CHAPTER 1

Overview of TrafficDirector

Introduction

TrafficDirector is a software package that lets you monitor, troubleshoot, and record information about your network's operation. TrafficDirector helps you identify and isolate a wide variety of fault conditions in data communications networks.

TrafficDirector works as a distributed system. It uses a central management console running TrafficDirector software in conjunction with data-gathering agents located at various points on a network. It can simultaneously collect wide-ranging statistical data, display selectively captured and fully decoded network traffic, set user-defined alarm conditions, and obtain real-time updates from all segments of a widely dispersed internetwork. TrafficDirector accomplishes this from a centralized, SNMP-compatible network management console.

TrafficDirector is based on two standards that enable it to operate in a multi-topology, multi-vendor environment:

- The **Simple Network Management Protocol (SNMP)**, which defines the protocol for all inter-communications between TrafficDirector, SwitchProbe devices, and Cisco Internetwork Operating Systems (IOS™) RMON agents.
- The **Remote Monitoring Management Information Base (RMON-MIB)**, which defines the type of information that is to be gathered and made available to the user for each network segment.

TrafficDirector has four main functions:

- Monitoring network traffic, measuring the flow of data
- Capturing network traffic and recording it for later examination
- Interpreting raw network data and translating it into a graphic form that you can then view and analyze
- Setting limit conditions on network traffic and generating alarms if those limits are exceeded

TrafficDirector gathers and analyzes network information using SwitchProbes and Cisco IOS RMON agents attached to network segments.

SwitchProbes

SwitchProbes are enhanced RMON probes that you attach to a specific network segment. The SwitchProbe agent gathers statistical information for that segment and provides a window into the segment which you use to observe and analyze network data.

A typical network has multiple segments and multiple agents. Normally, one agent is attached to each network segment.

SwitchProbe agents communicate with managers using the SNMP protocol either in-band (using the same network facilities as all other network nodes) or out-of-band (using a communications medium separate and distinct from the user network).

TrafficDirector currently supports SwitchProbes for Ethernet, Token Ring, Fiber Distributed Data Interface (FDDI), Copper Distributed Data Interface (CDDI), and Fast Ethernet local-area networks (LANs).

TrafficDirector

TrafficDirector is a set of software application programs from which you issue operational commands to SwitchProbes and Cisco IOS RMON agents to gather and analyze network information. TrafficDirector displays all results and diagnostic information.You can have multiple TrafficDirector programs active simultaneously within a single network, even working with the same SwitchProbe or IOS RMON agent.

Versions of TrafficDirector are available for the Sun SPARC, HP 9000, and IBM RS6000 platforms, and for Microsoft Windows.

TrafficDirector controls network data acquisition and analysis by configuring SwitchProbes, then obtaining network data from them and analyzing this data. When you use TrafficDirector you have full control over what network data is acquired and how this data is analyzed and displayed.

When a SwitchProbe is attached to a network segment it becomes a node on the network. As such, it “hears” all transmissions on the network, regardless of how they’re addressed. It can also analyze and record information about those transmissions. Also, many Cisco internetworking devices have embedded IOS RMON agents which provide monitoring of segments attached to that device.

Network Terminology

This section describes terms common to standard communication networks as well as terms exclusive to TrafficDirector and its agents.

Standard Communication Terminology

IP address — The four-byte Internet Protocol address convention that uniquely identifies each node on the network. Simple Network Management Protocol (SNMP) uses IP addresses to identify nodes to interrogate and manage. SNMP is the underlying protocol used for TrafficDirector communications.

The format of the IP address is X.X.X.X, where X is an integer with a decimal value of 0 through 255.

MIB — SNMP network devices store information about themselves in a Management Information Base (MIB) that resides at an agent. A MIB contains “managed objects” (variables) that describe the characteristics and current state of a network device. You can manage an SNMP device by querying or setting its MIB variables.

A standard or public MIB is one in which the definitions of the MIB variable have been approved by a standards organization (the IETF) and published for general use. A private MIB is one in which the set of variables is vendor-defined. Private MIBs are typically developed to extend a standard MIB, such as RMON-MIB, to collect specific segment traffic unique to the vendor’s network devices.

Network A group of interconnected nodes that can communicate with one another and that use the same network address.

Multiple network segments can be interconnected to form an **internetwork.** Data is passed from network to network by devices such as bridges, routers, and gateways on the basis of individual network addresses.

Node An individually addressable location on a data communications network.

In RMON-MIB terminology, a Host and a Node are identical. A node is a network connection in any of a variety of physical devices such as personal computers, larger scale server computers, printers, etc. A physical device can have multiple connections to a network and therefore may comprise multiple nodes.

Segment A network or subnet in which all nodes are physically and logically connected in such a way that all nodes receive all data traffic seen by all other nodes on the segment.

