

# Real-Time and Historical Event Management

---

## **Dell OpenManage™ Network Manager**

Enoch Suen

Sr. Consultant  
PowerConnect Engineering



November 17, 2003

# Contents

---

|   |    |
|---|----|
| Section 1 .....   | 4  |
| Introduction .....  | 4  |
| Section 2 .....   | 5  |
| Event Monitor .....   | 5  |
| • Switching Between Alarm and Event Viewing Modes .....       | 6  |
| • Setting MAX View Size .....                                 | 6  |
| • Creating Customized Views .....                             | 6  |
| • Adding an IP Source Address Column to the Event Table ..... | 7  |
| • Creating Event Filters .....                                | 9  |
| • The Powerful Right-click .....                              | 11 |
| • Short-Cut to Equipment Inventory .....                      | 11 |
| • Manually Sending Event via Email .....                      | 12 |
| • Automatically Sending an Event via Email.....               | 13 |
| • Sorting Events.....   | 13 |
| Section 3 .....   | 15 |
| Event History .....   | 15 |
| • The Event History Screen .....                              | 15 |
| • Event History Reloaded.....                                 | 16 |
| • Exporting Events .....                                      | 16 |
| Section 4 .....   | 17 |
| Event Forwarding.....   | 17 |
| Section 5 .....   | 20 |
| Conclusion.....   | 20 |

# Figures

---

|  |    |
|--|----|
| Figure 1. The Event Monitor screen. ....                               | 5  |
| Figure 2. The Event View editor. ....                                  | 7  |
| Figure 3. Adding a Source IP address column. ....                      | 8  |
| Figure 4. Resulting view including a Source IP address column. ....    | 8  |
| Figure 5. Event Filter Manager. ....                                   | 10 |
| Figure 6. Defining an Event Filter. ....                               | 10 |
| Figure 7. Right-Click options. ....                                    | 11 |
| Figure 8. Discrete Management screen accessed from Event Monitor. .... | 12 |
| Figure 9. Setting "Auto Send Email" in Event Template Editor ....      | 13 |
| Figure 10. The Event History screen. ....                              | 15 |
| Figure 11. Filter Editor Panel. ....                                   | 17 |
| Figure 12. Filter Selection Panel. ....                                | 18 |
| Figure 13. Scheduling forwarding to a Northbound System. ....          | 19 |

---

## Introduction

Dell's OpenManage Network Manager is configured to listen for SNMP "Traps" on UDP port 162, and interprets all traffic received on that port as network Events. In particular, Network Manager defines any Event that has been classified as significant to be an Alarm. Generally, traps that indicate a traffic disruption or service affecting problem are classified as Alarms. More detail on these default configurations and instructions for modifying the default behavior appear in your Network Manager User's Guide.

Network Manager's Event Service provides a number of powerful, yet easy-to-use features for managing network events, including the Event Monitor, Event History and Event Forwarding. This document provides information on how to use each of these features as well as handy tips for the most commonly performed tasks in each area.



**Note:** In order to effectively use Network Manager's Event Service, you must configure your switches so that Network Manager's server is selected as their "Trap Host". This requires entering the IP address of the server on each switch. One way to do this is to cut-thru into the individual switch from the Equipment Manager screen and another is to use a Group Operation as described in the "Update SNMP Community Strings" section of the "Group Operations With PowerConnect™ Switches" How-To document.



**Note:** For 3324 and 3348 switches, when a trap host is added to an existing read-write SNMP community, access for that trap host will be changed to read-only. Thus, in order to manage that switch using the server just assigned as its trap host, you must manually add the trap host IP address back to the read-write community. One way to do this is to issue the following command either at the switch console or using a telnet cut-thru from the management station:

```
snmp-server community private rw aaa.bbb.ccc.dcd
```

Where "private" is the read-write community string on the switch and aaa.bbb.ccc.dcd is the IP address of the management station.

## Section 2

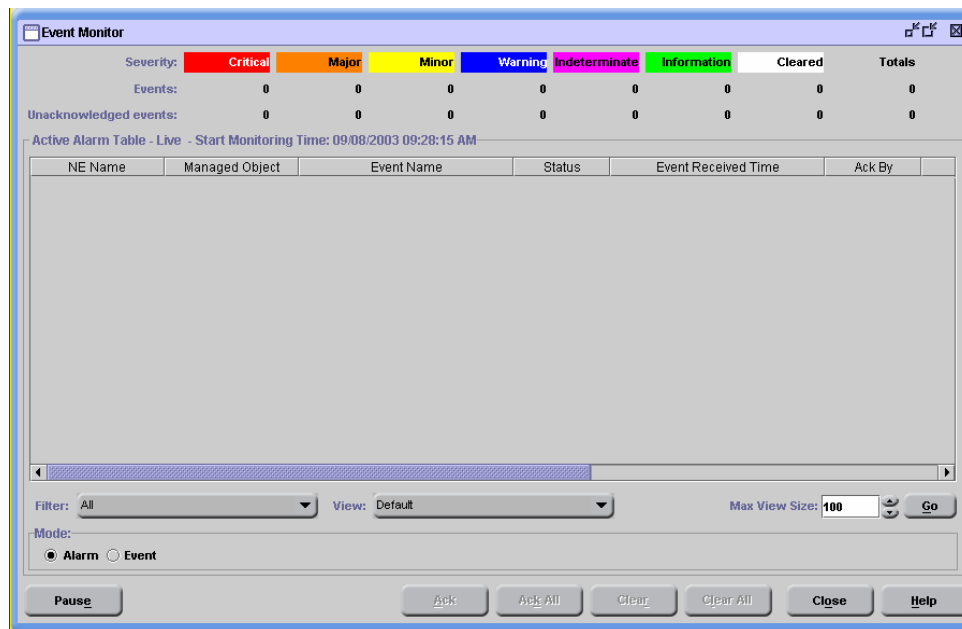
# Event Monitor

Network Manager's Event Monitor displays a real time view of events as they are received by the server. To open the Event Monitor, select **Event Services -> Event Monitor** on the navigation panel or **File->Open->Event Services->Event Monitor** from Network Manger's menus.



