Using Threshold Manager

Threshold Manager is a CiscoView-launched threshold management application that allows you to set thresholds and retrieve event information. Threshold Manager relies on RMON (Remote Network Monitoring) alarm and event groups supported in Cisco routers and switches. A working knowledge of RMON is required for using this application.

Threshold Manager provides an easy-to-use interface to access device-specific threshold settings. You can set thresholds for network devices using Cisco-provided, predefined default policies. These policies can be applied automatically to target devices. Threshold Manager also supports detailed customization of threshold settings.

For a list of supported devices refer to Chapter 1, “Introducing CiscoView,” or the Readme file and the release note. Threshold Manager also has online help.

Note There are slight differences in the depiction of Threshold Manager when you use a UNIX platform or a Windows platform. However, functions and procedures are the same except where differences are indicated. For UNIX users, a three-button mouse is a prerequisite to performing some functions.

This appendix contains the following sections:

- Introducing Threshold Manager Terms
- Starting Threshold Manager
- Starting Threshold Manager from the Command Line
- Managing Events
- Managing Thresholds

- Using Policy Files
- Starting a New Threshold Manager
- Filtering Profiles
- Troubleshooting Threshold Manager

Introducing Threshold Manager Terms

To understand Threshold Manager, you should be familiar with the terminology associated with this application. This section defines common terms you see throughout the interface.

What Is a Threshold?

A *threshold* defines the range in which you expect your network to perform. If thresholds exceed or go below the expected bounds, you examine these areas for potential problems. You can create thresholds for a specific device.

What Is a Policy?

A *policy* is predefined configuration data that specifies the condition for triggering a threshold event. Threshold Manager uses policies to set thresholds in a Cisco router or switch.

What Is a Policy File?

A *policy file* is a collection of one or more policies that defines threshold values for specific MIB variables. Each threshold policy is associated with a single SNMP MIB variable type. If a policy specifies an interface type, Threshold Manager applies the policy to the matching device interface. If the policy does not specify an interface type, the application applies the value to all device interfaces. Multiple policy files can be enforced in a device or against a specific interface on a device.

Two types of policy files are available:

- Default: a set of generic preconfigured thresholds that can be used for all supported devices. Cisco Systems provides 18 default policy files that reflect a set of commonly monitored SNMP MIB variables and can be used as is or modified to meet the needs of a specific network. These policy files follow the naming convention <default policyname>*.thd*. For more information on default policies, see "Using Default Policy Files" later in this chapter.
- Customized: a set of configured thresholds that deviate from the default policies. Users create a customized policy when it is necessary to trigger events not covered by a default policy. These policy files follow the naming convention <MIB_variable>*.thd*. For more information on customized policies, see "Customizing Policy Files" later in this chapter.

  For more information on MIBs, refer to "Introducing CiscoView" section in the "Introducing CiscoView" chapter.

What Is a Profile?

A *profile* is a group of threshold policy files that cover a specific management area. Threshold Manager supports four profile types:

- System contains the default policy files that monitor device configuration information. Policy files of this type can include tracking the amount of free memory in the device, the number of buffer failures resulting from lack of memory, or the number of times the CPU surpasses a capacity limit.
- Interface contains the default policy files specific to an interface. Policy files of this type can include tracking the number of time the interface detected a carrier transition or the number of times the interface internally reset.
- rmon_EtherStats contains the policy files specific to the Ethernet card. Policy files of this type can include the total number of fragmented packets received or the total number of collisions detected on a specific Ethernet segment.
- Customize contains all user-defined policy files regardless of group.

What Is an Alarm?

An *alarm* is a list of parameters to be watched and pointers to events that are triggered when defined values cross a given threshold. These parameters and pointers are defined by the RMON alarm group. For instance, you define an alarm by picking a variable, such as the number of Ethernet collisions, plus a time interval, such as 1 second, and a threshold, such as 60 collisions. Given this scenario, an alarm is generated when the number of Ethernet collisions exceeds 60 in 1 second.

What Is an Event?

Alarms and events go hand in hand. An *event* defines the action triggered as a result of an alarm. For example, when the number of collisions on an Ethernet segment exceeds 60 per second, the corresponding event can cause a trap message to be sent to one or more management stations. Events are defined by the RMON event group.

An event is generated by the RMON agent, which could be triggered by a threshold crossing. An event can be signaled as a trap, a new entry in the RMON MIB log table, both, or neither. Threshold Manager displays all events captured from the log table of the RMON agent and correlates threshold-related events to the user-configured threshold policies.

What Is an Agent?

An *agent* is a process in the device that handles SNMP requests.

Starting Threshold Manager

After Threshold Manager is installed, the CiscoView menu has an additional pulldown menu item called **Tools**.

Threshold Manager is available only when CiscoView is invoked on devices that support RMON and have a Cisco IOS image with RMON support built into it. The Tools menu is always enabled for non-Cisco IOS devices such as Catalyst switches.

To start Threshold Manager from CiscoView, complete the following steps:

Step 1 Go to CiscoView - Main window.

Note For information on device display setup requirements, starting CiscoView, and opening an installed device, refer to Chapter 1, “Introducing CiscoView.”

Step 2 Select **File>Open Device**.

Step 3 Enter the IP address or host name from where Threshold Manager has to be invoked in the Host field.

Step 4 Enter the Read community string.

Step 5 Enter the Write community string.

Step 6 Click **OK**.

Step 7 Select **Tools>Threshold Manager** from the CiscoView menu bar.

The Threshold Manager window events list appears.

Note For procedures on starting CiscoView, refer to Chapter 1, “Introducing CiscoView,” *CiscoView CD Installation Instructions* for UNIX users, or *CiscoWorks Windows CD Installation Instructions* for Windows users.

Starting Threshold Manager from the Command Line

To start Threshold Manager from the command line, do one of the following:

- If you are using UNIX, enter the following command at the prompt:

```
$NMSROOT/etc/cview/devices/Threshold-Mgr/tm [-I IP-address [-n host_name
[-p /$NMSROOT/etc/cview/devices/Threshold-Mgr [-r
read_community_string [-w write_community_string [-e retry_count [-m timeout [-f
refresh_interval]]]]]]]]
```

where:

-I *IP-address* — is the IP address of the device you want to monitor.

or use

-n *host name* — is the host name of the device.

-p — is the directory where Threshold Manager is installed.

-r *read_community_string* — is an SNMP password. The default is public.

-w *write_community_string* — is an SNMP password. The default is private.

-e *retry count* — is the number of times Threshold Manager sends a request to an unreponsive device. The default is 3.

-m *timeout* — is the amount of time, in seconds, Threshold Manager waits before issuing another retry. The default is 10 seconds.

-f *refresh_interval* — is the time, in seconds, the Threshold Manager window events list refreshes. The default is 360 seconds.

- If you are using Windows NT 4.0 or Windows 95, do the following:

Step 1 Locate TM.EXE in Explorer.

