CHAPTER 10

Configuring Thresholds

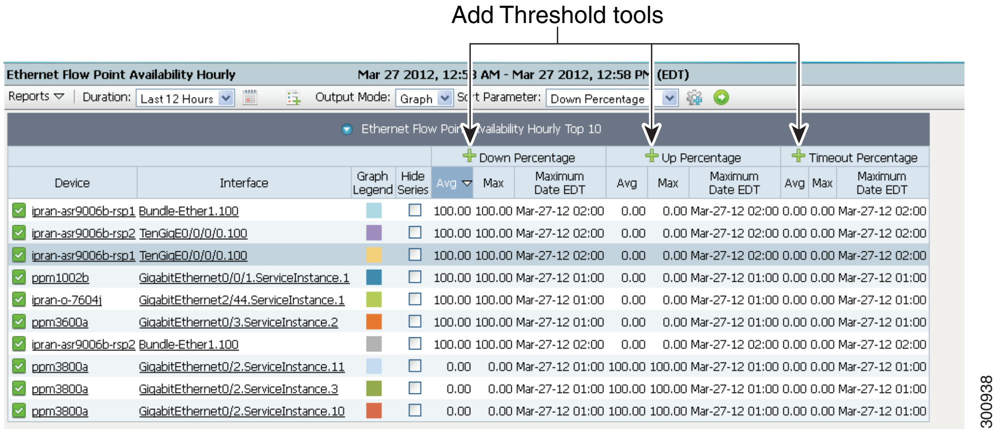
You can create thresholds for any key performance indicators (KPIs) displayed in Prime Performance Manager reports, views, or dashboards. Prime Performance Manager provides latitude in defining the alarm severities and onset and remission points. The following topics provide information about configuring thresholds in Prime Performance Manager:

- Creating Thresholds, page 10-1
- Managing Thresholds, page 10-5

Creating Thresholds

Prime Performance Manager allows you to create thresholds to generate alarms when a given report key performance indicator rises or falls to a specified point. Threshold-eligible report KPIs are identified by Add Threshold tools in the report KPI column header. Figure 10-1 shows an example.

Figure 10-1 Add Threshold Tools



Ethernet Flow Point Availability Hourly Mar 27 2012, 12:58 AM - Mar 27 2012, 12:58 PM (EDT)

Reports ▽ | Duration: Last 12 Hours Output Mode: Graph Sort Parameter: Down Percentage

Ethernet Flow Point Availability Hourly Top 10

				Down Percentage			Up Percentage			Timeout Percentage		
Device	Interface	Graph Legend	Hide Series	Avg ▽	Max	Maximum Date EDT	Avg	Max	Maximum Date EDT	Avg	Max	Maximum Date EDT
☑ ipran-asr9006b-rsp1	Bundle-Ether1.100	🟦	☐	100.00	100.00	Mar-27-12 02:00	0.00	0.00	Mar-27-12 02:00	0.00	0.00	Mar-27-12 02:00
☑ ipran-asr9006b-rsp2	TenGigE0/0/0/0.100	🟪	☐	100.00	100.00	Mar-27-12 02:00	0.00	0.00	Mar-27-12 02:00	0.00	0.00	Mar-27-12 02:00
☑ ipran-asr9006b-rsp1	TenGigE0/0/0/0.100	🟨	☐	100.00	100.00	Mar-27-12 02:00	0.00	0.00	Mar-27-12 02:00	0.00	0.00	Mar-27-12 02:00
☑ ppm1002b	GigabitEthernet0/0/1.ServiceInstance.1	🟦	☐	100.00	100.00	Mar-27-12 01:00	0.00	0.00	Mar-27-12 01:00	0.00	0.00	Mar-27-12 01:00
☑ ipran-o-7604j	GigabitEthernet2/44.ServiceInstance.1	🟩	☐	100.00	100.00	Mar-27-12 01:00	0.00	0.00	Mar-27-12 01:00	0.00	0.00	Mar-27-12 01:00
☑ ppm3600a	GigabitEthernet0/3.ServiceInstance.2	🟧	☐	100.00	100.00	Mar-27-12 01:00	0.00	0.00	Mar-27-12 01:00	0.00	0.00	Mar-27-12 01:00
☑ ipran-asr9006b-rsp2	Bundle-Ether1.100	⬜	☐	100.00	100.00	Mar-27-12 02:00	0.00	0.00	Mar-27-12 02:00	0.00	0.00	Mar-27-12 02:00
☑ ppm3800a	GigabitEthernet0/2.ServiceInstance.11	🟦	☐	0.00	0.00	Mar-27-12 01:00	100.00	100.00	Mar-27-12 01:00	0.00	0.00	Mar-27-12 01:00
☑ ppm3800a	GigabitEthernet0/2.ServiceInstance.3	🟩	☐	0.00	0.00	Mar-27-12 01:00	100.00	100.00	Mar-27-12 01:00	0.00	0.00	Mar-27-12 01:00
☑ ppm3800a	GigabitEthernet0/2.ServiceInstance.10	🟥	☐	0.00	0.00	Mar-27-12 01:00	100.00	100.00	Mar-27-12 01:00	0.00	0.00	Mar-27-12 01:00