Thus, a segment can be either a single physical bus or loop, or may be interconnected by repeaters that pass all traffic. A segment cannot be connected by bridges, routers, or gateways, since these devices logically separate networks.

TrafficDirector Terminology

Agent An agent is a piece of software installed on a specific network segment to gather statistical information for that segment. An agent can be included in a specialized hardware and software package, such as SwitchProbe, that you connect specifically to monitor a network segment. It can be software included in an existing network device, such as the embedded IOS RMON agent found in many Cisco devices. The agent includes the MIB that stores device information, and provides a window into the network segment that you use to observe and analyze network data.

Agent Group An agent group is a user-defined collection of agents used to consolidate and organize information about the network.

Domain A domain is an RMON-based virtual monitor that lets you monitor a subset of network traffic. This concept is important to understanding and using TrafficDirector, and is explained fully later in this chapter.

Scope The user-defined set of agents and domains that TrafficDirector monitors.

Watchdog Watchdog is a tool that lets you monitor network activity and devices proactively. Watchdog lets you establish alarm thresholds on selected events, using either rising or falling data rates (or both). When the data reaches a threshold that you've specified, the watchdog sends an alarm message.

Conversations A Conversation is the TrafficDirector name for the set of statistics (RMON Matrix group table entries) that describe the traffic between pairs of hosts.

Domains

In the TrafficDirector architecture, a domain is a virtual RMON monitor. A domain lets you monitor RMON statistics (Top N Talkers, conversations, watchdog, etc.) for a specific subset of network traffic such as IP, IPX, or DECNET. You can monitor segment traffic on the physical, protocol, or application level.

Domains are not limited to protocols. You can also define a domain as an application, such as Lotus Notes, or a device, such as a router.

You can use pre-defined domains to obtain RMON statistics for specific protocols, or add a custom domain, such as **xyz**, and obtain RMON statistics for that domain. The special pre-defined domain, ALL, provides RMON statistics for *all* the other domains in the segment (the sum of the statistics in the other domains).

The OSI Protocol Model

Protocols are the rules by which data communications devices carry out their communication process. The generalized model for protocols is the Open Systems Interconnections (OSI) model. This model includes seven layers, each of which carries out a particular subset of the communications process.

The seven-layer model is often described as a **stack** or **suite**. By examining these protocol stacks you can often identify network malfunctions.

The OSI protocol model is:

APPLICATION
PRESENTATION
SESSION
TRANSPORT
NETWORK
DATA LINK
PHYSICAL

The functions of each layer are:

Physical Layer — The physical layer specifies the physical and electrical characteristics of the connections that make up the network, such as twisted pair cables, coaxial cables, repeaters, and so forth. This layer is sometimes called the hardware layer.

Data Link Layer — The data link layer recognizes the electrical representation of the data (bit patterns, encoding methods, and so forth). Errors are detected at this level and corrected by requesting the retransmission of corrupted packets.

Network Layer — The network layer switches and routes the packets as required to get them to the correct destination. It addresses and delivers message packets.

Physical Layer	The physical layer specifies the physical and electrical characteristics of the connections that make up the network, such as twisted pair cables, coaxial cables, repeaters, and so forth. This layer is sometimes called the hardware layer.
Transport Layer	The transport layer controls the sequencing of message components and regulates inbound traffic flow when more than one packet is in process. It recognizes and discards duplicate packets.
Session Layer	The session layer enables applications running at two workstations to coordinate their communications into a single session. It supports the creation of the session, manages packets sent back and forth during the session, and terminates the session.
Presentation Layer	The presentation layer converts data either into or from a particular machine's native internal numeric format.
Application Layer	The application layer is the point at which a message to be sent across the network enters the OSI model. User interfaces are present at this layer.

The TrafficDirector Protocol Model

Various network protocols (such as IBM, TCP/IP, DECNET, VINES, etc.) are based on the OSI standard protocol stack. As an example, a protocol interpreter suite is shown below. Notice the correspondence with the standard OSI protocol stack.

TrafficDirector contains a set of filters used to isolate an individual protocol from other network traffic. A second filtering process (domains) separates out the components of the protocol stack for each supported protocol. Thus, using Data Capture, you can select only specific traffic, such as IBM traffic, in a segment by using a filter that passes only IBM traffic. Then you use Protocol Decode to separate each packet (also called a "frame") into its component layers and decode each layer according to the selected protocol.

The RMON-MIB Standard

The first standard for network management evolved into a specification that became known as Simple Network Management Protocol (SNMP). SNMP was given RFC number 1098 by the Internet Engineering Task Force (IETF). By embedding the basic SNMP MIB within data communication devices, multi-vendor management systems can manage these devices from a central site and view information graphically.