**Note:** *Event Monitor displays only those events that have occurred since the Event Monitor window was opened.*

The default Event Monitor window is shown in Figure 1. The remainder of this subsection will provide a general description of the window layout. The use of its various features will be described in the following subsections.



**Figure 1. The Event Monitor screen.**

The area at the top of the window provides you with a concise summary of the numbers of each event type and number of acknowledged events of each type present in the current view. If your view uses a filter to focus on a subset of events, the overall numbers will reflect the number of filtered events. The default event types are Critical, Major, Minor, Warning, Indeterminate, Information and Cleared. On the following line, the type of screen you are viewing (in this case the active alarm table) is shown along with the time the monitoring started. This information is important since you will need to use Event History to look at events/alarms that arrived prior to the monitoring start time. The presentation area below provides several columns that contain information about each of the displayed alarms/events. The most commonly seen alarms/events in this area of the screen are the MIB II traps; linkUp, linkDown, coldStart, warmStart,

“authentication Failure” and “Spanning Tree topology change”. The columns in the presentation area can be rearranged and the information displayed can be modified as described later in this document. Below the presentation area, tools are provided that allow you to select filters to apply to your view, change the view itself, set the maximum view size and switch from alarm to event viewing. The area at the bottom of the screen provides buttons that allow you to pause activity on the screen, acknowledge events, clear events, close the window and get help on Event Services. Details for many of these capabilities follow.

- **Switching Between Alarm and Event Viewing Modes**

By default, the Event Monitor is brought up in Alarm view. This view shows only events for which a fault condition exists. As with most Network Manager views, the information can be filtered to show a subset of the overall alarms that are of particular interest to the user.

Clicking on the “**Event**” radio button at the lower left screen changes to the Event mode. The Event view is a superset of the Alarm view and includes informational events from all managed devices in addition to alarms. This view can also be filtered.



**Note:** When you change from Alarm to Event mode or vice-versa, the window is cleared and monitoring re-starts at the time of the switchover. Thus, if you leave the Alarm window to look at Events and then return, the Alarm window will be empty and only alarms that arrive after you switch back will be displayed. To view events that occur in the past (for example, the ones that were visible before you switched modes), use Event History. You can open both Event Monitor and Event History simultaneously.

- **Setting MAX View Size**

By default, the Alarm and Event views are limited to 100 items. More information is kept in the database and, if you believe that more than 100 Alarms may be active at any one time, you can increase the maximum number displayed by adjusting the **MAX View Size** which is located in the lower right part screen. The table size may be increased up to a maximum of 500 entries. Once the table size has been changed, you will need to click the **Go** button immediately to the right of the **MAX View Size** field in order to refresh the screen.



**Note:** When changing the **MAX View Size**, clicking the **Go** button will clear the screen contents and cause monitoring to re-start. Alarms and Events previously visible in the Event Monitor window can be accessed through Event History.



**Note:** If the number of Alarms or Events being viewed exceeds **MAX View Size** the oldest items will be dropped from the list in order. Although those items will no longer be viewable in the Event Monitor window, they can be accessed through Event History.

- **Creating Customized Views**

Customized views can be created by simply re-arranging columns in the event tables directly. Just position the cursor to the column header and drag the column to the desired location. To save your view, select File->Save View. The Event View Editor appears (see Figure 2), populated with the current view. You can make any additional changes, and then click Save to store the new view. It will then appear in the View drop-down menu.

To apply the new view, select it in the **View** drop-down menu located below the event table.

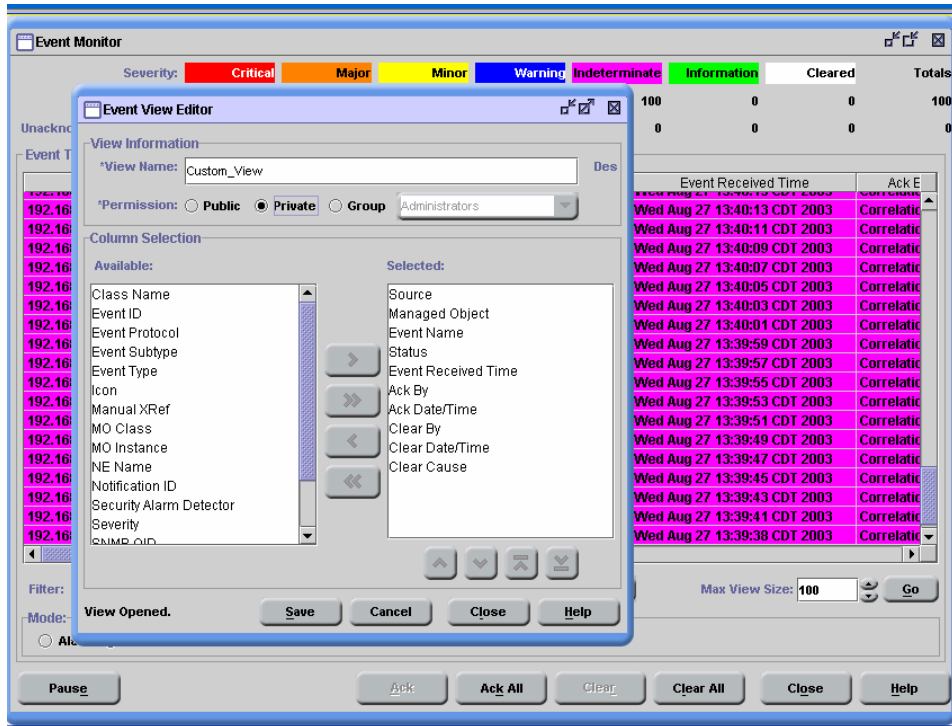


Figure 2. The Event View editor.