Step 2 Start Threshold Manager and select **File>Open**.

Step 3 Enter **`TM.EXE`** **-I** *IP_Address* or **`TM.EXE`** **-n** *host_name* in the command field

where:

-I *IP-address* is the IP address of the device you want to monitor.

or use

-n *host_name* is the host name of the device. The default is the local machine.

-p is the directory where Threshold Manager is installed.

-r *read_community_string* is an SNMP password. The default is public.

-w *write_community_string* is an SNMP password. The default is private.

-e *retry count* is the number of times Threshold Manager sends a request to an unreponsive device. The default is 3.

-m *timeout* is the amount of time, in seconds, Threshold Manager waits before issuing another retry. The default is 10 seconds.

-f *refresh_interval* is the time, in seconds, the Threshold Manager window events list refreshes. The default is 360 seconds.

Managing Events

When you start Threshold Manager, the Threshold Manager window events list appears. The Threshold Manager window events list displays threshold events stored as RMON log records in the managed device. This window also displays the name of the target device as either the host name or IP address. The name depends on how you identified the device when you launched Threshold Manager or CiscoView.

Threshold Manager correlates the event information with an existing policy by comparing the object identifier (OID) of the event with the value of the alarm variable in the policy configuration file. If a match occurs, Threshold Manager complements the event display fields of the logged entry with information from the policy file. If no match occurs, Threshold Manager displays a value of *undefined* in those fields that would be completed by the policy.

Each event occupies a single line in the Threshold Manager window events list and is displayed until one of the following situations occurs:

- You delete the event.
- Another user managing that device deletes the event.
- The RMON agent reaches its event limit and records over the event or deletes it.

Viewing Threshold Events

Select **View>Retrieve Events**.

The Threshold Manager window contains the logged events retrieved from the agent. Threshold Manager retrieves events at startup and again when the refresh timer reaches a specified interval. For more information on the refresh timer, see “Retrieving Events.”

When a threshold event is retrieved from the agent, Threshold Manager tries to correlate the event information with existing policies to show additional information. If an event cannot be correlated with any policy, Threshold Manager displays “undefined.”

Table A-1 shows the fields and associated policy for each threshold entry in the event list.

Table A-1 Threshold Manager Event List Fields And Policies

Field	Policy
Capture of Event Priority Icon (Windows only)	The Event Priority icon represents the event severity. The policy file for the thresholds that generate this event sets the priority. Allowable values are 1 through 3, with 1 being the most severe. If Threshold Manager cannot correlate the event with a policy file, the application assigns a priority of 3.
Log Time	Time and date the event was logged. The RMON agent in the managed device generates this value.
Profile	The profile to which the threshold belongs. A profile is a group of policies. There are four profiles: system, interface, rmon_EtherStats, and customize.
Description	Threshold policy description.
Alarm Variable	Name of the MIB variable.
Event Priority	Priority of the event. Values are 1 (highest) to 3 (lowest). The predefined threshold policies have default priority value, but you can change the value according to the importance of the information to you. If Threshold Manager cannot correlate the event with a policy file, it assigns the event a priority of 3.
Log Description	Description of the event as defined in the corresponding RMON event entry.
Event Index	Index of the RMON corresponding event entry.
Log Index	Index of the RMON log entry.
Owner Description	A text string that identifies the network management station or person to contact about the associated policy file.

You can sort the event list by clicking on the field headers. You can also change the width of the columns by clicking on the dividers between the field headers and stretching the column to the desired size. If you are using UNIX, press the **Shift** key and click the middle mouse button while dragging the divider. If you are using Windows, click the left mouse button while dragging the divider.

To view a single event, double-click on the event you want to see from the Threshold Manager window events list.

The Single Event View dialog box appears, displaying complete information about a specific event. You use the Single Event View dialog box to determine what threshold settings in the RMON agent generated the event.

The Single Event View dialog box is divided into two panes: Profile Identification and Agent Log Information.

Profile Identification Pane

The Profile Identification pane contains parameters related to the threshold settings that generated the event. This information helps you determine what conditions triggered the event. Table A-2 shows the parameters and their description.

Table A-2 Profile Identification Parameters

Parameter	Description
Profile	The name of the profile to which the policy file belongs.
Policy Description	A description of the policy. This is the MIB variable name.
Alarm Variable	Name of the MIB variable.
Threshold Parameters: Interval	Interval, in seconds, over which the data is sampled and compared with rising and falling thresholds.
Threshold Parameters: Rising Threshold	Threshold for the sampled statistic. When the current sampled value is greater than or equal to this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes active, is greater than or equal to this threshold, and the associated Startup Alarm is equal to rising. After a rising event is generated, another such event is not generated until the sampled value falls below this threshold and reaches Falling Threshold. See “Creating New Policy Files.”

Table A-2 Profile Identification Parameters (continued)

Parameter	Description
Threshold Parameters: Falling Threshold	Threshold for the sampled statistic. When the current sampled value is less than or equal to this threshold, and the value at the last sampling interval was greater than this threshold, a single event is generated. A single event is also generated if the first sample after this entry becomes active, is less than or equal to this threshold, and the associated Startup Alarm is equal to falling. After a falling event is generated, another such event is not generated until the sampled value rises above this threshold and reaches Rising Threshold. See “Creating New Policy Files.”
Sampling Type	Method of sampling the selected variable and calculating the value to be compared with the thresholds. If the value is Absolute, the value of the selected variable is compared directly with the thresholds at the end of the sampling interval. If the value is Delta, the value of the selected variable at the last sample is subtracted from the current value, and the difference compared with the thresholds.
Startup Alarm	Alarm that can be sent when this entry first becomes active. If the first sample after this entry becomes active, is greater than or equal to Rising Threshold, and Startup Alarm is equal to rising, then a single rising alarm is generated. If the first sample after this entry becomes active or is less than or equal to Falling Threshold, and Startup Alarm is equal to falling, a single falling alarm is generated.
Rising Event Type	Agent notification for the rising event. In the case of log, an entry is made in the log table for each event. In the case of snmp-trap, an SNMP trap is sent to one or more management stations.
Falling Event Type	Agent notification for the falling event. In the case of log, an entry is made in the log table for each event. In the case of snmp-trap, an SNMP trap is sent to one or more management stations.
Event Priority	The priority of the event.

If the threshold settings were created by a Threshold Manager policy file, the values from that policy file are displayed. If no policy file is associated with the threshold settings, the fields remain blank.

Agent Log Information Pane (Configuration Information)

The Agent Log Information pane contains information obtained by Threshold Manager from the RMON agent log. This information provides:

- The time the event was generated
- A description of the event
- The index number of the event
- The log index number of the event

Because the Agent Log Information pane contains information from the RMON agent log in the managed device, these values display whether a Threshold Manager policy file can be associated with the event.