SNMP has significant limitations. It allows regular polling of devices, but does not provide for extensive active monitoring of critical functions or the monitoring of network traffic on a LAN segment. SNMP-based devices can identify only traffic specifically addressed to themselves and cannot provide statistics on conversations *between* devices—an important concept for network troubleshooting. RMON-MIB is designed to address many of these limitations.

RMON-MIB, (Remote MONitoring-Management Information Base) was developed by the IETF (Internet Engineering Task Force) and became a standard in 1992 as RFC number 1271. The RMON-MIB specification was developed to provide traffic statistics and analysis on many network

parameters for comprehensive network fault diagnosis, planning, and performance tuning. In 1994 RFC 1513 was added. RFC 1513 specifies characteristics associated with the token ring topology. RFC 1757 for Ethernet RMON was released in 1995, obsoleting RFC 1271.

RMON-MIB delivers seamless multi-vendor interoperability between SNMP management stations and monitoring agents. It also provides a standard for a set of MIBs which collect rich network statistical information not available from the standard SNMP MIB.

Finally, RMON-MIB allows active network diagnostics through a powerful Alarm Group that lets you set thresholds for critical network parameters to automatically deliver alerts to centrally located management consoles.

Basic RMON Groups

This section describes the basic RMON-MIB groups. An RMON-MIB group is a related set of variables used with RMON functions, such as monitoring and collecting certain types of data, setting alarms, and event trapping. RMON goes far beyond SNMP in providing useful tools for network monitoring.

The basic RMON-MIB groups for Ethernet/Token Ring networks are:

Statistics For Ethernet, the statistics include packets, packet distribution, octets, broadcasts, collisions, dropped packets, fragments, CRC alignment errors, undersize/oversize, etc.

For Token Ring, statistics are compiled in promiscuous and MAC-layer modes including packets, octets, broadcasts, multi-casts, packet distribution, dropped packets, line/burst/abort/lostframe/token/ AC/ congestion/ frame copied errors, drop/ RingPurge/beacon events, etc.

History Stores multiple samples of values from the Statistics group, so you can compare the current behavior of a selected variable with its performance over the specified period.

Alarms You can set a wide variety of thresholds and sampling intervals on any statistic to create an alarm condition. Threshold values can be an absolute value, a rising or falling value, or a delta value. You can fully customize each node or segment.

Host A table for each active node that includes a variety of node statistics, including the time the node was discovered. The host table lets you gather data for all nodes. This data is retrievable under SNMP, even for non-SNMP devices.

Host Top N A user-defined study of sorted host statistics. Host Top N provides detailed information for the stations that have transmitted or received the most frames for a selected RMON host table object during the last study period. Host Top N is calculated locally by the agent, substantially reducing network traffic.

Matrix Shows how the amount of traffic and number of errors between any pair of nodes, either by source or by destination address, are changing over time.

Filters You can define specific packet match filters and have them serve as a stop/start mechanism for all packet capture activity.

Packet Capture Under the control of the selected filters, matched packets are captured and stored for further analysis. You can select buffer sizes and have the buffers either wrap or stop when full.

With managers equipped with the protocol decode function, you can send captured packets to the centralized network management console, providing distributed protocol analysis.

Events — Let you create entries in a monitor log or generate SNMP traps from the agent to the manager. Events can be initiated by a crossed threshold on any counter or from a specific packet match count.

Events may, in turn, trigger other functions such as a data capture session. The log includes the time of day for each event and a description of the event.

Ring Station — A collection of information specifically related to Token Ring configuration and operational characteristics. This group includes Token Ring statistics for each node, for each node in ring order, and for each node based on source routing.

Using Domains

The original RMON standard supports network monitoring of link layer traffic only. This means that it can present statistics only for aggregate traffic, not statistics for the different layers of various protocol stacks (such as IP, FTP, IPX). Because it is not capable of monitoring at the network layer, an RMON device cannot distinguish traffic on its segment that originated across a router. By not monitoring above the MAC layer, many useful applications, such as monitoring WAN links, measuring client-server response time, or providing seven-layer protocol statistics, are not possible.

Domains provide an architecture that allows the monitoring of network traffic for all seven ISO layers within the framework of the RMON standard. Using domains lets you monitor any protocol traffic for any device or subnet on any segment of an enterprise network.

TrafficDirector supports three host address modes: MAC, NET, and SUBNET. In the MAC address mode, host and matrix tables are built using the six-byte physical-layer MAC address as specified by the RMON standard. TrafficDirector includes the RMON domain, which is used with third-party RMON agents to monitor MAC-level (plain vanilla) RMON statistics.

In the NET address mode, TrafficDirector creates host and matrix tables containing network addresses for IP, IPX, and DECNET packets.