- **Adding an IP Source Address Column to the Event Table**

The default view does not include the event source IP address as a column in the table. This information is often used by network administrators to identify undiscovered devices so it is a useful column to add to your view. To add this column, select any event, then right-click on it and select **Insert Column -> Source** on the menu (see Figure 3); the Source column will then be added to the table (see Figure 4). Now you are able to view the source IP address for every alarm/event in the table.

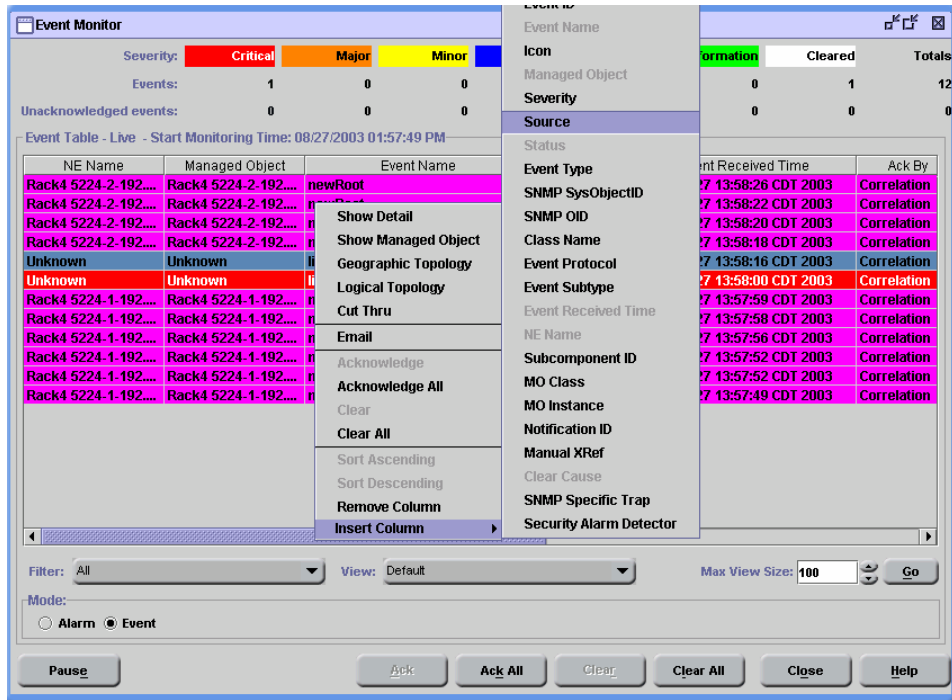


Figure 3. Adding a Source IP address column.

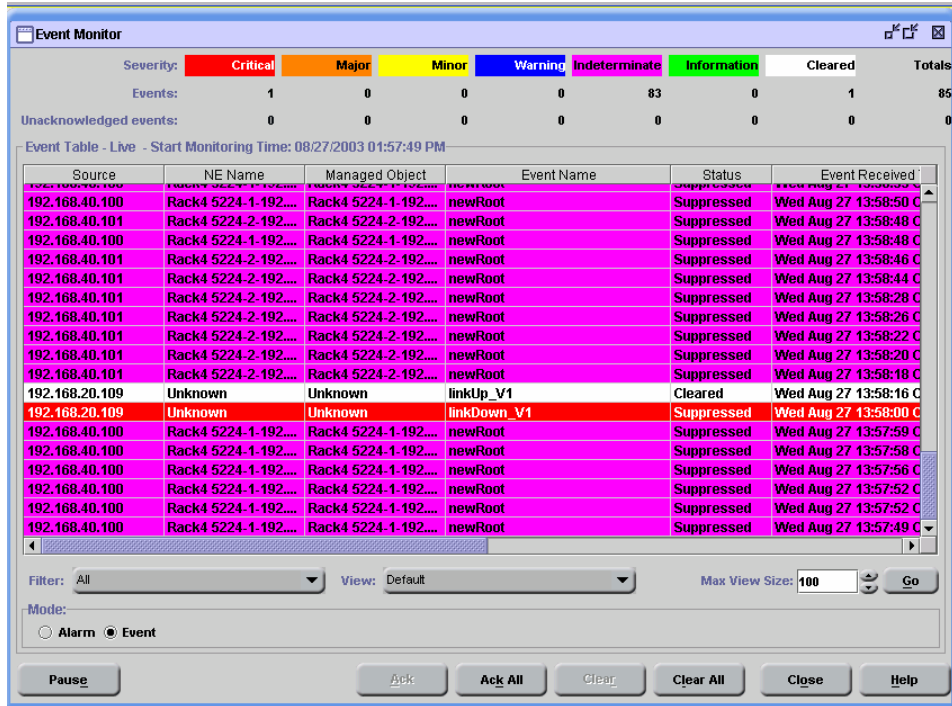


Figure 4. Resulting view including a Source IP address column.

- **Creating Event Filters**

Event Filters are useful in focusing on those events of interest from a management perspective. Select **File->Filter Manager** to access the Event Filter Manager (see Figure 5), then click the **'New'** button to create an event filter. The **File->Filter Manager** menu item is only visible when you are in the Event Monitor or Event History view.

In order to create a valid filter you must enter at least a **Name** and one filter criterion. Filter criteria are built up by selecting an **Attribute**, a **Connector** and an **Operator** and then clicking the **Add** button to add the selection to your overall filter criteria. You can build up a logical filter construct by repeating the **Add** operation. Selecting a particular attribute will bring up an entry field appropriate to that attribute. For example, Figure 6 shows the selections available for the "Event Type" attribute.