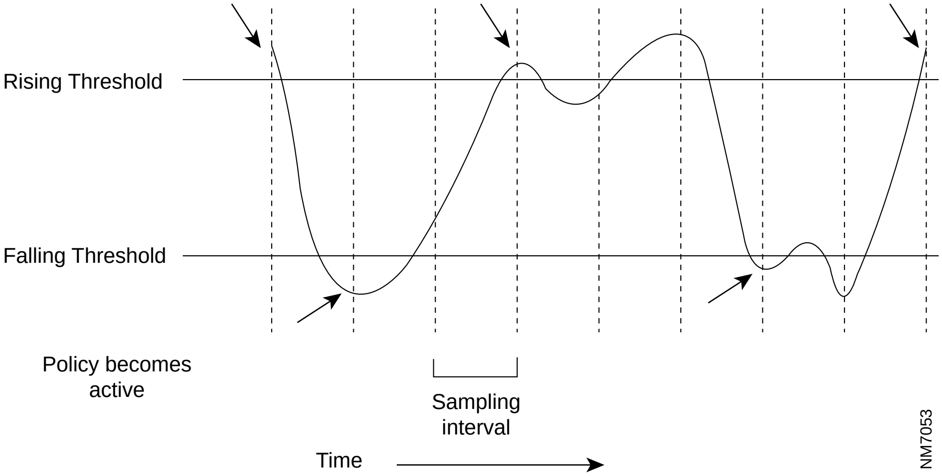
Table A-3 describes the action buttons.

Table A-3 Action Buttons

Button	Action
Description	Click to see more details of the event.
Delete	Click to delete the event from the event log. This has the same effect as selecting the event in the Threshold Manager window events list and selecting **Delete>Selected Events**. You might want to delete events after you have finished analyzing a particular event type and no longer need to view it or you want to decrease the number of events displayed in the Threshold Manager window events list.
Cancel	Click to close the window.
Help (Windows only)	Click to get online help about this window.

Figure A-1 shows when rising and falling events occur with the Startup Alarm set to Rising and Falling.

Figure A-1 When Threshold Events Occur



Retrieving Events

Select **View>Retrieve Events** to force a retrieve event action from the Threshold Manager window events list.

Threshold Manager retrieves events from the RMON agent log in the following situations:

- You launch an instance of Threshold Manager.
- The refresh interval ends.
- You request a retrieve operation.

When the application is operational, Threshold Manager automatically retrieves events from the RMON log at regular intervals. This interval is defined by the refresh timer parameter associated with that instance of Threshold Manager. This parameter is defined when you initiate a Threshold Manager session. The default is 360 seconds. If the refresh timer is set to 0, the Threshold Manager will not automatically retrieve events from the RMON agent.

Sorting Events

To sort events, go to the Threshold Manager window events list and click on any column header to sort the items in that column.

Threshold Manager allows you to change the order in which you view events in the Threshold Manager window events list. This capability permits you to view events in a manner that is most meaningful to you. You can reorder the following fields:

- Log Time—Descending alphanumeric
- Profile—Ascending alphabetic
- Description—Ascending alphabetic
- Alarm Variable—Ascending alphabetic
- Priority—Ascending numeric
- Log Description—Ascending alphabetic
- EventIndex—Ascending numeric
- LogIndex—Ascending numeric
- Owner—Ascending alphabetic

Printing Events

You can print events from the Threshold Manager window events list by selecting **File>Print** and clicking **OK**. Make sure your printer is set up properly.

Because events can be deleted from the log, printing lets you maintain a history log of device activity. This log helps you accumulate data to determine your network baselines and performance trends. The printed version of the Threshold Manager window events list contains the information described in “Viewing Threshold Events.”

Deleting Events

You can remove events from the RMON log in the managed device. You delete events in the following cases:

- You have completed analysis of a particular event type and no longer need to view it.
- You want to decrease the number of events displayed on the Threshold Manager window events list.

Because events are physically removed from the RMON agent log, deleting events also improves the performance of Threshold Manager when it retrieves and displays new events.

To delete a selected event from the RMON agent log:

Step 1 Highlight the event to be deleted by selecting it from any field within the Threshold Manager window events list.

Step 2 Select **Delete>Selected Events**.

To delete all events from the RMON agent log, select **Delete>All Events**.

You can also delete selected events from the Single Event View dialog box.

Any user who has launched an instance of Threshold Manager against a device can delete events from that RMON agent log. This means that your Threshold Manager window events list might not display the current contents of the RMON agent log of a device if that device is being managed by more than one Threshold Manager. Your Threshold Manager window events list reflects the change when

- You delete an event using Threshold Manager.

- Threshold Manager automatically updates the window at the end of the refresh interval.
- You force a retrieve operation by selecting **View>Retrieve Events**.

Threshold Manager allows you to delete selected events or all events in the log. When you delete a selected event, all events with the same EventIndex value are removed from the RMON log.

Event Task Examples

Table A-4 shows examples of event tasks that you can use to help manage your network.

Table A-4 Event Tasks

Task Description	Solution	Operations
Diagnose a network segment that has congestion problems.	Check whether any threshold events have occurred in the device close to the segment.	**Step 1** Open the Threshold Manager window. **Step 2** Select **View>Retrieve Events**. **Step 3** View all of the displayed events. **Step 4** Click on the header of any column in the main window to sort the events to investigate the correlation between threshold events and the network problem. **Step 5** Double-click on an interesting event to bring up the Single Event View dialog box to investigate the threshold setting that caused the event to occur. **Step 6** Click **Description** to read the description of why this event was generated.
Sort the tasks by priority.	N/A	**Step 1** Open the Threshold Manager window. **Step 2** Sort the events by priority by clicking on the header of the Priority column.

Table A-4 Event Tasks (continued)

Task Description	Solution	Operations
Finish investigating the displayed events.	Delete some events in the box to reduce memory use in the agent.	**Step 1** Open the Threshold Manager window. **Step 2** Select the events and use **Delete> Delete Selected Events** to delete the selected ones or **Delete>Delete All Events** to delete all the events.

Managing Thresholds

With Threshold Manager, you can manage existing threshold settings and policies or create new policies. This capability allows you to tailor alarms and events to your specific network needs. The Configure Thresholds dialog box provides you with the tools to do the following:

- Manipulate current threshold settings and policies.
- Create new policies.
- Obtain current information about the managed device.
- Change the target device for this instance of Threshold Manager.

Displaying Thresholds

To access the Configure Thresholds dialog box, select **Config>Thresholds**.

The Configure Thresholds dialog box defaults to the Config Threshold tab. The Config Threshold tab is divided into two panes. The upper pane is called the Policies pane. The lower pane is called the Current Threshold Settings pane.

Policies Pane

The Policies pane displays all the existing policy files that can be applied to the managed device. The displayed policies can be default policies provided by Cisco Systems, modified policies, or any user-defined policies. Threshold Manager provides detailed information about each policy to help you determine which thresholds to set in the RMON agent.

The content of this pane is specific to the instance of Threshold Manager and is visible only at your local machine.

