CHAPTER 3

Getting Started

Introduction

This chapter tells you how to get started with TrafficDirector. You'll learn about the TrafficDirector main window, and how to use TrafficDirector to monitor your network.

In this manual, you'll learn how to use TrafficDirector in two stages. This chapter presents a general overview of network monitoring and troubleshooting with TrafficDirector. In the remaining chapters, you'll find detailed descriptions of the tasks you can perform with TrafficDirector and the tools you use to perform these tasks.

This chapter provides an overview of the following topics:

- Adding agents and agent groups to TrafficDirector (you need to do this first, before you can do anything else with TrafficDirector).
- Monitoring overall network traffic.
- Zeroing in on different types of network traffic to get a closer look at network activity and problems.
- Setting alarms on different types of network traffic to detect specific network problems and activity.
- Creating reports of various types of network statistics.

The information in this manual is presented in sequential form, from general to specific network monitoring. However, in practice you can use any tool you want to, at any time, to meet your network monitoring and troubleshooting needs. The presentation in this chapter provides a systematic description of TrafficDirector, and shows you with a general way to proceed to use the product.

Window Conventions

Any window that appears in TrafficDirector is referred to either as a **window** or as a **dialog** box, depending on its function. Within each window are **menus**, which provides lists of choices. Beneath menus on some windows are **selection buttons**. Selection buttons initiate a single action when you select them, rather than presenting a list of choices.

Windows can also contain **displays**, in which TrafficDirector presents graphical network data, and **list boxes**, which contain tabular data related to the window function.

Dialog boxes can contain **fields for data entry**, selection buttons, or both.

Mouse Conventions

You perform all mouse selection with the left mouse button. The terms **select** and **click on** refer to a single mouse click.

Entering Window Information

When you enter information into TrafficDirector windows, there are a few restrictions you'll have to keep in mind. They are:

- All names (agents, filters, domains, etc.) must start with a letter.
- Names can contain only letters, numbers, dashes, and underscores.
- Agent and agent group names can contain a maximum of 15 characters, and are case-sensitive.
- Domain and filter names can contain a maximum of 15 characters, and are case-sensitive.
- All numeric data entries are decimal integers unless specifically stated otherwise.

Using a Printer

TrafficDirector lets you print most screens that contain graphs and numerical data. You can also print reports. To print graphical screens, you must have a postscript printer. To print numerical data, you can use any convenient printer.

Starting TrafficDirector

To start TrafficDirector from the UNIX command line, do the following:

- Make the TrafficDirector installation directory your current directory.

  ```
  cd $NSHOME/bin
  ```

- Enter the command **tdir &.**

Note This assumes that you have added the TrafficDirector environment settings to your **.cshrc** file. See Chapter 2 "Installing TrafficDirector Software" for more details.

The TrafficDirector Main Window

When you start TrafficDirector, the Main window appears. Here, you can choose from several menu items and three groups of icons to perform most of TrafficDirector's functions. You can also use the Main window to add agents and agent groups to TrafficDirector, and to edit agents you've already added. This is very important, since TrafficDirector does not recognize the existence of an agent until you've added it using the functions in the Main window.

The TrafficDirector tools represented by each icon are described in the following chapters of this manual.

Note Not all TrafficDirector tools may be available at your site. If you select a tool that is not available, a message appears telling you that it is not supported.

Exiting TrafficDirector

You can exit TrafficDirector at any time. When you do, all changes you've made such as adding agents and agent groups and installing domains are retained.

To exit TrafficDirector:

Step 1 Select the **File** menu on the TrafficDirector Main window.

Step 2 Click on **Exit**.

Selecting and Using TrafficDirector Tools

TrafficDirector tools are described in this manual. They are:

- Protocol Monitor
- Traffic Monitor
- Alert Monitor
- Resource Manager
- Domain Manager
- Data Capture
- Protocol Decode
- Remote Login
- Filter Editor
- Domain Editor

You can launch all TrafficDirector primary functions from the Main window. Applications are launched from primary tool windows.

Using Multiple Windows

You can open multiple TrafficDirector tools at the same time. You can also open multiple windows of the same tool at once. When you do this, however, remember that each window has an independent sample rate (30 seconds, 1 minute, etc.), so updates can be different with different windows. Thus, you can be monitoring the same data with two versions of the same window, and the data may appear different.