Valid Connectors are:

|     |    |
|-----|----|
| AND | OR |
|-----|----|

Valid Operators are:

|                               |                            |
|-------------------------------|----------------------------|
| = (Equals)                    | <> (Not Equals)            |
| > (Greater Than)              | < (Less Than)              |
| >= (Greater Than Or Equal To) | <= (Less Than Or Equal To) |
| LIKE                          |                            |

Valid Attributes are:

|                    |                         |
|--------------------|-------------------------|
| Ack By             | Ack Date/Tim            |
| Class Name         | Clear By                |
| Clear Cause        | Clear Date/Time         |
| Event ID           | Event Name              |
| Event Protocol     | Event Received Time     |
| Event Subtype      | Event Type              |
| Icon               | Managed Object          |
| Manual XRef        | MO Class                |
| MO Instance        | NE Name                 |
| Notification ID    | Security Alarm Detector |
| Severity           | SNMP OID                |
| SNMP Specific Trap | SNMP SysObjectID        |
| Source             | Status                  |
| Subcomponent ID    |                         |

The variety of attributes available allows very complex filters to be constructed. Once you have defined your filter you can save it and make it available for use by selecting **File->Save** on the menu bar or selecting the "floppy disk" save icon on the icon bar. To apply the new filter to your view, use the **Filter** drop-down menu located below the event table. Before the filter is applied, Network Manager

warns you that changing the filter clears existing events from the display. If that is not acceptable, selecting **No** will cancel the filter application.

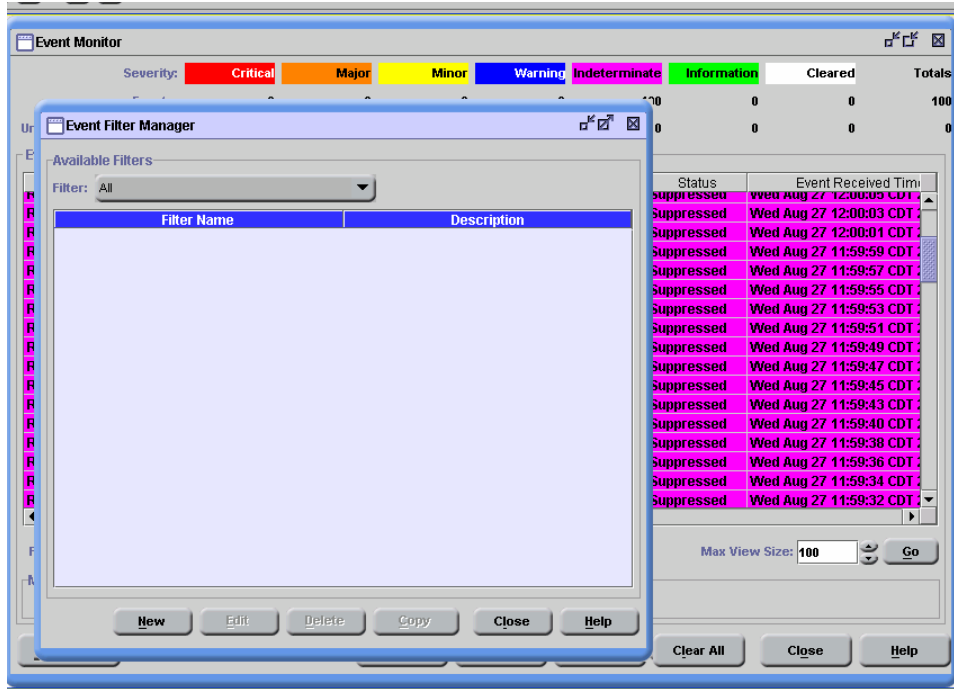


Figure 5. Event Filter Manager.