This pane also allows you to do the following:

- View the default policies
- Add selected or all policies to the Current Threshold Settings pane
- Modify an existing policy
- Create a new policy

For more information on the policies, see “Using Policy Files” later in this chapter.

Current Threshold Settings Pane

The Current Threshold Settings pane displays the threshold settings for the RMON agent in a managed device. The threshold settings that display an active status are those enforced in the RMON agent. These threshold settings are viewable from any Threshold Manager launched against that device. The Current Threshold Settings pane also provides information on the number of current threshold settings, the status of those settings, and the last time the current threshold settings pane was updated. From the Current Threshold Settings pane, you can do the following:

- Obtain detailed information about a current threshold setting.
- Modify a current threshold setting in the RMON agent.
- Enforce all or selected threshold settings. Enforcing a threshold setting changes it from pending to active. The status displays a failed value if the threshold setting cannot be enforced in the RMON agent.
- Delete all or selected threshold settings. Deleting a threshold setting deletes all events in the RMON log that have been generated as a result of those settings.
- Print the contents of the Current Threshold Settings pane.
- Retrieve current threshold settings from the RMON agents. Retrieving current threshold settings deletes all pending threshold settings.

If Threshold Manager created the threshold settings, the fields displayed in the Current Threshold Settings pane will contain data provided by the policy file. If Threshold Manager did not create the policy or Threshold Manager cannot associate a policy with an event, only the information provided by the RMON agent will be displayed.

Managing Thresholds

With Threshold Manager you can manage existing threshold settings and policies or create new policies. This capability allows you to tailor alarms and events to your specific network needs. The Configure Thresholds dialog box provides you with the tools to do the following:

- Manipulate current threshold settings and policies
- Create new policies
- Obtain current information about the managed device
- Change the target device for this instance of Threshold Manager

To access the Configure Thresholds dialog box, select **Config>Thresholds**.

Obtaining Managed Device Information

The Device Summary dialog box displays summary information about the device and the RMON MIB. The Device Summary dialog box displays information about the device currently managed by Threshold Manager. This is helpful if you want to determine the class of the target device or obtain information about the device interfaces. In a Windows platform, from the Configure Thresholds dialog box, click the **Device Summary** tab to access the Device Summary dialog box. On a UNIX platform, from the Threshold Manager window, select **Config>Device Summary** to access the Device Summary dialog box.

Table A-5 describes the fields in the Device Summary dialog box.

Click **Retrieve** to get the latest Interface/Port List information.

Table A-5 Device Summary Dialog Box

Field	Description
Device Class	Type of device.
Last Refresh Time	Last time events were retrieved by the agent.
Log Entries Alarm Entries Event Entries	Number of entries in the log, alarm, and event tables.[1]
System Name System Contact System Uptime System Description System Location	Information about the system. One or more fields might be blank, depending on the device configuration.
Interface/Port List	List of interfaces and ports available to the device. The icon (Windows NT only) in the left column is either an I (interface) or P (port). A red icon means the interface or port is down, and a green icon means the interface or port is up. The list of ports and interfaces for the device provides you with information about individual interfaces. This is helpful when you are designing and applying policies to specific interfaces. You can sort on the fields in this dialog box to present the information in a meaningful manner.

[1] The counters of the RMON tables in the Device Summary dialog box reflect the value at the time the interface table entries were retrieved completely. Because tables are retrieved asynchronously within Threshold Manager and a large log table might be completed much later than the interface table, there are situations when the counters in the Device Summary dialog box do not match the actual counters.

Changing the Managed Device

There is a one-to-one relationship between a single instance of Threshold Manager and the managed device. Also, when Threshold Manager is launched from CiscoView, the application receives default run-time arguments used for operations. Threshold Manager allows you to alter both the target device and the run-time parameters from within the application. This is particularly useful if you want to use a single instance of Threshold Manager to apply threshold settings in multiple devices or if you started the application with the wrong run-time parameters.

This device information is changed from the Properties dialog box. The Properties dialog box allows you to do the following:

- Manage a new device.
- Increase or decrease the value of the refresh timer.
- Alter the Read-Write community strings.
- Increase or decrease the amount of time Threshold Manager waits to receive a response from the device before timing out.
- Increase or decrease the number of times Threshold Manager attempts to contact the target device if no response is received.

To access the Properties dialog box on a Windows platform, click the **Properties** tab from the Configure Thresholds dialog box. On a UNIX platform, select **Config>Properties** from the Threshold Manager window.

Configuring Thresholds

The Configure Thresholds dialog box allows you to modify and create policies and work with threshold settings.

This dialog box consists of two panes: the Policies pane and the Current Threshold Settings pane, which are described in “Managing Thresholds.” For information on changing policies, see “Using Policy Files” later in this chapter. When Threshold Manager is installed, 18 policy files appear in this dialog box. You can select one or all to use as thresholds.

Adding a Threshold Setting

Before you can set a threshold in the RMON agent, you must add the settings to the Current Threshold Settings pane. You can add all policies as threshold settings or you can add specific policies. A policy can result in multiple threshold settings in the Current Threshold

Settings pane. The number of times Threshold Manager adds the policy to the Current Threshold Settings pane depends on the target type and number of interfaces defined in the policy file.

To add all policies in the Policies pane to the Current Threshold Settings pane, click **Add All Policies**.

To add selected policies to the Current Threshold Settings pane:

Step 1 Click on the selected policy.

Step 2 Click **Add Selected Policies**.

To add multiple selected policies to the Current Threshold Settings pane while using UNIX:

Step 1 Click on the selected policies.

Step 2 Click **Add Selected Policies**.

To add multiple selected policies to the Current Threshold Settings pane while using Windows:

Step 1 Hold down the **Shift** key and click on the policy at the beginning of the desired range.

Step 2 Hold down the **Shift** key and click on the policy at the end of the desired range.

Step 3 Click **Add Selected Policies**.

A policy added to the Current Threshold Settings pane retains a pending status. This status does not change until you enforce the threshold settings to the RMON agent. Threshold settings with a pending status are viewable only from local machines.

Modifying Threshold Settings

To modify threshold settings:

Step 1 Select **Config>Thresholds**.

The Configure Thresholds dialog box appears.

Step 2 In the Current Threshold Settings pane, double-click on the selected threshold setting.

The Modify Threshold Settings dialog box appears. From this dialog box, you can do the following:

- Increase or decrease the threshold parameters.
- Change the sampling type to absolute or delta.
- Indicate the startup alarm as rising or falling.
- Specify the rising event type notification as trap, log, or both.
- Specify the falling event type notification as trap, log, or both.
- Modify the owner identification name of the policy file owner.
- Modify the event priority setting.
- Change the event community string to that of the managed device.
- Delete an existing threshold settings or enforce the changes.
- View policy identification.
- View miscellaneous information.
- View a description of the policy identification pane.

