CHAPTER 7

Examining Captured Packets Using Protocol Decode

Introduction

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

You have two options when you use Protocol Decode:

- You can use Protocol Decode as part of a real-time data capture process:
  - Start data capture from an agent, using Data Capture.
  - Stop data capture after an appropriate interval.
  - Upload the captured data to a file.
  - Examine the individual frames with full seven-layer decoding using the Protocol Decode application.
- You can run Protocol Decode at any time on a file that contains previously captured or collected data.

Note TrafficDirector can convert and use data captured in Sniffer format by Network General Corporation's Sniffer™ Network Analyzer.

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

Capturing Data to a File Using Data Capture

Before you can use Protocol Decode, you must first use Data Capture to capture packets selectively from an RMON agent, and save them in a file. You can capture the desired traffic for either standard or user-defined protocols.

Once you've captured the data you want to examine, you can analyze it using the Protocol Decode tool.

To set up a data capture session:

Step 1 Select an agent from the Agent list box in the TrafficDirector Main window.

Step 2 Click on **Data Capture** from the TrafficDirector Main window. The Data Capture window appears. Note that the agent name appears at the top of the window.

Note Select **Delete** to remove the current data capture configuration in the agent. The capture setup remains configured until you delete it, even if the Data Capture window is closed.

Step 3 Enter the information in the appropriate fields in the Data Capture window. Each field is described below.

Step 4 Click on **Start**. This initiates an SNMP session that instructs the selected agent to begin collecting packets in accordance with the filter definition.

Step 5 Click on **Stop** to end the data capture session. The captured data is stored in a buffer in the agent. If you selected the mode Lock When Full, the data capture function stops automatically.

Step 6 Click on **Upload** to transfer the captured data from a buffer in the agent to the file you have specified in the Captured File Name field. The default file is **tmp.dat**.

When the upload process begins, a status report showing the number of packets uploaded appears in the lower margin of the window.

Step 7 When you have uploaded the data and you want to decode it, use Protocol Decode from the TrafficDirector window, or click on the **Decode** button from the Data Capture window to initiate protocol decode.

Note You can decode the uploaded file at any time, using the **Decode** button from the Data Capture window, or Protocol Decode from the TrafficDirector main window.

The Data Capture Window

This section describes the contents of the Data Capture Window.

Data Field	What it Contains
Captured File Name	The name of the file in which the packets from the agent are uploaded. This file is stored in the $NSHOME/usr directory. The file name 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-sensitive. The default file name is **tmp.dat**
Mode	Determines whether the session halts when the capture buffer is full. **Lock When Full** stops the session when the capture buffer is full. **Wrap When Full** lets the capture session continue when the buffer is full, with the most recent packets overwriting the earliest, until you click on the **Stop** button. The default mode is **Lock When Full**.

Data Field	What it Contains
Buffer Size	The maximum number of bytes to be saved in this capture buffer, including any implementation-specific overhead. Select either KB or MB. The range is from 32 - 8192 KB or from 1 - 8 MB. The value must be a decimal number. The default buffer size is 64 KB.
Slice Size	The maximum number of bytes of each packet that are saved in the capture buffer. For example, if a 1500 byte packet is received and **Slice Size** is set to 500, then only 500 bytes of the packet are stored in the associated capture buffer. The range is from 0 - 1518 bytes. If you set Slice Size to 0, the capture buffer saves the entire packet. The value must be a decimal number. The default slice size is 128 bytes.
Address Type	You can specify address type as either MAC or IP. The address or symbol entered at Source and Destination Address is interpreted on this basis. The default address type is MAC.
Source/Destination Address (two fields)	Valid MAC address, valid IP address, or valid Name are allowed. TrafficDirector uses these addresses to create more specific filters related to the source/destination of the data to be captured. MAC addresses must be in the format: 01-23-45-67-89-ab. IP addresses must either in dotted IP notation (for example: 204.205.206.207). Name must be a valid host name.
Direction	Determines whether to capture traffic from source-to-destination only (**Single**), or in both directions (**Both**). The default direction is **Both**.
Filter Type	**Inclusive** captures all traffic if the specified conditions *are* matched. **Exclusive** captures all traffic if the specified conditions are *not* matched. The default filter type is **Inclusive**.
Update Interval	The duration, in seconds, of the time between status field updates. The value must be a decimal integer. The fields are described below. The minimum and also the default value is 5 seconds. The maximum value is 99 seconds.