You can create thresholds on device objects, such as CPUs and memory pools. For example, if you navigate to the Resources CPU, click a slot or CPU. Thresholds can be created on the CPU utilization.

In addition, you can create and apply report policies that modify report intervals when thresholds are crossed. For example, if a CPU nears 100% utilization, you can create and apply a report policy that reduces the polling frequency until it returns to normal. Conversely, you can create and apply report policies that increase polling frequencies when KPIs pass critical thresholds. For information about creating report policies, see Creating Report Policies, page 7-25.

To create a threshold, you provide the KPI onset and abate points. Onset is the rising or falling KPI value that, when reached, generates an alarm. Abate is he rising or falling KPI value that, when reached, clears the alarm. Additionally, you can specify the type of alarm you want raised, the days and times you want the threshold to run, and the number of required threshold-crossing occurrences before the alarm is raised or cleared.

As you prepare to create thresholds in Prime Performance Manager, keep the following in mind:

- Prime Performance Manager includes predefined thresholds that you can use as is or duplicate and modify to meet your needs. For a list of predefined thresholds, see Appendix C, “Predefined Thresholds.”
- Prime Performance Manager validates your threshold entries based on the KPI type, either rising or falling. For a rising threshold, for example interface availability down percentage, the higher alarm threshold value must be greater than the lower alarm. For a falling threshold, for example, interface availability up percentage, the higher alarm threshold must be lower than the one entered for the lower alarm.
- To avoid flooding the system with alarms, testing thresholds on a small group of devices before rolling them out to the full network is recommended.
- To avoid alarm flapping, set the abate value at a reasonable distance from the onset value. The distance depends on the expected KPI fluctuation. KPIs with larger fluctuations should have a wider onset-to-abate gap than KPIs with smaller fluctuations.
- Prime Performance Manager displays Add Threshold tools for any threshold-capable KPI, and excludes report, view, or dashboard data that cannot have thresholds created, such as name and description.
- The TCA is generated if the beginning of the data period falls within the active TCA range. For example, if data crosses a threshold between 1:15-1:30 and the TCA active period is defined as 1:00-5:00, the TCA is generated. If the TCA active period is 12:00-1:00, the TCA is not generated.
- After a TCA is generated, the onset and abate values are set to zero.

To create a Prime Performance Manager threshold:

Step 1 Log into Prime Performance Manager GUI as a System Administrator user.

Step 2 Display the report, view, or dashboard containing the KPI for which you want to create a threshold.

Step 3 Click the Add Threshold tool (green + icon) in the KPI column header.

The Add Threshold dialog box appears.