Threshold Manager lets you temporarily alter threshold settings for an alarm object instance. This is useful when you want to monitor network performance for a specific period of time or fine-tune threshold settings before applying them permanently. Changes to existing threshold settings are not saved in the associated policy file. Therefore, if the device loses power or is shut down, the modifications are lost. To make permanent changes to the threshold settings, alter the associated policy file, and add the new threshold settings to the Current Threshold Settings pane.

You can alter a threshold setting that has a pending or active status. A threshold setting with a failed status means the threshold setting was rejected by the RMON agent and cannot be altered.

Deleting a Threshold Setting

You can remove active threshold settings enforced in the RMON agent and pending threshold settings from the Current Threshold Settings pane of the Configure Thresholds dialog box. Deleting a threshold setting removes all events associated with that threshold setting from the RMON log.

To delete a threshold setting, regardless of status:

Step 1 Click on the threshold setting.

Step 2 Click **Delete Selected**.

A Threshold Manager Warning popup window appears. Click **OK**, or click **Cancel** to cancel the deletion.

To delete more than one threshold setting, regardless of status, while using UNIX:

Step 1 Click on the selected policies.

Step 2 Click **Delete Selected**.

A Threshold Manager Warning popup window appears. Click **OK**, or click **Cancel** to cancel delete.

Step 3 Click **Delete All** to remove all threshold settings, regardless of status.

To delete more than one threshold setting, regardless of status while using Windows:

Step 1 Hold down the **Shift** key and click on the threshold setting at the beginning of the desired range.

Step 2 Hold down the **Shift** key and click on the threshold setting at the end of the desired range.

Step 3 Click **Delete Selected**.

A Threshold Manager Warning popup window appears. Click **OK**, or click **Cancel** to cancel delete.

Step 4 Click **Delete All** to remove all threshold settings, regardless of status.

Threshold settings with a pending status are removed from the Current Threshold Setting pane when you do the following:

- Delete them.
- Retrieve threshold settings from the RMON agent.
- Exit the Configure Thresholds dialog box.

Threshold Manager Task Examples

Table A-6 describes common Threshold Manager tasks.

Table A-6 Threshold Manager Task Examples

Task Description	Operations
Modify the number of occurrences of a particular kind of event that are reported.	Modify the threshold parameters because they are set too low or too high with respect to the network baseline by performing the following steps: **Step 1** Open the Threshold Manager window. **Step 2** Double-click on the threshold. The Single Event View dialog box appears. **Step 3** Modify the rising and/or falling threshold parameter(s) to adjust to network baseline so that the events are generated only on exceptions.

Table A-6 Threshold Manager Task Examples (continued)

Task Description	Operations
Delete some thresholds to reduce load added by threshold monitoring.	**Step 1** Open the Threshold Manager window. **Step 2** Select **Config>Thresholds** to open the Configure Thresholds dialog box. **Step 3** Click **Retrieve Thresholds** in the Current Threshold Settings pane to retrieve the current active thresholds from the managed agent. **Step 4** View the count of the current thresholds to learn how many thresholds are active. **Step 5** Select the threshold rows that are less critical to monitor. **Step 6** Click **Delete Selected** to delete the thresholds from the agent. The events associated with these deleted thresholds are removed as well.
Use different threshold settings for each interface for interface-specific thresholds when the thresholds are still pending in the management station.	**Step 1** Open the Threshold Manager window. **Step 2** On a Windows platform, select **Config>Thresholds** to open the Configure Thresholds dialog box. On a UNIX platform, select **Config>Properties** to access the Properties dialog box. **Step 3** Double-click on a threshold row in the Current Threshold Setting pane. **Step 4** Modify the threshold parameters in the Modify Threshold Settings dialog box. **Step 5** Click **Enforce** to enforce to the agent. **Step 6** Double-click on another threshold, and repeat the steps until the threshold setting for each interface is configured properly.
Adjust the event retrieving interval, because events are retrieved too frequently, and there is not that much event activity in this device.	**Step 1** Open the Threshold Manager window. **Step 2** On a Windows platform, select **Config>Thresholds** and click the **Properties** tab. On a UNIX platform, select **Config>Properties** to access the Properties dialog box. **Step 3** Set the Refresh Timer to a larger number. **Step 4** Click **OK**.

Using Policy Files

Threshold Manager is delivered with a set of predefined policy files that are used to set threshold values into RMON device agents. A Threshold Manager policy file contains at least one threshold policy (the default policy) for the alarm variable defined in the policy file. A policy file can contain more than one threshold policy to define threshold values for specific interface types, but it contains policies for only one MIB variable. In other words, there is a separate policy for each MIB variable. When an interface-specific policy is defined, Threshold Manager applies the threshold policy to the matching interface type. If no interface-specific threshold policy is defined, Threshold Manager applies the default threshold value to all device interfaces.

Formatting Policy Files

A policy file is an ASCII file; it is defined by keywords used by Threshold Manager to scan the file. Each policy file defines an alarm variable to be monitored by a device RMON agent and one or more threshold policies to be sent to the device agent for monitoring purposes.

To understand the meaning of policies and to simplify file parsing, Threshold Manager imposes strict rules whenever a policy file is created either manually or through the Create Threshold Policy dialog box. It is strongly recommended that you customize policy files by using the Threshold Manager graphical user interface (GUI).

A policy file is composed of many keyword-value pairs. A keyword and its value are separated by an equal sign (=). If the keyword requires more than one value, each value is separated by a colon (:). Each line of a policy profile contains only one keyword-value pair, for example:

```
Target_Type = etherStats
Rising_Threshold = 200
Falling_Threshold = 20
Sample_Interval = 60:0:300
```

The order of the keyword-value pair is not important. All white spaces are ignored during file parsing. If a keyword appears more than once, the last keyword-value pair takes effect. The only exception to this rule is keyword **Interface_Threshold**.

Defining Interface-Specific Policies

An interface-specific policy is defined by the keyword **Interface_Threshold**. There can be multiple **Interface_Threshold** keyword-value pairs in a policy profile, each of which defines a specific threshold policy (value) for a particular interface type, for example:

```
Interface_Threshold = ethernetCsmacd:375000000:187500000:100000000
Interface_Threshold = ethernetCsmacd:37500000:18750000:10000000
```

The syntax of this special keyword-value pair is as follows:

```
Interface_Threshold=interface_type:rising_thresh_value:falling_thresh_va
lue:interface_speed
```

where *interface_speed* is optional.

Threshold Manager uses interface-specific policies to set specific interface thresholds. If the interface speed is specified in the policy, the policy is applied to interfaces that match both the interface type and speed. If interface speed is not present, the policy is applied to the interface that matches the specified interface type, regardless of speed. The default policy is used to set thresholds for interfaces without an interface-specific policy defined.

Loading Policies

Policies are loaded into Threshold Manager during startup and when a new instance of Threshold Manager is launched to monitor another device. After the policies are loaded, any new policy file created manually is ignored by Threshold Manager. However, a new policy file that is created and saved in the Create Threshold Policy dialog box is immediately visible inside Threshold Manager.