- For IP packets, the NET-mode address is the four-byte IP address (example: 45.20.0.20)
- For IPX packets, the address is the IPX host address (example: 08002B534256)
- For DECNET packets, the address is the area.node address (example: 1.1023)

SUBNET address mode is similar to NET address mode, except that the agent uses subnet addresses for collection purposes. The resulting host and matrix tables thus contain total statistics for each subnet. TrafficDirector uses only IP, IPX, and DECNET packets to create the tables.

The management of remote network segments is critical to providing high network availability. Key network management standards such as RMON and SNMP are the technology enablers to build the tools, such as TrafficDirector, to manage distributed networks.

- With RMON, network statistics can be gathered for problem resolution. Active monitoring alerts the administrator to problems before they become critical.
- With domains, many more network traffic parameters, devices and LAN Segments can be monitored for the most effective and focused problem resolution.
- With SNMP, devices can be regularly pinged and the device status can be polled from a central site.

Resource Management

Network administrators must constantly balance the cost of network management versus that of network availability. Network administrators are increasingly using RMON probes to monitor LAN traffic because of the economic benefits derived from distributing management devices onto critical remote network segments —whether in a large corporate facility or across the country.

However, SNMP management creates problems due to the amount of bandwidth needed to obtain SNMP management information from a remote site. The dilemma for the administrator is that if network management bandwidth is minimized for SNMP polling and ping sweeps, then network fault conditions will be missed, jeopardizing the health of the enterprise network. Also, because SNMP is not active (it has a limited alarm capability), problems are flagged only after a query (polling) is made from a central site.

The ideal solution is to combine the use of domains and remote SNMP management (resource management) into a single, cost-effective device that can provide active management for all critical resources at the remote site, while also eliminating expensive and congestive regular polling. The integration of these two important network management technologies has resulted in TrafficDirector Resource Manager.

Note Resource Manager is available as an option on all SwitchProbes. It is *not* available on agents provided by other vendors.

SNMP-based network management systems have the ability to obtain status information and statistics for network devices by utilizing the SNMP “get” command to query MIB variables (objects) of interest. However, this must be performed with continuous polling. Since a network can involve hundreds or even thousands of devices with each device having hundreds of MIB variables, present SNMP-based device management is extremely inefficient. Furthermore, MIB I, MIB II, and private MIBs do not provide features for setting alarms, eliminating any method of recording and notification when selected resources reach predetermined values.

Resource Manager lets you efficiently monitor the resources of any SNMP device. To do so, the TrafficDirector console downloads MIB variables selected from a list to the agent, creating *proxy resources* at the agent. Now, instead of polling from the management console, the agent polls each resource at a selected interval and records the result.

You can select either an SNMP “get” resource or an IP ping resource.

In addition, you can set alarms in the agent and be notified when any variable reaches a predetermined value. In this way, the agent notifies the management console only when an alarm condition sets off a trap, eliminating continuous polling.

Protocol Analysis

A basic capability of TrafficDirector is its ability to have its agents selectively gather network traffic in the form of frames from any operational segment protocol, node, or conversation, store that information in a file in the agent and then transmit the file to TrafficDirector on command. TrafficDirector’s Protocol Decode application reads the data file and breaks each captured packet into individual protocols. You can then view or print either the raw data (in byte form) or a full seven-frame decode.

The following list shows the protocols supported by the TrafficDirector protocol decode software.

Table 1-1 Protocols Supported by TrafficDirector Protocol Decode Software

Ethernet	IEEE8023	IEEE8025	IEEE8022
DODIP	DODARP	DODRARP	DODICMP
DODGGP	DODTCP	DODUDP	DODSMTP
DODFTP	DODTFTP	DODDNS	DODTLNT
DODNTB	DODNTDAT	DODNTNAM	DODSMB
NOVIPX	NOVSPX	NOVRIP	NOVECHO
NOVERRP	NCP	XNSIPX	XNSSPX
XNSRIP	XNSECHO	XNSERRP	XNSPEXP
XNSSMB	DECDRP	DECMOPDL	DECMOPRC
DECLAT	DECLDATA	DECNSP	DECSCP
DECDAP	DECNICE	DECFOUND	DECCTERM
DECSMB	APPLAP	APPARP	APPSDDP
APPLDDP	APPNBP	APPATP	APPZIP
APPRTMP	APPAEP	APPPAP	APPASP
APPDSP	APPAFP	VINESIP	VINESRTP
VINESARP	VINESICP	VINESIPC	VINESSPP
VINESMM	VINESST	VINEMAIL	SNMP
SUNNFS	SUNRPC	SUNMOUNT	SUNPMAP
SUNYP	SNAXID	SNATH	IBMNETB
SNARHREQ	SNARHRES	SNARU	SNAFM
SNAPS	IBMSMB	CLNS	ES-IS
TP 0/2/4	ISO-Session	ISO-Presentation	FTAM
X400			