Also remember that when you open multiple windows you use extra network resources. It is good practice to open only the windows you need to do your work.

Using TrafficDirector

In the sections that follow you'll find a brief description of each major type of network monitoring, such as monitoring all traffic for several agents, examining host traffic, traffic in a single domain, and so forth. Each description is accompanied by a chart that shows the steps necessary to perform this function. These flow charts are repeated in the chapters that follow, and can also serve as a handy reference later on.

Each section also references the chapter that contains a detailed description of the monitoring function.

The functions described in the next section are:

- Adding agents and agent groups; configuring agents (Main window, Remote Login).
- Getting an overview of network traffic (Traffic Monitor and Protocol Monitor).
- Getting RMON statistics for a single domain (Segment Zoom).
- Examining host activity (Host List, Host Zoom, and Host Conversations).
- Getting a graphical segment history and statistics (Short-Term History, Long-Term History, and Segment Statistics graphs).
- Monitoring network resources (Resource Manager).
- Installing and deinstalling domains (Domain Manager).
- Creating and viewing alarms (Watchdog, Alarm Monitor).
- Generating reports (Report Generator).
- Customizing TrafficDirector (Filter Editor, Domain Editor).

Adding Agents and Agent Groups

Before you use TrafficDirector to monitor data, you need to add at least one agent in the Single Agent list box. The agent or probe must already be installed and operational on a network segment. Once you've added an agent, TrafficDirector can use it to monitor segment data.

An agent group is a collection of one or more agents. TrafficDirector handles an agent group as though it were a single agent, enabling you to collectively monitor network statistics from more than one segment or point on a segment.

A description of adding agents and agent groups appears in Chapter 4, "Adding and Modifying Agents and Agent Groups."

Configuring an Agent from TrafficDirector

Since agents on a particular network may be physically located almost anywhere, it is often impractical to change agent parameters at the agent itself. Once you've added an agent to TrafficDirector you can change its parameters directly from the management console using Remote Login.

Remote Login is discussed in detail in Chapter 4, "Adding and Modifying Agents and Agent Groups."

Getting an Overview of Network Traffic

The first thing to do in a network monitoring or troubleshooting situation is get an overview of network traffic. This will help you decide which aspects of network traffic to examine more closely.

You can get an overview of network traffic using three TrafficDirector tools:

- **Traffic Monitor** is TrafficDirector's most general network monitoring tool. It lets you monitor Enterprise-level statistics for multiple agents/segments for a single domain. Figure 3-6 shows you how to use Traffic Monitor to do this. For example, you can use Traffic Monitor to compare the packet rate or utilization in different segments.
- **Protocol Monitor** is similar to Traffic Monitor, except that Protocol monitor lets you monitor multiple remote sites by domain, protocol or application. You can also customize Protocol Monitor to present the graphical display of your choice.

- **Domain Manager** is a multi-segment, multi-domain tool. Use Domain Manager to monitor network traffic in specific domains; that is, to monitor RMON statistics for a specific subset of RMON traffic (such as IP, IPX, or DECNET). It is called a manager rather than a monitor because you also use it to install and de-install domains (which change the agent).

These tools are described in detail in Chapter 5 “Monitoring Your Network Using Traffic Monitor and Protocol Monitor.”

Applications that let you zoom in on specific traffic are described in the next section.

The tools described in this section provide you with a good overview of network operation. The next section covers tools to zoom in on specific portions of your network to monitor selected traffic and locate problems.

Monitoring RMON Statistics from a Single Domain

You use Traffic Monitor, Protocol Monitor, and Domain Manager to provide an overview of network traffic. Once you identify the possible sources of a network problem, you can zero in on specific parts of the network to examine the traffic more closely. Single-agent, single-domain tools help you do this.

In this section, you’ll find a flow chart that shows you how to view RMON statistics from a single domain using the Segment Zoom application. The Segment Zoom windows you actually see display different statistics depending on the type of network, Ethernet, Token Ring, FDDI, or WAN. The tools described in this section are discussed in more detail in Chapter 8, “Monitoring and Troubleshooting Single Domains.”

Monitoring Host Activity

Once you’ve isolated a network problem to a specific segment and domain using Segment Zoom, you may see unusual activity associated with a specific host. You may also suspect a host of having problems for other reasons, or simply want to monitor that host.