Policy files are grouped into three types: global, device class, and host. All policy files are saved under the *config* directory of the Threshold Manager. Policy files under the *config* directory are global policy files and are used for all devices. Policy files under the device class subdirectory apply to devices that belong to the same device class family. Policy files that are saved in the host subdirectory are used to set thresholds against only the specific host.

When reading policies for a given device, Threshold Manager searches that host subdirectory to locate any host-specific policy files defined for that device. It then scans the device class subdirectory for policy files defined for that device class. Last, it picks up any policy files not defined elsewhere.

Naming Policy Files

Threshold Manager policy files require specific naming conventions to simplify file parsing for existing policies and when a new policy file is created. The two Threshold Manager policy file naming conventions are described below.

- Policy File

  All policy files have a *.thd* file extension. Threshold Manager loads only policy files with a *.thd* extension. You can create new policy files manually or by using the Threshold Manager GUI. A policy file created through the GUI is saved as one of the policy file classes based on user's choice, with a file name *alarm_variable_name.thd*, where *alarm_variable_name* is the alarm variable entered.

- *Config* Directory

  The *config* directory is installed by the Threshold Manager installation script under *$NMSROOT/etc/cview/devices/Threshold-Mgr*. The *config* directory is under Threshold-Mgr. CiscoView launches Threshold Manager with a default *config* directory of *$NMSROOT/etc/cview/devices/Threshold-Mgr/config*. However, this can be overridden by starting the Threshold Manager with *-p Threshold Manager* argument. Once Threshold Manager is started, you cannot change the Threshold Manager directory even when you launch a new instance of Threshold Manager from within the application to monitor another device.

Using Default Policy Files

Threshold Manager comes with 18 policy files already defined. In addition, there could be policies that are device-specific that are under the device subdirectories. These device-specific policies override the default policies.

Table A-7 contains a brief description of the policy files.

Table A-7 Threshold Manager Policy Files

Policy File	Description	Default Threshold
avgBusy5	Average CPU busy in the last 5 minutes. See the description in the next entry.	90%

Table A-7 Threshold Manager Policy Files (continued)

Policy File	Description	Default Threshold
avgBusy1	Average CPU busy in the last minute. Both policies 1 and 2 are used so that the user gets at least 2 events (traps and/or logs) in case the CPU load keeps increasing.	70%
etherStatsOctets	Ethernet segment utilization (RMON Ethernet statistic group).	50%
freeMem	Free memory.	Falling threshold (absolute): 500 KB
ifInOctets	Interface input utilization.	50%
ifOutOctets	Interface output utilization.	50%
locIfCarTrans	Carrier transitions.	10/minute
locIfReliab	Reliability of the interface.	Falling threshold: 240
locIfResets	Number of resets.	10/minute
locIfRestarts	Number of restarts.	10/minute
bufferFail	Buffer allocating failures.	5/30 seconds
bufferNoMem	Buffer creation failures.	5/30 seconds
etherStatsPkts	Ethernet segment utilization (RMON Ethernet statistic group).	500/second
etherStatsCRCAlign Errors	Ethernet segment alignment error (RMON Ethernet statistic group).	50/minute
etherStatsCollisions	Ethernet segment collision errors (RMON Ethernet statistic group).	50/minute
etherStatsUndersizePkts	Ethernet segment size errors (RMON Ethernet statistic group).	50/minute
etherStatsOversizePkts	Ethernet segment size errors (RMON Ethernet statistic group).	50/minute
etherStatsFragments	Ethernet fragmentation errors (RMON Ethernet Statistic group).	50/minute

Modifying a Policy File

Threshold Manager allows you to modify an existing threshold policy file so that you can change threshold settings for an Alarm variable without redefining the complete policy. You can create a policy file once and then tailor it for specific interface types. Altering policy file values does not change any threshold settings, regardless of the status of those settings.

Double-click the selected policy in the Policies pane of the Configure Thresholds dialog box to display the Modify Threshold Policy dialog box. From this dialog box, you can do the following:

- View profile identification.
- Increase or decrease the threshold parameters.
- Change the sampling type to absolute or delta.
- Indicate the startup alarm as rising or falling.
- Specify the rising event type notification as trap, log, or both.
- Specify the falling event type notification as trap, log, or both.
- Alter the event priority.
- Modify the owner identification name of the policy file owner.
- Change the event community string to that of the managed device.
- Determine the physical interface type against which the threshold settings are applied.

When you complete your modifications, you can save the changes in the host-specific, device class, or global directories. Saving a policy file automatically updates the existing policy file in the Policies pane. Clicking **Continue** applies the altered policy directly to the Current Threshold Settings pane without saving the changes.

Customizing Policy Files

A powerful feature of Threshold Manager is that it allows you to easily create customized threshold policies. This means that you can design threshold settings specific to the conditions and performance of your network. Customization also means you can define which alarm variables to monitor, the type of threshold variable, and the specific interfaces to which the thresholds apply.

You create new threshold policies to do the following:

- Set new thresholds for an alarm OID.
- Define configuration files for alarm OIDs supported by the RMON agent but not covered by an existing policy.
- Apply new thresholds to one or more interfaces on a device.

Cisco maintains a list of all SNMP MIBs supported by Cisco IOS Release 10.2 and later. This list is located at

ftp://ftp.cisco.com/pub/mibs/supportlists/

The SNMP MIBs are organized by device class for both routers and switches.

Creating New Policy Files

You create a new policy from the Create Threshold Policy dialog box. To access this dialog box, click the Create New Policy button in the Policies pane of the Configure Thresholds dialog box.

The Create Threshold Policy dialog box contains the following fields:

- Profile—the name of the profile to which the new policy file will belong. The value of this field is customized and cannot be altered.
- Policy—a string of any alphanumeric characters used to describe the policy file. You must enter a value in this field.
- Alarm Variable—a string of any alphanumeric characters representing the name of the SNMP MIB object. If the policy file is saved, the value of this field is used as the policy file name.

- Alarm OID—uniquely identifies the threshold variable. You must enter a value in this field. You may or may not have to qualify the instance ID, depending on the value of the next field.
- Target Type—defines how Threshold Manager manipulates the alarm object ID. If this value is one of the five Threshold Manager target types, you do not have qualify the instance identifier for the OID. These target types are known variables to Threshold Manager, and the application provides the mechanism to access the instance identifier of the object in the SNMP MIB. If you define this value as customized, you must provide the instance identifier for the alarm object.

The Create Threshold Policy dialog box lets you define the following fields:

- Sampling Interval—sets the minimum and maximum values, in seconds, for the boundaries of the sampling interval.
- Rising and falling thresholds for the sampled data. You must enter a value in these fields.
- Interface Type—determines the type of physical interface against which the threshold settings are applied. You can define multiple interface specific thresholds within a single policy file. This field is optional and can be used only if the variable is part of an interface table or the Ethernet statistical table.
- Interface Speed—used to calculate the line usage. Like the Interface Type, this field applies only to interface-type variables and is optional.
- Interface List—indicates the specific threshold values for each interface you selected.
- Sampling Type.
- StartUp Alarm.
- Rising Event Type and Falling Event Type.
- Event Priority.
- Owner Identification.
- Event Community.