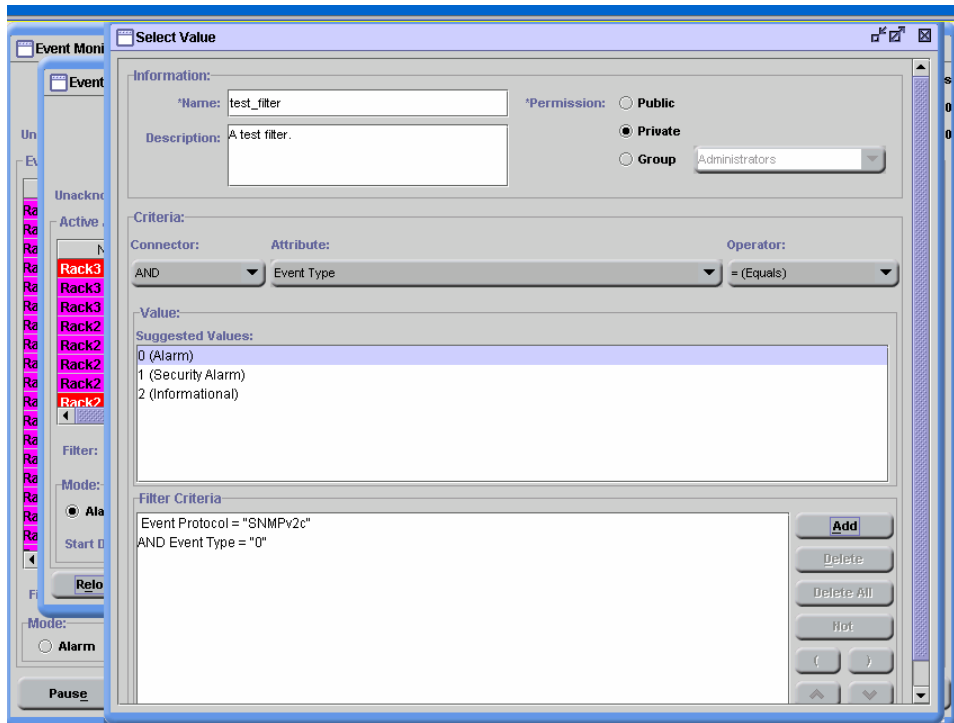
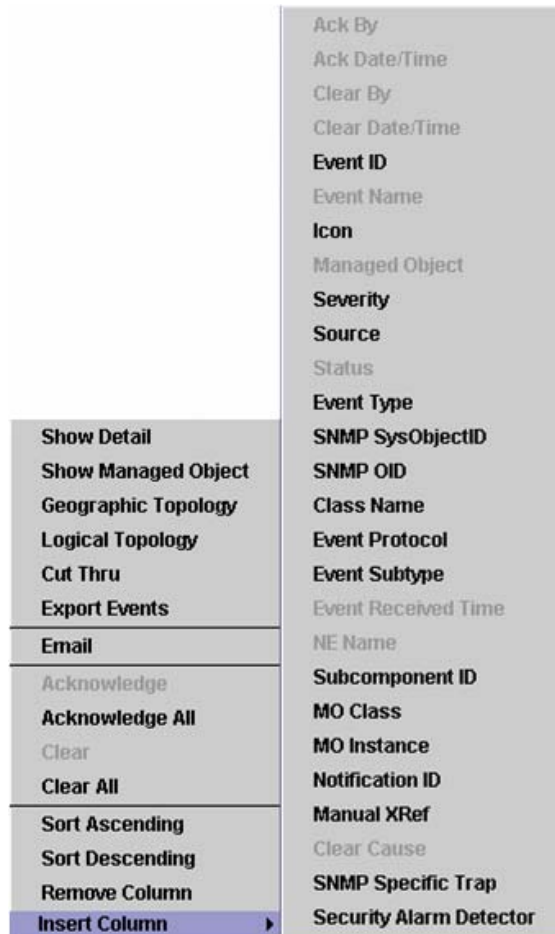


Figure 6. Defining an Event Filter.

- **The Powerful Right-click**

Selecting an event in either the Alarm or Event view and right-clicking enables you to access functionality that will help to diagnose, trouble-shoot, process and clear events. Figure 7 shows the selections available following a right-click operation. Since the Insert Column option spawns a second menu, that is also shown in the Figure. The following subsections present details for a number of the tasks that can be accessed through this feature.



**Figure 7. Right-Click options.**

Please reference the Network Manger User's Guide "Event Monitor and History" chapter for complete descriptions of all options.

- **Short-Cut to Equipment Inventory**

You can access the discrete management screen for a switch by right-clicking on a selected event in the event table and selecting **Show Managed Object** from the menu. This is a short cut to the discrete management screen (see Figure 8).

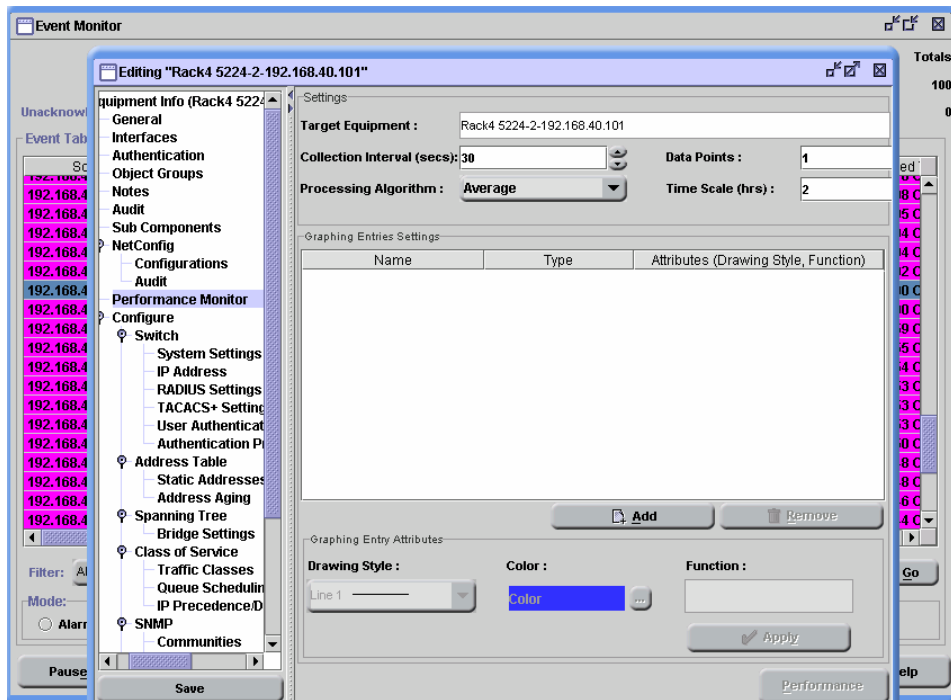


Figure 8. Discrete Management screen accessed from Event Monitor.

- **Manually Sending Event via Email**

To email an event to a specified recipient, simply select an event from the event table, right-click on it, and select the **Email** menu item. You will be asked to enter a full Email address – for example, [john.doe@xyzco.com](mailto:john.doe@xyzco.com).



**Note:** Before using this feature, you need to ensure that the host computer has a properly set up mail server. Additionally, the SMTP host and the return address should be configured on the Network Manager server by modifying the file:

`Dell\OpenManage\NetworkManager\lowareapps\redcell\lib\redcell.properties`

Search for the following lines in the file and set to your SMTP host and return address appropriately. The parameters specified below are purely an example.

```
# Set to the SMTP host for sending e-mail from within
RedCell
# (defaults to localhost)
#redcell.smtphost=localhost
# This is an example...
redcell.smtphost=smtp.dell.net

# Set to the return address for messages from RedCell
# defaults to RedCell@localhost
#redcell.returnaddress=redcell@domain.com
redcell.returnaddress=netadmin@dell.com
```

- **Automatically Sending an Event via Email**

You can configure Network Manager to automatically send an email notification to a specified user when a certain event is received.