Step 4 Enter the threshold parameters:

- Name—Enter a unique name for the threshold.
- KPI Name—Is automatically generated from the report, view, or dashboard attribute name. It cannot be edited.
- KPI Report—Is automatically generated from the report, view, or dashboard name. It cannot be edited.
- KPI Type—Indicates the KPI type, either rising or falling. For a rising threshold, the critical alarm threshold must be higher than the major alarm threshold, and the major alarm threshold must be higher than the minor alarm. For falling KPI thresholds, the critical alarm entry must be lower than the major alarm, and the major alarm must be lower than the minor alarm.
- Report Data Interval—Choose the time interval when you want Prime Performance Manager to check the data point value identified by the threshold. Threshold intervals include:
  - 1 Minute

  - 5 Minute
  - 15 Minute (default)
  - Hourly
  - Daily
  - Weekly
  - Monthly

Note Verify that the report has these intervals enabled. Be default, Prime Performance Manager 15-minute, hourly, daily, weekly, and monthly intervals are enabled. To run a threshold every 5 minutes, you must enable 5-minute report interval. For information about configuring reports, see Chapter 7, "Managing Reports, Dashboards, and Views."

- Scope—Set the threshold scope. The scope indicates the devices for which you want the threshold reported. The "default" value means report the threshold for any reportable device. You can set the scope for a subset of devices, for example, you can choose Cisco7606s to report the threshold only for Cisco 7606 routers, and so on. The device groups that appear come from the Polling Groups tab. Device groups are based on the device types that are found during device discovery.

Note If you create a threshold on a device element, for example, a CPU, the element will be displayed in the Scope, for example, "...CPUNum=123".

- Description—Add any notes, as needed, to help describe the threshold. The field accepts any alphanumeric text.
- Enabled—The threshold is enabled by default. If you want to create the threshold but do not want to enable it, uncheck this box. You can enable the threshold later on the Threshold Editor window. For example, you might want to create all the thresholds first, review them in the Thresholds Editor window, then enable them at one time. For information about Thresholds Editor, see **Managing Thresholds, page 10-5**.
- Alarm Type—Indicate the alarm type you want raised: Communications, Processing Error, Environmental, QoS, or Equipment.
- Probable Cause—Threshold Crossed is the default probably cause. If you want to assign a different probably cause, choose one from the displayed list.
- Alarm Nature—Choose the alarm nature ADAC (automatically detected and automatically cleared), or ADMC (automatically detected and manually cleared). ADAC is the default.

Note If you set Alarm Nature to ADMC, abate values are not allowed. If you change a threshold from ACAC to ADMC, any existing abate values are cleared.

- Run Script—If you want a script to be run when the threshold is crossed, enter the script path here. The script can reside anywhere on your file system as long as you specify the full path, and the root user has the appropriate file and directory permissions to execute the script. If you enter an OSS host automation script, you can specify whether the threshold script has priority. See Editing Upstream OSS Hosts, page 9-13 and Tuning Event and Alarm Parameters, page 9-16 for more information.

  The following paramaters can be passed to scripts as $params:

  - Severity

  - OriginalSeverity
  - Action
  - Name
  - TcaName
  - TcaMetric
  - Message
  - ProbableCause
  - AlarmType
  - AckBy
  - ClearBy
  - AlarmNature
  - Category
  - IsAlarm
  - Element
  - DeviceType
- Mail To—If you want an e-mail generated when the threshold is crossed, enter the e-mail address here. If you enter an e-mail address, an e-mail server must be entered in the Event Editor Mail Server field. (To display the Event Editor, from the Administration menu, choose **Event Editor**. For more information, see Tuning Event and Alarm Parameters, page 9-16.)

  Note If you enter an e-mail address in the Mail To field here, it overrides e-mail addresses entered in the Event Editor Mail To field.

- Message Text—Allows you to define custom message to display when the TCA occurs. For example, the following text: TCA : $Severity : $TcaName : TcaMetric : $relation, would be displayed as the following message text when the alarm is raised:

  TCA : Critical : CPU_AverageUtilization_duplicate : CPU 5 Min Utilization 5 Minute/Average Utilization : value ‘23’ threshold ‘20’.

