CHAPTER 13

Customizing Filters and Domains

Introduction

TrafficDirector is shipped with the capability to respond to most network management needs. However, you can customize TrafficDirector to conform to your specific network management requirements. This chapter describes the two primary tools you can use to customize TrafficDirector, Filter Editor and Domain Editor.

Creating Custom Data Filters with Filter Editor

Before you initiate a data capture session or create a custom domain, you need to decide the type and extent of the data to collect for display and analysis. You select an appropriate filter to screen the incoming data at the time you initiate a data capture session or create a custom domain.

TrafficDirector is shipped with a number of predefined filters. These filters should handle most data capture and domain requirements. If you need filtering parameters that are not available in the existing filters, however, you can use Filter Editor to edit existing filters or create new filters that meet your requirements. You can view the list of available filters by invoking the Domain Editor's Add function (see "Defining a New Domain").

To collect only selected data, you can create a set of filters that are either inclusive or exclusive, and that pass, capture, and store only the packets that meet the filter criteria.

Filter creation begins with a filter format that uniquely describes the specific characteristics of the frame which must be matched for acceptance or rejection of data packets from the data capture buffers. Filter formats are based on the detailed structure of the seven-level protocol stack that makes up a transmission frame.

TrafficDirector includes a substantial number of preestablished formats for the most commonly used stacks. You can create new filters using these formats to explore a current problem, or define and store them for later use. To get a list of the filter formats that are available, use the Add function in the Filter Editor (see "Adding a NTo add a new filter, follow these steps:.").

When you've created the appropriate filter, you insert it into the filter definition to be used for the data capture session. You can create highly selective filters that eliminate extraneous detail that may otherwise obscure the protocol decode process.

The TrafficDirector Filter Editor has four functions:

- Adding a new filter definition.
- Editing an existing filter definition.
- Viewing an existing filter definition.
- Deleting an existing filter definition.

Adding a NTo add a new filter, follow these steps:.

Step 1 Select **Filter Editor** from the TrafficDirector main window. The Filter Editor window appears.

Step 2 Select **Add**. The Add Filter window appears.

Step 3 Enter a name for the new filter in the **Filter Name** field. This can be a maximum of 15 letters and must begin with a letter. You can use only letters, numbers, dashes, and underscores. The name is not case-sensitive.

Step 4 Select a format for the new filter from the **Filter Formats** list. Then click on **Select Format** to add the filter format.

Step 5 For certain filters, some parameters are already filled in. Fill in additional fields as needed.

Step 6 Click on **OK** to add the filter. The filter now appears on the filter list.

Editing Filter Definitions

To edit an existing filter definition:

Step 1 Click on **Filter Editor** from the TrafficDirector main window. The Filter Editor window appears.

Step 2 Select the filter you want to edit from the filter list in the Filter Editor window.

Step 3 Click on **Edit.** The Edit Filter window appears. This window is the same as the Add Filter window, except that existing fields are already filled in. Change the fields you want to edit.

Step 4 Click on **OK** to create the new filter or **Cancel** to quit.

Note You can use Edit Filter as an easy way to create a new filter with characteristics similar to an existing filter. Simply edit the fields that are different, change the filter name, and save the new filter.

Viewing Filter Definitions

Before using a filter in the Data Capture tool, or creating a new filter, you can look at the field definitions for one or more existing filters. You can view the field definitions for an existing filter without changing any filter information.

To view exiting filter definitions:

Step 1 Select **Filter Editor** from the TrafficDirector main window. The Filter Editor window appears.

Step 2 Select the filter you want to view from the filter list in the Filter Editor window.

Step 3 Click on **View**. The View Filter window appears. It is the same as the Edit Filter window, but you cannot change any fields.

Step 4 Click on **OK** when you are finished viewing the filter.

Deleting a Filter Definition

When you no longer need a filter, you can delete the filter definition to conserve system resources.

To delete a filter definition from the filter list:

Step 1 Select **Filter Editor** from the TrafficDirector main window. The Filter Editor window appears.