To configure this behavior, select **Event Services -> Event Template Manager** on the navigation panel. This selection will bring up the Event Template manager (shown in the background of Figure 9) showing all the events and alarms that are understood by Network Manager. Select the event for which you wish to configure automatic email notifications and click the **Edit** button. This will bring up the Event Template Editor screen shown in Figure 9. Click on the **Email** tab, and within the Email screen, click on the ellipsis button “...” to display a list of defined users. Select a name from this list and click **OK**. The **Subject** line and **Message** box should be filled in so that the recipient has a clear indication of why they are receiving the message. Once you are happy with the content, select **File->Save** or use the “Floppy Disk” save icon to save the configuration.



**Note:** Before using this feature, ensure that the selected user has an email address specified. To do this, use the **Settings->Permissions->User Manager** menu to open the User Manager, select the user in question and click the **Open** button. On the following screen, ensure that a primary email address has been entered on the **General** tab. Save changes if necessary and return to the Event Template Editor.

The event template editor provides a very powerful tool for setting up additional features such as alarm/event correlation and thresholding. Please see the Network Manager User’s Guide for details on these features.

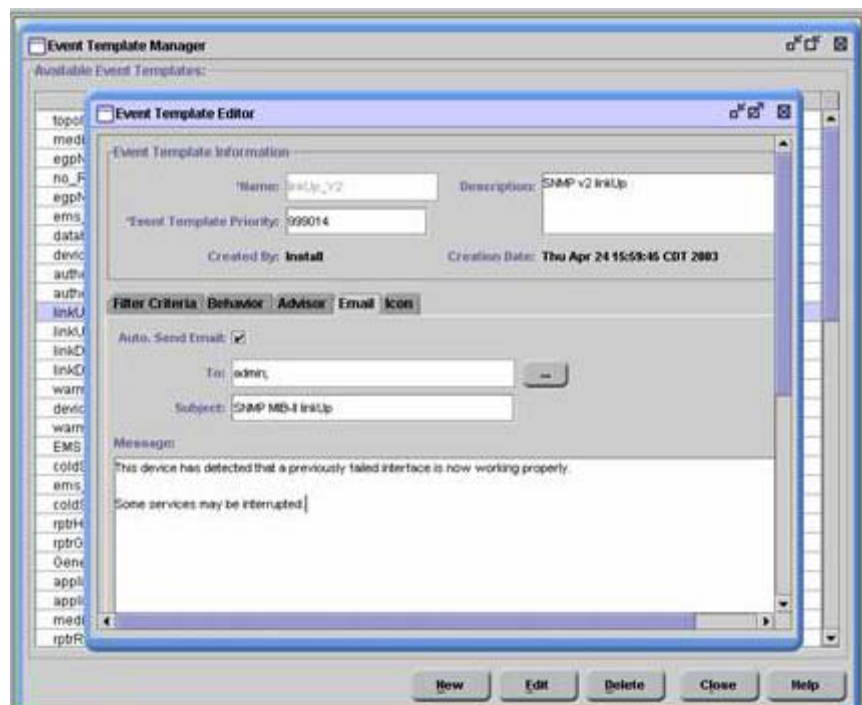


Figure 9. Setting “Auto Send Email” in Event Template Editor

- **Sorting Events**

You can sort the event table in ascending or descending order based on the value in a column. Select an event from the table, position the cursor to the

column you want to sort by, right-click on it, and select either the **Sort Ascending** or the **Sort Descending** item.

## Event History

Event History allows the display of alarms and events that have occurred in the past by retrieving them from the Network Manager database. The user interface shares many common characteristics with the Event Monitor so this section describes only those features that are unique to the Event History service. To view event history, select **Event Services -> Event History** on the navigation panel.

- **The Event History Screen**

The Event History screen (shown in Figure 10) is similar to the Event Monitor screen with a few exceptions. Since the information displayed in this screen is drawn from the database, a mechanism for selecting the start and stop time of the display is provided.

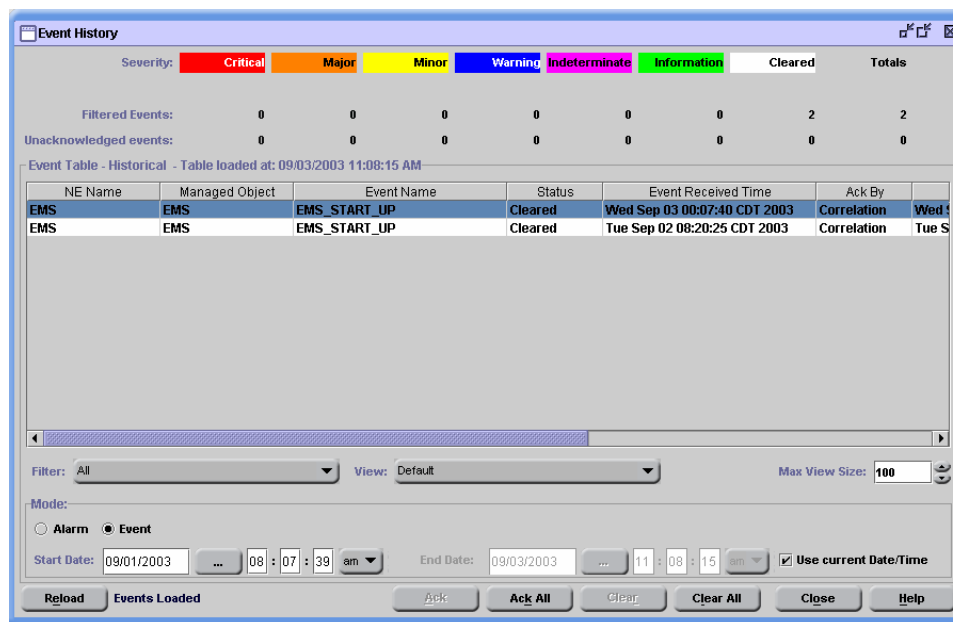


Figure 10. The Event History screen.