TrafficDirector updates the following status fields while data capture is running:

Started @	The date and time at which the packet capture function was initiated.
Buffer Status	If capture is already on, Buffer Status displays “Running” and the time the capture was started. If capture is stopped, it displays “Stopped.” If a capture entry does not exist, this field displays “Not Known”. It also shows buffer status in brackets (“Full” or “Available”).

Data Field	What it Contains
Captured Packets	The number of packets captured in the agent with the matched condition. This field is periodically updated during the capture sequence.
Filter List	You select one or more filters from this list. Remember that the Filter Type field determines whether the filters you select are exclusive or inclusive.

Clearing the Data Capture Buffer

You may want to stop a data capture session and clear the buffer. To do so, use the **Delete** button.

Getting Agent Information

To get a description of the Agent you're using for data capture:

Step 1 Select the **Tools** menu.

Step 2 Select Agent Info. The Agent Information window appears.

Step 3 Select **OK** to dismiss the window.

Exiting the Data Capture Window

To exit the Data Capture window:

Step 1 Select the **File** menu.

Step 2 Select Exit.

Decoding Captured Data Using Protocol Decode

Once you've captured data into a file, you can decode it, one frame at a time.

This section starts with a general overview of how to perform a protocol decode, followed by descriptions of each function.

Using Protocol Decode

To examine individual frames using Protocol Decode:

Step 1 Make sure the data you want to analyze is captured in a file, and you know the file name and path..

Step 2 Select the Protocol Decode icon from the TrafficDirector Main window. The Protocol Decode window appears.

Step 3 Load the data capture file you want to examine (see "Loading a Data Capture File" below). The data appears in the Protocol Decode list box. Each line is one frame.

Step 4 Select the frame you want to decode.

Step 5 Using the **Properties** menu, determine how the data is to be decoded.

Step 6 If needed, select **Post-Capture Filtering** for additional filtering. See "Filtering Previously Captured Data Using Post-Capture Filters."

Step 7 Perform protocol decode in either Raw mode or Summary mode as described beginning on "Viewing Decoded Data in Raw Byte Form."

Loading a Data Capture File

Before you can perform a protocol decode, you must load the captured data file. To do so:

Step 1 Select **Load** from the **File** menu in the Protocol Decode window. The Select File window appears.

Step 2 Select the directory and file that contains the captured data you want to decode from the list boxes. Use the directory filter to help you select files. To use the filter, enter a directory path and file filter, such as ***.dat**, then select **Filter**.

Note The data is stored in a file with the file name **xxx.dat**.

Step 3 Select **OK** to load the data capture file, or **Cancel** to quit. The file information appears in the list box on the Protocol Decode window. It is listed by frame number.

Selecting Protocol Decode Properties

Before you decode a frame, you can modify four properties that determine how decoded data in each mode is displayed. To determine protocol decode properties, select the **Properties** menu on the main Protocol Decode window. The Properties window appears.

The selection fields simplify the process of specifying the protocol decode properties. These fields contain toggle buttons that you can click to indicate your preferences. The following describes each of the selection fields and its contents.

Selection Field	What It Does
Raw Mode	Determines whether the decoded bytes are displayed in Raw Mode as **ASCII** or **EBCDIC** characters. The default is **ASCII**.
Time Mode	Determines whether the time displayed is **Absolute** (Month-Day-Time in *secs.msecs*) or **Delta** (time difference between the arrival of the current frame and the previous frame, in *hh:min:sec:msecs*). The default is **Absolute**.
Address Mode	Sets the Source/Destination address display as Network (IP), Vendor, or Hex. The default is Network.
Zoom Mode	Enables and disables the multi-paneled, multi-color effect in the 7-layer Protocol Decode window. The default is Enable.