You monitor host activity using the Host Zoom application and the Host List and Host Conversations windows. Host-monitoring tools are described in detail in Chapter 8, “Monitoring and Troubleshooting Single Domains.”

Viewing Segment Statistics and History Graphs

You can examine a segment in detail by viewing three graphs. These statistics are different, depending on whether the segment is Ethernet, Token Ring, WAN, or FDDI:

- **Segment Statistics Graph.** Provides four data views for the selected segment:
  - — Vital Signs. A measure of the general health of the segment. Includes Broadcasts, Multicasts, errors, etc.
  - — Size Distribution. Indicates the percentage of each packet size (18, 64, 128, etc.).
  - — Destination Breakdown. Shows packet destinations by Ucasts, Bcasts, and Mcasts.
  - — Error Breakdown. Shows where errors are occurring.
- **Short-Term History Graph.** Provides short-term data (residing in the selected agent**)** for a brief time period you select.
- **Long-Term History Graph.** Provides long-term data (residing in the selected agent**)** for a longer time period you select.

The Segment Statistics and History graphs are described in detail in Chapter 8, “Monitoring and Troubleshooting Single Domains.”

Monitoring Network Resources

It is very useful to monitor network resources from a central point. For example, you may want to be alerted if the utilization of a router exceeds a certain point, if a host stops responding, or if the disk space on a server falls below a certain level.

The remote monitoring of critical network resources has traditionally been problematic because polling the resource from the network manager occupies excessive bandwidth, tying up valuable network resources.

TrafficDirector’s Resource Manager lets you select and monitor network resources without tying up the network. Resource Manager is a single-agent, single-domain tool that combines both DomainView and remote SNMP management in a single device. This device provides active management for all critical resources at the remote site (including private MIBs), while eliminating regular polling between management station and agent.

The result is that the *agent* polls the resource. Polling is thus limited to the segment and does not tie up the network.

Note To use Resource Manager, the agent must be a SwitchProbe agent equipped with the Resource Manager option.

You can see the results of your resource monitoring in the Resource Manager window. In addition, you can use Watchdog to set up traps. In this way, you’ll be notified when selected resource conditions occur.

For example, suppose you want to monitor available disk space on a server. First, use Resource Manager to create a proxy resource on the agent to read the MIB variable for server disk space. (This assumes that the MIB on the agent you use has a variable that reads this value.) Then select a host so that the agent knows which device you are referring to. You can now use Watchdog to create a trap that triggers an alarm when the disk space variable falls below a pre-determined value.

The agent polls the resource at the interval you specified when you set up the proxy resource, and triggers an alarm when the disk space falls below the specified threshold.

Resource Manager lets you select either of two types of proxy resource:

- Remote Protocol Ping (IP Ping), which tells you if the resource is responding.
- Remote SNMP “get,” which provides the value of the variable and detects any errors in reading the variable.

Resource Manager is described in detail in Chapter 9, “Managing Remote Resources Using Resource Manager.”

Capturing, Decoding, and Viewing Protocol Information

Protocol Decode lets you examine previously-captured data packets stored in a user-defined file.

Use Protocol Decode when you want to see the contents of individual data packets. You can specify the way you want the data decoded and displayed, and limit the amount and type of data you'll see by specifying filters. As an option, you can specify your filter so that it either passes or rejects captured data frames that match its pattern.

You must first use Data Capture to create a file containing the data you want to decode.

Protocol Decode is described in detail in Chapter 8, "Monitoring and Troubleshooting Single Domains."

Installing and Deinstalling Domains

Domain Manager lets you view network traffic and activity associated with selected domains in selected agents. A domain is a subset of network activity that you want to monitor. You use Domain Manager to monitor RMON statistics for specific domains, or subset of segment traffic, such as IP, IPX, or DECNET.

TrafficDirector is shipped with a number of standard domains already defined. These domains should be sufficient for most network monitoring needs. However, you can also define your own domains at any time, as well as edit previously defined domains by using Domain Editor. Domain Editor is described in detail in Chapter 13, "Customizing Filters and Domains."2

You must install a domain before you can use it. When a domain is installed on an agent, TrafficDirector sends SNMP messages to that agent enabling data collection for the domain. For example, if a domain is defined as all IP traffic, you can install it both on an agent in New York called NYC and an agent in Paris called PARIS. You can then monitor IP traffic on both segments directly from your TrafficDirector console.