As with the Event Monitor, you can create a new filter or select an already existing filter to focus on a particular subset of events or alarms (filters created in Event Monitor are available within Event History and vice-versa) and select a view appropriate to your needs. You can also select Alarm or Event mode and the Max View Size in the same way as for Event Monitor.

The Start Date and End Date fields allow you to further refine the scope of data retrieved from the database. By default, the End Date is grayed out and the Use current Date/Time box is selected. This has the effect of picking up the latest entries in the database when the Reload button is clicked. Also by default, the Start Date is set to the current time minus 3 hours.



**Note:** You can configure a different default Start Date value by changing the following parameter in the system property (located at **Settings->Configuration->Control Settings in Properties tab**)

`Redcell.assure.fault.alarmwindow.history.starthoursdiff`

You can set the start and end dates by typing directly into the fields, or you can use the “...” button to bring up a calendar pop-up to aid in your selection. Note that the End Date field is only enabled when the Use Current Date/Time box is not selected. Start and stop times must be entered directly into the provided fields and AM/PM selection is handled by the drop-down menu beside the time field.

- **Event History Reloaded**

Clicking the **Reload** button causes Network Manager to pull information from the database based on the **Filter**, **Start/End Date** and **Max View Size** selected and populates the event table with that data. When the Event History screen is opened, no information is displayed so you must click **Reload** in order to see any of the historical events.

You also need to click the **Reload** button to refresh the view after any change in filtering, the selected view, Start Date/End Date, Alarm/Event mode or the Max View Size.



**Note:** It is important to note that Event History does NOT give you a real-time view of alarms and events. You will not see new traps as they are received by the Network Manager using this view. Event Monitor and Event History can both be active at the same time allowing you to monitor the real-time view of the network while analyzing past events.

- **Exporting Events**

In order to export events, simply select an event then right-click and choose **Export Events** from the menu. This creates a comma delimited text file you can use in other programs. All events currently displayed in Event History (up to **Max View Size**) are written to the file. Note that if you have rearranged the columns after selecting the view this is not reflected in the export file – it maintains the default column order of the current view at the time of export.

## Event Forwarding

Forwarding events, also known as sending events to the Northbound interface, allows Network Manager to transfer selected events to other Operational Support Systems. This is useful in a distributed management environment. To start the service, select **Event Services -> Northbound Manager** on the navigation panel. The steps to forward events are as follows:

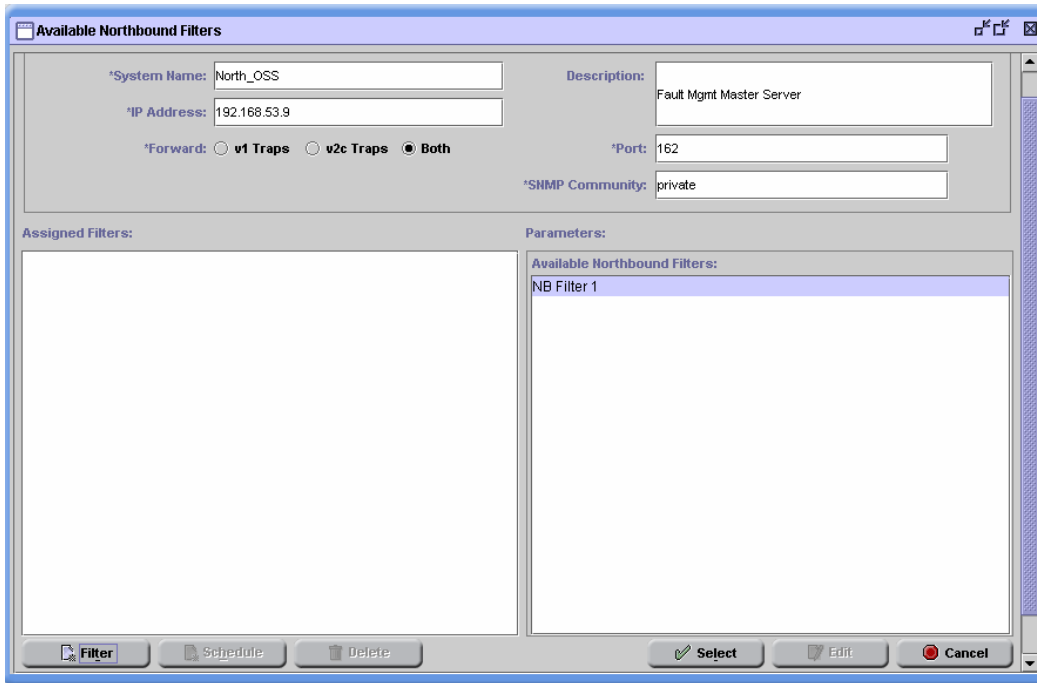
If you have not already done so, you will need to create a forwarding filter that designates what kind of events you want to forward. Select **File-> New->Northbound System Filter** to display the Filter Manager screen, then click **New** to open the Filter Editor Panel (see Figure 11).. Fill out the **Name** field, and compose criteria for the filter as described in the “Creating Event Filters” section. Once you have defined the desired filter, select **File->Save** or click the floppy disk icon to save the filter definition.