- Applicable—Enter the days for which you want the threshold applied. For example, you might only want to check some thresholds once a week, in which case, you would pick the day of the week when you want the threshold to apply. After selecting the days, enter the beginning and ending time in the Begin Time and End Time fields (hours and minutes) for which you want the threshold applied. If you enter the same value, the threshold is always applied.
- Threshold Values—Enter the threshold onset, abate, and number of occurrence values for the alarms you want raised: minor, major, critical:
  - Onset—Enter the onset threshold value(s) in the alarm box(es) that you want raised. You can set values for any or all alarm types. However, alarm entries must match the KPI type. For a rising KPI, the critical alarm threshold entry must be higher than the major alarm, and the major alarm threshold must be higher than the minor alarm. For a falling KPI type, the critical alarm threshold must be lower than the major alarm, and the major alarm must be lower than the minor alarm.
  - Abate—Enter the threshold value in the box of the alarm(s) when you want the alarm cleared. For a rising KPI type, the abate value must always be lower than the onset value. For a falling KPI type, the abate value must be lower than the onset.

Note If you do not define threshold values for all alarm levels, Prime Performance Manager skips them and goes to the next defined threshold level. For example, if you only define critical alarms, the threhold will go to normal after the the critical alarm reaches the abate level.

- Onset Occurrences—Enter the number of onset threshold crossings that must occur before the alarm is raised.
- Abate Occurrences—Enter the number of abate occurrences that must occur before the alarm is cleared.
- Report Policy Override—If you created a report policy for the specific alarm threshold, select the report policy here. Only user-created report policies are displayed.

  If you create report policies for each threshold level, the minor report policy is applied when the threshold crosses the minor level, the major report policy is applied when the threshold cross the major threshold, and the critical report policy is applied when it crosses the critical threshold level. If a threshold level does not have an associated report policy, the default report policy is applied.

  Individual TCA definitions and their associated report policy overrides are based on the KPI interval. If you apply a report policy to the threshold that excludes the TCA interval, the threshold will never clear. For example, suppose you create a default interface usasge report policy that includes the 5-minute, 15-minute, hourly, and daily intervals. You then create a custom interface usage report policy X that includes the 15-minute, hourly, and daily report intervals, but not the 5-minute interval. Suppose you create an interface usage TCA for the 5-minute interval and assign report policy X to the Critical level report policy Override . When this threshold is exceeded, report policy X is applied but the TCA will never clear because the underlying KPI is not generated by the report policy (X).

Step 5 Click **OK**.

The TCA is added to the gateway thresholds. To view and edit the thresholds, from the Network menu, choose **Threshold Editor**. For more information, see Chapter 10, “Managing Thresholds.”

Managing Thresholds

Prime Performance Manager thresholds can be viewed, edited, disabled, enabled, and deleted from the Thresholds Editor, shown in Figure 10-2. The editor displays thresholds added from the Prime Performance Manager reports GUI (see Creating Thresholds, page 10-1), and ones created using an XML editor and added directly to the gateway. Threshold management is covered in the following topics:

Editing Thresholds from the Threshold Editor, page 10-6

Enabling and Disabling Thresholds, page 10-9

Deleting Thresholds, page 10-10

Editing Thresholds from the Alarms Window, page 10-7

Displaying Threshold Events, page 10-10

Editing Thresholds from the Threshold Editor

You can edit thresholds either by displaying the Threshold Editor, selecting a threshold, and entering your edits, or by selecting a threshold alarm in the Active Alarms window and editing the threshold there.

To edit a threshold using the Threshold Editor:

Step 1 Log into Prime Performance Manager GUI as a Network Operator or higher user.

Step 2 From the Network menu, choose **Threshold Editor**.

Step 3 In the Actions column of the threshold you want to edit, click **Edit This [*Rising/Falling*] Threshold**.

Step 4 In the Edit Thresholds dialog box, edit any of the following values.

Note Only brief parameter descriptions are provided here. For detailed descriptions, see Creating Thresholds, page 10-1.