Configuration File Content

The policy configuration file is a text file that sets the parameters of the threshold for a specific MIB variable. The data in the configuration file is composed of keyword-value pairs in the form of <item name> = <item value>. The keywords contained in the configuration file are as follows:

- **Profile_Name** defines the group to which the policy file belongs. There are four allowable profiles: System, Interface, mon_EtherStats, and Customize.
- **Policy_Name** provides a description that further defines the policy. The value of this item is contained in a default policy name. For a customized policy, the creator of the policy provides this information.
- **MIB_Name** is the name of the SNMP MIB object to be monitored. The value of this item is derived from combining the alarm variable name plus the OID. Cisco Systems provides these values in the default policy files. For a customized policy, you must define a string of alphanumeric characters for the alarm variable name and identify a valid SNMP MIB OID. The name of the customized policy file is derived from this value.
- **Target_Type** defines how Threshold Manager accesses the OID. The possible entries for this keyword are as follows:
    - **Sys** defines the value as a scalar variable and represents the system object.
    - **loc_if** defines the value as a columnar variable of the Cisco local interface table.
    - **mib2_if** defines the value as a columnar variable of the Cisco local interface table.
    - **mib2_util** defines the value as a percentage of utilization and is derived by a columnar variable of the MIB II ifTable. The threshold setting for the interface is determined from this value and the speed of the interface.
    - **etherstats** defines the value of the columnar field of the RMON etherStatsTable.
- **Sample_Interval** defines the amount of time (in seconds) over which the data is sampled and compared with a threshold.
- **Sample_Type** defines the method used to derive the value of the selected variable to be compared with the threshold. Allowable values are
    - **abs** means that the value of the selected variable will be compared directly with the thresholds at the end of the defined period of time.

  - — **delta** means that the value of the selected variable from the last sampling interval is subtracted from the current value. The difference is then compared with the threshold.

- **Startup_Alarm** defines the alarm generated for the first sample interval. Allowable values are rising or falling.
- **Rising_Threshold** indicates a threshold value. When the current sampled value is greater than or equal to this threshold value and the value of the last sample interval is less than this threshold value, a rising alarm is generated. A rising alarm is also generated if the value of the first sampling interval is greater than or equal to this threshold value and the **Startup_Alarm** value is set to Rising.
- **Falling_Threshold** indicates a threshold value. When the current sampled value is less than this threshold value, and the value of the last sample interval is greater than this threshold value a falling alarm is generated. A falling alarm is also generated if the value of the first sampling interval is less than this threshold value and the **Startup_Alarm** value is set to Falling.
- **Owner_Spec** identifies who created the policy or the person to contact in case there are questions or problems regarding the policy file. All default policy files have an **Owner_Spec** value of admin. The **Owner_Spec** value is user-defined for customized policies.
- **Event _Priority** indicates the severity of the event generated as a result of the policy file. This keyword is predefined in the default policy files. For customized policies, the event priority value is assigned by the creator of the policy. Allowable values are 1 to 3, with the value of 1 being most critical.
- **Interface_Threshold** defines a rising and falling threshold specific to an interface type. This keyword is optional if the values of the rising and falling threshold keywords are defined. However, if no values are specified for the rising and falling threshold keywords and the **Interface_Threshold** keyword is not defined, Threshold Manager will not apply the policy file in the RMON agent.

  The syntax of the **Interface_Threshold** keyword is

  <interface type>:<rising threshold value>:<falling threshold value>:<interface speed>

  The following is an example of the **Interface_Threshold** keyword and value:

  ```
  Interface_Threshold = ethernet Csmacd:375000000:187500000:100000000
  ```

- **Rising_Event_Type** indicates the type of notification the RMON agent makes when a rising event is triggered. Allowable values are log, trap, or both. If the log value is selected, the agent is the device makes an entry in its log table when a rising event is generated. If the trap value is selected, an SNMP trap message is sent to one or more management stations when a rising event is generated. The RMON agent for the device will generate an entry in its log and send a trap for a rising event when the both value is indicated.
- **Falling_Event_Type** indicates the type of notification the agent in the device makes when a falling event is triggered. Like the **Rising_Event_Type**, allowable values are log, trap, or both.
- **Event_Community** specifies the SNMP community where the trap is sent.

Policy configuration files are secured using the standard file security procedures in the host operating system.

After you create a policy file, you can do the following:

- Save the policy file.
- Apply the policy file to one or more interfaces.
- Add the policy file as a current threshold setting.

You can save a threshold policy file in the host-specific, device class, or global directory. Remember that the host-specific directory takes on the name of the managed device. This name can be the host name or IP address of the device, depending on how you identified the device when you launched Threshold Manager. Policy files previously saved under the host name of a device will not appear in the Policies pane if you specify the IP address of the managed device when you launch Threshold Manager.

You cannot save a policy file that has a customized target type.

If the policy file is of an interface variable type, you can apply the threshold settings to one or more interfaces.

You can also add a policy file directly as a threshold setting without saving it to disk. This feature lets you create and add temporary threshold settings. However, there is no permanent record of these policies. They are lost when the managed device is turned off or goes down or when you delete the threshold settings from Threshold Manager.

After creating the policy file, click **Continue** to add it to the Current Threshold Settings pane. The new threshold setting will have a status of pending.

Adding Settings to Multiple Interfaces

Threshold Manager lets you assign multiple threshold settings to one or more interfaces within a single policy file. You can define common variables once while retaining the freedom to specify individual threshold on an interface-by-interface basis.

To add multiple interface threshold settings within a single policy file:

Step 1 Define the first set of threshold parameters.

Step 2 Select the interface type of the target interface.

Step 3 Click **Add** to add the interface type with its configured threshold settings to the Interface List.

Step 4 Define the next set of threshold parameters.

Step 5 Select the target interface type and add it to the interface list.

Repeat Step 3 and Step 4 as many times as necessary to add interface threshold settings.

After you have defined each specific threshold setting, you can apply it to one or more physical interfaces. Click **Continue** to access the Interface Selection dialog box. This dialog box displays all available interfaces in an up state for that device. Select the desired interfaces, and click **OK** to apply the threshold settings to the physical interfaces. This action also places the threshold settings in the lower pane of the Configure Threshold dialog box with a status of pending.

Deleting Policy Files

The current Threshold Manager implementation does not provide a mechanism for deleting existing threshold policies from within the application. You delete policies using the delete function of the UNIX or Windows operating systems.

The policies are located in the *Threshold-Mgr/Config* directory. Depending on how you saved the policy file, it can be found in one of the following subdirectories:

- Global
- Device Class
- Host-specific

All default policies in this release of Threshold Manager are found in the global directory.