Step 2 Select the filter you want to delete from the filter list in the Filter Editor window.

Step 3 Click on **Delete**. A cautionary window appears asking if you really want to delete the filter.

Step 4 Click on **OK** to delete the filter definition, or **Cancel** to quit without deleting the filter definition.

Defining and Editing Domains Using Domain Editor

TrafficDirector is shipped with a number of standard domains already defined. These domains let you monitor most types of network traffic. If these are not sufficient, you can use the Domain Editor tool to create new domains or edit existing domains to meet your monitoring needs.

When you define a domain, you determine the subset of network traffic that the domain represents. Once you define a domain, you can install it on one or more agents and monitor that portion of network traffic.

In this section, you'll learn how to define new domains, modify existing domains to meet new monitoring requirements, and delete domains when you no longer need them.

Defining a New Domain

The Domain Editor lets you add, edit, and delete domain definitions. When a domain is defined, you can attach it to one or more agents. TrafficDirector is shipped with a number of predefined domains. However, you can define a custom domain to monitor a specific subset of traffic on your network.

To define a new domain, follow these steps:

Step 1 Select **Domain Editor** from the TrafficDirector main window. The Domain Editor window appears .

Step 2 Select **Add**. The Add Domain window appears.

Step 3 Enter the name of the domain as you want it to appear throughout TrafficDirector. This can be a maximum of 15 letters and must begin with a letter. You can use only letters, numbers, dashes, and underscores. The name is case-insensitive.

Step 4 Select the **Domain Type**. Inclusive means that a packet is accepted into the domain if it matches any of the filters. Exclusive means that a packet is accepted into the domain if it *fails* to match all of the filters. The default is Inclusive.

Step 5 Select the **Packet Type**. This is the kind of packet accepted as part of the domain. Good selects only good packets. Bad selects only bad packets. All selects all packets. The default is All.

Step 6 The **Tokenring RIF Field** is a routing information field for Token Ring networks only. If you do not have a Token Ring network, leave this field blank. If you have a Token Ring network, fill in the appropriate routing information for your network.

Step 7 Select the filters you want to use. These filters determine the type of packets the new domain will recognize. If you select Inclusive as the domain type, these are the packets the domain will pass. If you select Exclusive, these are the packets the domain will reject. You can associate up to 16 filters with a domain.

Step 8 Click on **OK** to define the new domain or **Cancel** to return to the Domain Manager window.

Note When you add a domain, you define it, but it has no practical function until you **install** it on one or more agents. To install a domain on an agent, see "Installing Domains at Agents" in Chapter 6.

Editing or Viewing an Existing Domain Definition

You can change a domain's definition in order to monitor a different subset of network traffic. You can also use the Edit Domain function to create a new domain by modifying an existing domain, and then renaming it. You can view the parameters of an existing domain without editing it. You can also edit a previously defined domain whether it is attached to an agent or not.

To change or view the information for an existing domain:

Step 1 Select the domain you want to edit from the Agent Summary area in the Domain Editor window.

Step 2 Click on **Edit** or **View** from the Domain Editor window. The Edit Domain or View Domain window appears. These windows are the same as the Add Domain window, except that the fields are already filled in for the selected domain.

Step 3 If you selected **Edit**, change the fields you want to modify. If you selected **View**, you can view the window but not make any changes.

Step 4 Click on **OK** to modify the domain, or **Cancel** to return to the Domain Manager window.

Deleting a Domain Definition

When you no longer need to monitor the subset of network traffic defined by a domain, you can delete the domain definition to save resources.

To delete a domain definition from TrafficDirector:

Step 1 Select the domain you want to delete from the Agent Summary list box in the Domain Editor window.

Step 2 Click on **Delete** from the Domain Editor window. A cautionary prompt appears, asking if you want to continue.

Step 3 Click on **OK** to delete the domain definition, or **Cancel** to return to the Domain Editor window.