- Name—The threshold name (not editable).
- KPI Name—The key performance indicator name (not editable).
- KPI Report—The report containing the KPI (not editable).
- KPI Type—The KPI type, either rising or falling.
- Report Data Interval—The time interval when you want Prime Performance Manager to check the data point value identified by the threshold.
- Scope—Indicates the devices for which you want the threshold reported.
- Description—Edit or add any threshold notes.
- Enabled—Enables and disables the threshold.
- Alarm Type—Indicate the alarm type you that is raised: Communications, Processing Error, Environmental, QoS, or Equipment.
- Probable Cause—Indicates the TCA probable cause.
- Alarm Nature—Indicates the alarm nature, either ADAC or ADMC.
- Run Script—If you want a script to be run when the threshold is crossed, enter the script path here. See Editing Upstream OSS Hosts, page 9-13 and Tuning Event and Alarm Parameters, page 9-16 for more information.
- Mail To—If you want an e-mail generated when the threshold is crossed, enter the e-mail address here.
- Message Text—Allows you to define custom message to display when the TCA occurs.
- Applicable—Edit the days for which you want the threshold applied.
- Threshold Values—If needed, edit the threshold onset, abate, number of occurrence values, and report policy for the critical, major, or minor alarms you want raised.

  Note If a report policy is applied to the threshold, an asterisk appears in the Onset and Abate columns with onset and abate values if a report policy is set for that level. If you move your mouse over the cell with the asterisk, the report policy name is displayed.

Step 5 When finished, click **OK**.

The edits are displayed in the Thresholds Editor.

Editing Thresholds from the Alarms Window

From the Prime Performance Manager Alarms window can perform the following perform the following actions from a threshold crossing alarm:

- Display threshold parameters (all users).
- Edit threshold parameters (administrator users only).
- View a report for the threshold crossing (all users).

When threshold crossing alarms occur, you can display the threshold parameters from the Alarms window:

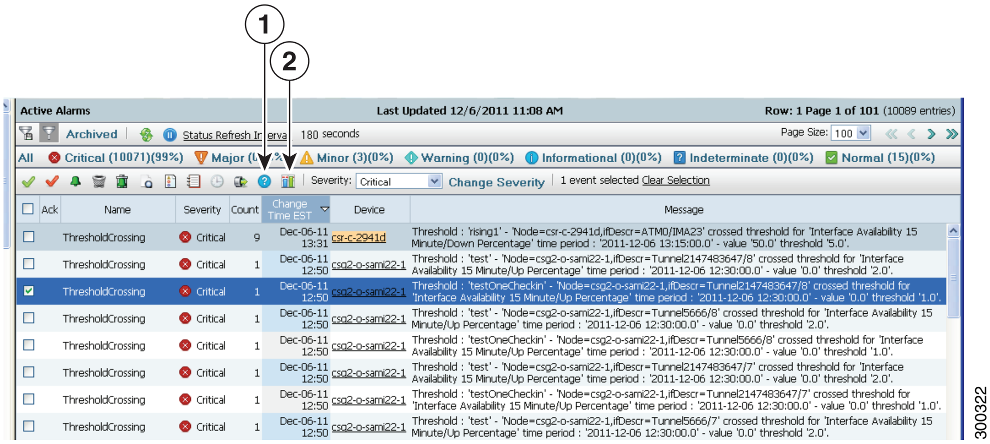
Step 1 Log into the Prime Performance Manager GUI.

Step 2 From the Network menu, choose **Alarms/Events**.

Step 3 In the Active Alarms window (Figure 10-2), choose a Threshold Crossing alarm.

Step 4 From the Active Alarms window toolbar, click **Help for Event**.

Figure 10-2 Displaying Threshold Parameters from the Alarms Window



Last Updated 12/6/2011 11:08 AM

Row: 1 Page 1 of 101 (10089 entries)

