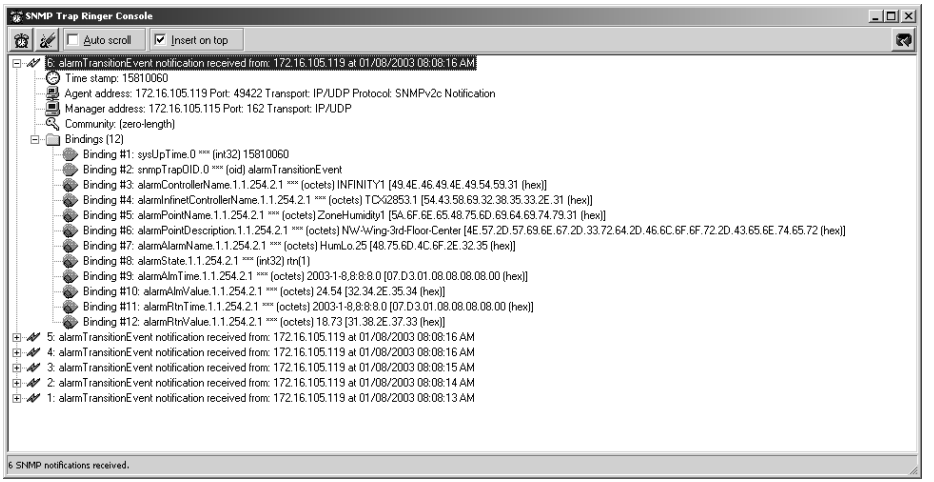


SNMP Alarm Test

1. Create an Expression alarm and attach it to a test Numeric point
2. Put the Point in alarm
3. Open the alarm browser in your NMS tool
4. Observe the following error posting (MG Soft tool shown):



5. Take the Point out of alarm, and observe another entry into the alarm browser.



6. Observe that Alarm Posting is working successfully

Appendix
Technical Information

Continuum SNMP Alarm Table

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.

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

The table entry consists of the following information:

Entry	Description
CX Controller Name	CX Controller Name
Infinet 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	Two values: ALM (2) for in alarm or RTN (1) for returned to normal
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
State	ALM, RTN or null
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 into the table. If Trap notification is enabled, a trap is then sent to the NMS device(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 intrinsic alarm, notifying the NMS that an overflow has occurred, is generated and sent along with the normal notification of the alarm. For complete information on Intrinsic alarms, see the next page.

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 assuming trap notification is enabled.

Continuum SNMP Intrinsic Alarms

There are two alarm conditions that the CX generates

Controller Reset Alarm

SNMP Alarm Table Overflow Alarm.

Note: Intrinsic alarms will not be sent if the notification is set to "none". Also, 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. The following is the description of the fields of the alarm.

Alarm IENAD	00.00.00.00
Alarm Link	1
Controller Name	When in alarm-state, the controller name is the Andover Controls' 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
Point Description	Database Lost
Alarm Name	Controller Reset
Alarm State	State of the alarm, rtn(1) or alm(2)
Alarm Value	0.00
Alarm Time	When 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 at one of the two scenarios:

When a SNMP alarm comes in, the controller can not 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.

When 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. Please refer to the *Configure SNMP Alarming* section of this document for details of how to change SNMP alarm table size.

Following is the description of the fields of the alarm.

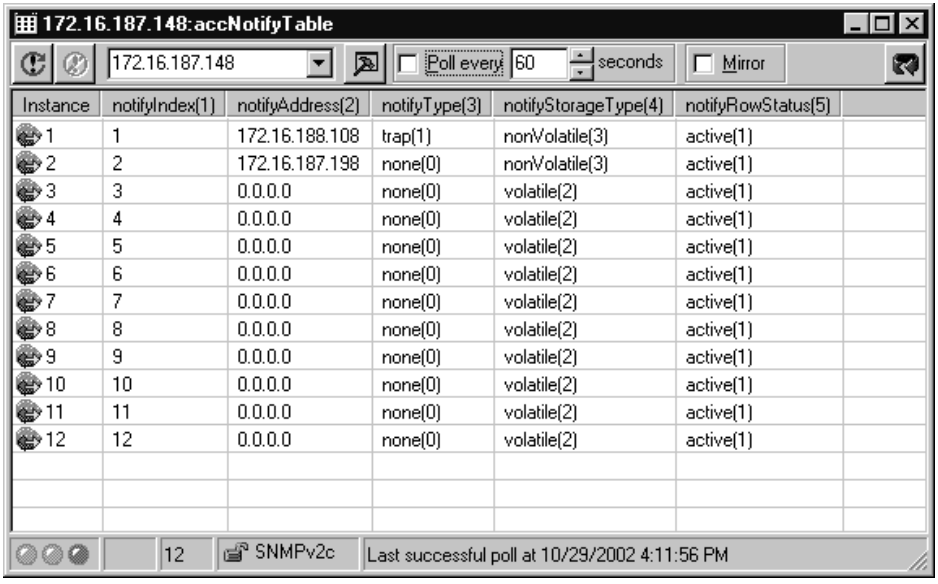
Alarm IENAD	00.00.00.00
Alarm Link	2
Controller Name	Name of the Ethernet Controller
Infinet Controller Name	Null
Point Name	Null
Point Description	SNMP Alarm Table Overflowed
Alarm Name	Alarm Overflow
Alarm State	State of the alarm, rtn(1) or alm(2)
Alarm Value	The SNMP alarm table size when the transition 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 CX 1.52 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 memory, and will not be lost even if the Controller resets. The other notifications are volatile. Their information is saved in the volatile RAM memory. If the Controller resets, their IP addresses will be initialized to 0.0.0.0, and the notification types will be initialized to None.

This section describes the accNotifyTable from which the Network Management System can change the 10 additional target IP addresses.

Actually, all the notification targets, even the two nonvolatile addresses, can be set from network management systems. The screen shot below shows a columnar view of the notification settings using the MG-Soft MIB Browser 7.10.



In this view you can see all the notification settings. The first two 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 also 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 reserved for future use.

Please refer to the documentation of your network management systems for how to read and set MIB entries.

Continuum 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.