The screenshot shows the Filter Editor Panel window. It has a title bar with the text 'FilterEditorPanel' and standard window controls. The main area is divided into several sections:

- Information:** Contains two text input fields. The first is labeled '\*Name:' and contains the text 'NB\_Filter'. The second is labeled 'Description:' and contains the text 'Northbound Filter'.
- Constraints:** Contains three dropdown menus. The first is labeled 'Connector:' and is set to 'AND'. The second is labeled 'Attribute:' and is set to 'Severity'. The third is labeled 'Operator:' and is set to '= (Equals)'.
- Value:** Contains a list box with the following items: 'Cleared', 'Critical', 'Indeterminate', 'Information', 'Major', 'Minor', and 'Warning'. The 'Critical' item is currently selected and highlighted.
- Criteria:** Contains a text area with the text 'Severity = Critical'. To the right of this text area are four buttons: 'Add', 'Delete', 'Delete All', and 'Hot'. Below these buttons are two small circular icons, one containing a left parenthesis '(' and the other containing a right parenthesis ')'.

Figure 11. Filter Editor Panel

In order to create a new Northbound system definition which tells the application how to communicate with the northbound system, what events to send, and when to send, click on **New** in the Northbound System Manager main screen. Begin by filling in a System Name (required for local reference), description, the northbound system's IP address and the port that system will be expecting to receive traffic over. At this point, you will need to tell Network Manager what filter to apply in determining what traps to forward by clicking on the filter button at the lower left of the screen. The resulting screen is shown in Figure 12.



**Figure 12. Filter Selection Panel.**

This lets you pick one or more filters to associate with the northbound system. When you highlight a filter that appears in the right pane of this screen and click the **Select** button, the filter moves to the left side of the screen, and its scheduling parameter input screen replaces the list of available filters as shown in Figure 13. You can select **Always On** with the checkbox, or program a Start and End Time in the right panel. If you have assigned multiple filters to the northbound system, you can apply a schedule to a particular filter by selecting the filter in the left pane, clicking the **Schedule** button at the bottom of the pane, selecting the appropriate time interval in the scheduling pane and finally clicking **Select** at the bottom of that pane. Multiple schedules can be applied to a single filter so, for example, you can use a filter to forward traffic to a northbound system from 9AM until 5 PM, Monday and Tuesday and again on Saturday and Sunday. Once you are satisfied with the filtering set-up, simply click the **Start Forwarding** button at the lower left of the Northbound System Editor to start forwarding traps to the defined northbound system.

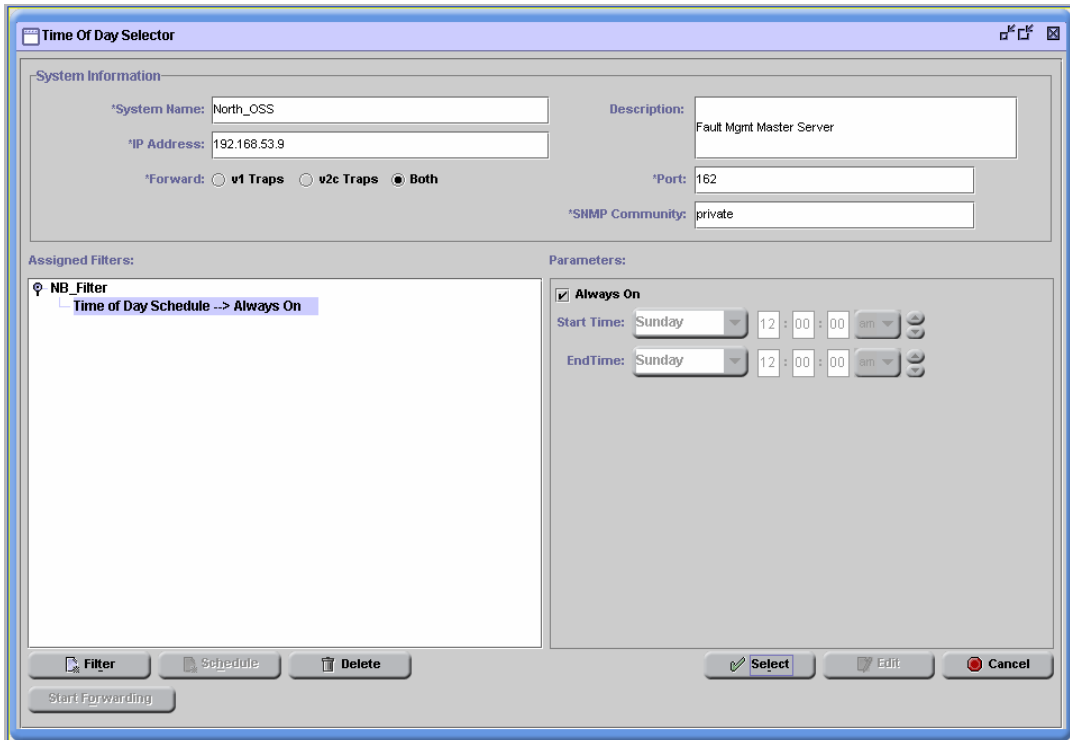


Figure 13. Scheduling forwarding to a Northbound System.

---

## Conclusion

Dell's OpenManage Network Manager delivers powerful features for managing SNMPv1 or v2c network events. Most tasks can be performed by end users with only a few mouse clicks. You need to set up trap host table properly in the switch before enjoying the benefits offered by Event Services. More details on using Event Services can be found in the Network Manager User's Guide.

---

THIS HOW-TO GUIDE IS FOR INFORMATIONAL PURPOSES ONLY, IT MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

Dell, OpenManage is a trademark of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell disclaims proprietary interest in the marks and names of others.

©Copyright 2003 Dell Inc. All rights reserved. Reproduction in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

Information in this document is subject to change without notice.