Status Refresh Interval 180 seconds

Page Size: 100

Severity: Critical

1 event selected

☐	Ack	Name	Severity	Count	Change Time EST	Device	Message
☐		ThresholdCrossing	Critical	9	Dec-06-11 13:31	csr-c-2941d	Threshold : 'rising1' - 'Node=csr-c-2941d,ifDescr=ATM0/IMA23' crossed threshold for 'Interface Availability 15 Minute/Down Percentage' time period : '2011-12-06 13:15:00.0' - value '50.0' threshold '5.0'.
☐		ThresholdCrossing	Critical	1	Dec-06-11 12:50	csg2-o-sami22-1	Threshold : 'test' - 'Node=csg2-o-sami22-1,ifDescr=Tunnel2147483647/8' crossed threshold for 'Interface Availability 15 Minute/Up Percentage' time period : '2011-12-06 12:30:00.0' - value '0.0' threshold '2.0'.
☑		ThresholdCrossing	Critical	1	Dec-06-11 12:50	csg2-o-sami22-1	Threshold : 'testOneCheckin' - 'Node=csg2-o-sami22-1,ifDescr=Tunnel2147483647/8' crossed threshold for 'Interface Availability 15 Minute/Up Percentage' time period : '2011-12-06 12:30:00.0' - value '0.0' threshold '1.0'.
☐		ThresholdCrossing	Critical	1	Dec-06-11 12:50	csg2-o-sami22-1	Threshold : 'test' - 'Node=csg2-o-sami22-1,ifDescr=Tunnel5666/8' crossed threshold for 'Interface Availability 15 Minute/Up Percentage' time period : '2011-12-06 12:30:00.0' - value '0.0' threshold '2.0'.
☐		ThresholdCrossing	Critical	1	Dec-06-11 12:50	csg2-o-sami22-1	Threshold : 'testOneCheckin' - 'Node=csg2-o-sami22-1,ifDescr=Tunnel5666/8' crossed threshold for 'Interface Availability 15 Minute/Up Percentage' time period : '2011-12-06 12:30:00.0' - value '0.0' threshold '1.0'.
☐		ThresholdCrossing	Critical	1	Dec-06-11 12:50	csg2-o-sami22-1	Threshold : 'test' - 'Node=csg2-o-sami22-1,ifDescr=Tunnel2147483647/7' crossed threshold for 'Interface Availability 15 Minute/Up Percentage' time period : '2011-12-06 12:30:00.0' - value '0.0' threshold '2.0'.
☐		ThresholdCrossing	Critical	1	Dec-06-11 12:50	csg2-o-sami22-1	Threshold : 'testOneCheckin' - 'Node=csg2-o-sami22-1,ifDescr=Tunnel2147483647/7' crossed threshold for 'Interface Availability 15 Minute/Up Percentage' time period : '2011-12-06 12:30:00.0' - value '0.0' threshold '1.0'.
☐		ThresholdCrossing	Critical	1	Dec-06-11 12:50	csg2-o-sami22-1	Threshold : 'test' - 'Node=csg2-o-sami22-1,ifDescr=Tunnel5666/7' crossed threshold for 'Interface Availability 15 Minute/Up Percentage' time period : '2011-12-06 12:30:00.0' - value '0.0' threshold '2.0'.

1	Help for Event tool	**2**	Report for Event tool

Step 5 The View Thresholds dialog box or the Edit Threshold dialog box (administrator users) displays the following threshold values.

> **Note** Only brief parameter descriptions are provided here. For detailed descriptions, see Creating Thresholds, page 10-1.

- Name—The threshold name (not editable).
- KPI Name—The key performance indicator name (not editable).

- KPI Report—The report containing the KPI (not editable).
- KPI Type—The KPI type, either rising or falling.
- Interval—The frequency at which Prime Performance Manager checks the data point value identified by the threshold.
- Scope—Set the threshold scope (not editable).
- Description—Edit or add any threshold notes.
- Enabled—Enables and disables the threshold.
- Alarm Type—Indicates the alarm type that is raised: Communications, Processing Error, Environmental, QoS, or Equipment.
- Probable Cause—Indicates the TCA probable cause.
- Alarm Nature—Indicates the alarm nature, either ADAC or ADMC.
- Run Script—If you want a script to be run when the threshold is crossed, enter the script path here. See Editing Upstream OSS Hosts, page 9-13 and Tuning Event and Alarm Parameters, page 9-16 for more information.
- Mail To—If you want an e-mail generated when the threshold is crossed, enter the e-mail address here.
- Message Text—Allows you to define custom message to display when the TCA occurs.
- Applicable—Edit the days for which you want the threshold applied.
- Threshold Values—Enter the threshold onset, abate, and number of occurrence values for the alarms you want raised: minor, major, critical

Step 6 When finished, click **OK**.

Step 7 To view a report for the threshold crossing, in the Alarms window toolbar, click **Report for Event**. A threshold report is displayed. The report is in graph format by default. For information about

The threshold crossing report window appears.