You can deinstall a domain to free agent resources when you no longer need the RMON traffic monitored by the domain.

Installing and deinstalling domains is described in Chapter 5, "Monitoring Your Network Using Traffic Monitor and Protocol Monitor."

Setting Alarms

It is impractical to continuously monitor a segment or device visually. Instead, you can use Watchdog to set alarms on the variables you want to monitor.

An *alarm* is a definition of a condition based on rising or falling data rates (or both). When this predefined condition occurs, it is called an *event*. When you set an alarm on a network device, the alarm detects an event when it occurs, and does two things:

- It records the event in the agent.
- It sends a notification, called a *trap*, to the TrafficDirector informing it that an alarm has occurred.

The Alarm Monitor in the TrafficDirector window blinks until you acknowledge it by selecting it. You can also create UNIX script files that execute network or system functions.

Watchdog lets you establish multiple alarms on selected events associated either with an agent/domain combination, or with a resource. It sends an alarm message (trap) when the data reaches the predefined threshold. You can view a list of previous alarm messages using the Alarm Monitor tool. Watchdog is described in detail in Chapter 12, “Setting Alarms Using Watchdog.”

Generating Reports

TrafficDirector provides comprehensive logging and reporting tools. You can set up and generate a variety of reports using the Report Generator, which you launch from the Domain Manager **Tools** menu. Reports can also be generated from command line. Logging and reporting is described in detail in Chapter 14, “Logging and Reporting.”

Table 3-1 summarizes the types of reports that TrafficDirector can provide using Report Generator. Each report is discussed individually in Chapter 14.

Table 3-1 Types of Reports

Report type (type parameter)	What it gives you	Why you use it
Segment Statistics (**seg-stats**)	A summary of segment traffic for the selected segment and domain during the report period.	To get an overview of network traffic for the specified agent and domain.
Segment Details (**seg-details**)	One line of output for each pair of log files available for the selected period.	To get more detail about the specified agent and domain, and to create a comma- or tab-delimited CSV data file that you can use as input to a word processor, database, or spreadsheet.
Conversation Statistics (**conv**)	A summary, for the selected agent and domain, of traffic between each pair of hosts that have talked during the report period.	To see both halves of each conversation listed together, sorted according to the metric you select and including either all conversations or only the top N conversations.
Host-Summary (**host**)	A summary of host traffic for the selected agent and domain during the report period, sorted according to the metric you select. You can choose to include one host or only the top N hosts.	To get an overview of host traffic for the selected agent and domain.

Table 3-1 Types of Reports

Report type (type parameter)	What it gives you	Why you use it
Host-Verbose (**host-verbose**)	A tabular-format report, identical to the Host (summary) report, with the information for each host expanded.	To view the details of the host traffic for the selected agent and domain for the selected hosts, sorted according to the metric you select and including either all hosts or only the top N hosts.
Host-Outbound (**host-outbound**)	A report similar to the Host-Verbose report listing only outbound statistics.	To view the details of the outbound host traffic for the selected agent and domain for the selected hosts, sorted according to the metric you select and including either all hosts or only the top N hosts.
Multi-Domain (**multi-domain**)	Comparative segment statistics for a hierarchy of domains for a specified agent, based on a tree of domains that you define.	Since domains often correspond to protocol layers, use this report to provide a Protocol Distribution, showing traffic at multiple protocol layers.
Billing (**billing**)	A report on the amount and cost of inter-subnet traffic over a LAN/WAN segment during the report period.	To analyze traffic flow between the specified subnets of your network and to determine the cost of that traffic.

Customizing TrafficDirector

TrafficDirector comes with a set of predefined data filters. These filters will take care of most of your data capture and domain requirements. If you need filtering parameters that are not available with existing filters, you can use Filter Editor to create new filters or edit existing filters for your requirements.

TrafficDirector also includes a number of predefined domains. These let you monitor most types of network traffic. However, 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 select a subset of segment traffic that the domain represents. You can install the domain on one or more agents and monitor that portion of network traffic. The Filter Editor and Domain Editor are described in detail in Chapter 13, “Customizing Filters and Domains.”