Policy Task Examples

Table A-8 describes common Threshold Manager policy tasks.

Table A-8 Threshold Manager Task Examples

Task Description	Operations
Monitor all recommended thresholds on the managed agent.	**Step 1** Open the Threshold Manager window. **Step 2** Select **Config>Thresholds** to bring up the Configure Thresholds dialog box. **Step 3** Click **Add All Policies** in the Policies pane. The thresholds are populated in the Current Threshold Settings pane based on the device configuration. **Step 4** Click **Enforce All**. All pending thresholds are downloaded to the agent and become active thresholds.

Table A-8 Threshold Manager Task Examples (continued)

Task Description	Operations
Do not want to overload the agent with too many active thresholds by leveraging only the interface profiles.	**Step 1** Open the Threshold Manager window. **Step 2** Select **Config>Thresholds** to display the Configure Thresholds dialog box. **Step 3** Click the column title, **Profile**, in the Policies pane to sort the policies by profile name. **Step 4** Select all of the policy rows in the interface profile to be monitored. **Step 5** Click **Add Selected Policies**. The selected thresholds are populated in the Current Threshold Settings pane for all Up interfaces and are marked “Pending” in the Status column. **Step 6** Click **Enforce All**. All pending thresholds are downloaded to the agent and become active thresholds, marked “Active” in the Status column.
Create a new threshold policy and save it for later use.	**Step 1** Open the Threshold Manager window. **Step 2** Select **Config>Thresholds** to display the Configure Thresholds dialog box. **Step 3** Click **Create New Policy** in the Policies pane. **Step 4** Choose the appropriate target type for the threshold to be defined. **Step 5** Set up all parameters for this customized threshold policy. **Step 6** Save this policy to the desired location by clicking the button representing the destination (global, device class, or host) on the right side of the dialog box.

Table A-8 Threshold Manager Task Examples (continued)

Task Description	Operations
Customize the threshold parameters for predefined thresholds.	**Step 1** Open the Threshold Manager window. **Step 2** Select **Config>Thresholds** to display the Configure Thresholds dialog box. **Step 3** Double-click on the threshold policy you want to modify in the Policies pane. **Step 4** Set up the parameters to fit your network baseline. **Step 5** Save the changes to disk. The changes can be saved at the global level, which can be used by all devices; at the device class level, which can be used by all devices of the same device type; or at the device instance level, which can be used again only for this particular device.
Determine what a policy means.	**Step 1** Open the Threshold Manager window. **Step 2** Select **Config>Thresholds** to display the Configure Thresholds dialog box. **Step 3** Double-click on a threshold policy that you want to learn more about. **Step 4** Click **Description** in the Modify Threshold Settings dialog box. Threshold Manager provides help text on what this policy means.
Apply an interface-specific threshold only to a particular interface, instead of all interfaces.	**Step 1** Open the Threshold Manager window. **Step 2** Select **Config>Thresholds** to display the Configure Thresholds dialog box. **Step 3** Double-click on the threshold policy you wish to enforce to the agent. **Step 4** Click **Continue** in the Modify Threshold Policy dialog box. **Step 5** Select the interface for setting the threshold from the Interface Selection dialog box. **Step 6** Click **OK** to push it to the staging area. **Step 7** Click **Enforce All** to download the changes to the agent.

Table A-8 Threshold Manager Task Examples (continued)

Task Description	Operations
Set thresholds for only system MIB.	**Step 1** Open the Threshold Manager window. **Step 2** Select **Config>Profiles** to hide profiles other than system. **Step 3** In the Show Profile box, select profiles other than system, and click on the arrow to move the profiles to the Hide Profile box. **Step 4** From the Threshold Manager window, select **Config>Thresholds** to display the Configure Thresholds dialog box. The Policies pane now shows only the system policies.

Starting a New Threshold Manager

You can run multiple instances of Threshold Manager simultaneously so as to manage thresholds on several devices. From the pull-down menu, select **File>New Threshold Manager** to open the Start a New Threshold Manager dialog box.

The defaults in this dialog box apply to the current device configuration. You need to set the IP address of the device to be managed. You also need to specify the Threshold Manager Directory if it is not installed in the default location. The Threshold Manager directory is under the *Threshold* directory called *Threshold-Mgr*. For example:

/CWW/etc/cview/devices/Threshold-Mgr/

For descriptions of the other input fields in this dialog box, see “Troubleshooting Threshold Manager” later in this chapter.

Filtering Profiles

Threshold Manager lets you filter out profiles. A profile is a set of policy files that belong to a specific management area. When you filter a profile, all the policy files in that profile are no longer available to this instance of Threshold Manager. Filtering profiles is useful when you want to limit the number or focus on the type of policies available to an RMON agent. You can also use it when you want to set interface-related thresholds. By disabling all other profiles, only the interface policies are shown in the windows that manage policies.

To filter one or more profiles:

Step 1 Select **Config>Profiles** to access the Filter Profiles dialog box.

Step 2 Highlight the desired profiles in the Show Profile pane.

Step 3 Click the right arrow.

Profiles appearing in the Hide Profile pane are no longer available to this version of Threshold Manager, and policy files contained in these profiles will not be displayed in the Policies pane of the Configure Thresholds dialog box. However, any threshold settings active in the RMON agent that belong to the filtered profile are not affected.

Troubleshooting Threshold Manager

Table A-9 describes known problems and how to correct them.

Table A-9 Threshold Manager Troubleshooting Procedures

Problem	Explanation
Threshold Manager does not show up in Cisco View Tools pull-down menu.	Check the IOS version of the device. It must be 11.1 or above.

Table A-9 Threshold Manager Troubleshooting Procedures (continued)

Problem	Explanation

Cisco 7000 devices do not display Threshold Manager in the CiscoView pull-down menu.	You might be using an older version of 7000 packages. If so, edit the *c7com.dd* file located in *$NMSROOT/etc/cview/devices/7000/dd/c7com.dd*
	Change:
	`source`
	`$Cv_Path/devices/Router-share/CRTOOLBR.dd`
	`source`
	`$Cv_Path/devices/Router-share/C47CH.dd`
	To:
	`source`
	`$Cv_Path/devices/Router-share/C47CH.dd`
	`source`
	`$Cv_Path/devices/Router-share/CRTOOLBR.dd`
	Change:
	`set DD(menubar.menu) {{{} “Admin” admin}}`
	To:
	`lappend DD(menubar.menu) {{} “Admin” admin}`

Threshold Manager shows undefined fields in the Threshold Manager window events list.	The Threshold Manager directory is incorrect. Go to the directory where the policy files that you want to use are defined.
Duplicate global/device/host policies may be allowed, depending on which window is used.	When creating a custom policy, you can save it only once, as either global, device, or host. After saving the policy, you can use the Modify Threshold Settings dialog box to modify the saved custom policy and save it as all three.
The policy that you are using was not created by this Threshold Manager.	Create the policy on this instance of Threshold Manager or copy it from the Threshold Manager where it is defined.