Step 8 When finished, click **OK**.

Duplicating Thresholds

You might occasionally want to create a new threshold with only one or two changes from an existing threshold. If so, you can duplicate the existing threshold, modify the parameters and save the new threshold.

To duplicate a threshold:

Step 1 Log into Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Network menu, choose **Threshold Editor**.

Step 3 In the Actions column of the threshold you want to edit, click **Duplicate This Threshold**.

Step 4 In the Duplicate Threshold dialog box, edit any of the following values.

Note Only brief parameter descriptions are provided here. For detailed descriptions, see Creating Thresholds, page 10-1.

- Name—The original threshold name is displayed with “duplicate” appended at the end. You can edit the threshold name. The name must be unique.
- KPI Name—The key performance indicator name (not editable).
- KPI Report—The report containing the KPI (not editable).
- KPI Type—The KPI type, either rising or falling.
- Interval—The frequency at which Prime Performance Manager checks the data point value identified by the threshold.
- Scope—Set the threshold scope (not editable).
- Description—Edit or add any threshold notes.
- Enabled—Enables and disables the threshold.
- Alarm Type—Indicate the alarm type you that is raised: Communications, Processing Error, Environmental, QoS, or Equipment.
- Probable Cause—Indicates the TCA probable cause.
- Alarm Nature—Indicates the alarm nature, either ADAC or ADMC.
- Run Script—If you want a script to be run when the threshold is crossed, enter the script path here. See Editing Upstream OSS Hosts, page 9-13 and Tuning Event and Alarm Parameters, page 9-16 for more information.
- Mail To—If you want an e-mail generated when the threshold is crossed, enter the e-mail address here.
- Message Text—Allows you to define custom message to display when the TCA occurs.
- Applicable—Edit the days for which you want the threshold applied.
- Threshold Values—Enter the threshold onset, abate, and number of occurrence values for the alarms you want raised: minor, major, critical

Step 5 Click **OK**.

Enabling and Disabling Thresholds

To enable or disable a threshold:

Step 1 Log into Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Network menu, choose **Threshold Editor**.

Step 3 In the Actions column of the threshold you want to enable or disable, check (enable) or uncheck (disable) the **Enable This Threshold** check box.

Prime Performance Manager will update the threshold information.

Note You can also enable and disable thresholds using the “Editing Thresholds from the Alarms Window” procedure on page 10-7.

Filtering Thresholds

To filter the displayed thresholds:

Step 1 Log into Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Network menu, choose **Threshold Editor**.

Step 3 In the Search field, enter the text that you want to use to filter the thresholds. For example, to filter the thresholds by response time, enter Responsetime.

Step 4 Press **Enter**.

Prime Performance Manager filters the thresholds by the text you entered.

Step 5 To display all thresholds, delete the text from the Search field and press **Enter**.

Deleting Thresholds

To delete a threshold:

Step 1 Log into Prime Performance Manager GUI as a System Administrator user.

Step 2 From the Network menu, choose **Threshold Editor**.

Step 3 In the Actions column of the threshold you want to delete, click the **Delete This Threshold** tool.

Step 4 On the confirmation, click **OK**.

Prime Performance Manager will remove the threshold from the table.

Displaying Threshold Events

To view threshold events, from the Navigation menu, choose **Alarms/Events**, then click **Event History**. The types of threshold events that appear include:

- All threshold crossing events, for example:

```
Threshold : 'rising1' - 'Node=csr-c-2941d,ifDescr=ATM0/IMA23' crossed threshold for
'Interface Availability 15 Minute/Down Percentage' time period : '2011-12-06
10:30:00.0' - value '50.0' threshold '5.0'.
```

  and

```
Threshold : 'rising1' - 'Node=csr-c-2941d,ifDescr=ATM0/IMA23' is below threshold for
'Interface Availability 15 Minute/Down Percentage' time period : '2011-12-06
10:15:00.0'
```

- All threshold user creation or edition activities, for example:

```
Gateway: node123- Threshold rising1 - Threshold2811 - 15 Minute was overwritten by
user123.
```