Make your selection for each field, then **Apply** to put your selections into effect or **Cancel** to cancel these selections and return to the previous window.

Performing Protocol Decode

There are four ways you can view a data captured file:

- **Summary Mode**. The complete file is displayed in the Protocol Decode window list box when you load it. Each line represents a frame of captured data. It has not yet been decoded.
- **Raw Mode**. A single frame you select is decoded and presented in raw byte form.
- **Protocol Decode** mode. A single frame you select is decoded and presented in full seven-level format.
- **Zoom Mode**. Any of the seven layers, as appropriate for the packet being decoded, can be displayed in the full window.

You'll learn more about each of these modes in this section.

Viewing a Data Capture File in Summary Mode

Before you perform a protocol decode, the file you selected appears in summary mode in the list box on the Protocol Decode window. Each frame is represented by a single line numbered from 1 to N, where N is the total count of frames in the capture buffer.

The summary mode list box information is:

List Box Entry	What it Tells You
Pkt ID	The index number of the frame, starting with 1. You can scroll through the list of frames by using the cursor. The frame currently selected is highlighted.
Timestamp	The timestamp indicating the date and time this frame was captured. The format of the timestamp is: *Month Day hh:mm:ss:ttt.* For example, **Dec 7 17:32:25.569**.
Size	The number of bytes in the frame.
Source Node	The address of the node that sent that frame. If Vendor Name is the default, however, the name of the node is displayed instead.
Destination Node	The address of the destination node specified in the frame. If Vendor Name is the default, however, the name of the vendor appears instead.

List Box Entry	What it Tells You
Status	If a frame is faulty, the type of fault (more than one may apply): • **R** indicates a runt frame (a frame less than 12 bytes long). • **J** indicates a jabber frame (a frame more than 1516 bytes long). • **C** indicates a CRC and alignment error frame. • **P** indicates a processing error. For example, Frame #40 with a processing error indicates that the agent was not able to process packets just prior to capturing Frame #40. • --> indicates a packet from DTE to DCE (WAN only). • <-- indicates a packet from DCE to DTE (WAN only).
Protocol	Identifies the highest-level protocol in that frame.

The selection buttons in the Protocol Decode window (Summary Mode) let you specify the parameters for the decoding function. The selections are:

Selection Button	What It Does
Change Mode	Lets you switch directly to Protocol Mode or Raw Mode.
GoTo Packet	Use **Goto Packet** to show the first frame on the first line (**Home**) or the last frame on the last line (**End**). Selecting either selection initiates the action. You can use the scroll arrows to scroll either forward or backward through the frames.
Packet Number	Inserting a frame number in the **Packet Number** field causes that frame to appear on the first line.

Viewing Decoded Data in Raw Byte Form

Raw mode presents decoded data in raw byte form.

To view protocol information in Raw Mode, Select **Raw** in the **Change Mode** field on the main Protocol Decode window. The Raw Mode window appears.

The list box headings include Frame Number, Size, Arrival Time, and display mode (ASCII or EBCDIC).

The selection buttons in the Raw Decode window let you specify the parameters for the decoding function. The selections are:

Selection Button	What It Does
Change Mode	Lets you switch directly to Protocol Mode.
GoTo Packet	Lets you jump immediately to either the first frame displayed in the list box (**Home**) or the last (**End**).
Packet Number	Lets you display a specific frame in the list box. Inserting a packet number in the **Frame Number** field displays the raw decode of that frame. Selecting the Up/Down arrows in the Frame Number field causes the raw mode frame display to scroll up or down one frame at a time.

The name and path of the capture file appears at the bottom of the window.

Viewing a Frame in Seven-Level, Decoded Format

Selecting **Protocol** in the Change Mode field of either the Protocol Decode window or the Raw Decode window displays the highlighted frame in seven-level, decoded format. The decoding is fully automatic and causes the frame to display in up to seven list boxes, each of which corresponds to successive layers of the protocol.

Using the scroll bars on the list boxes, you can scroll through each protocol layer and examine in detail the contents of each layer (of the ISO 7-layer model) expressed in a readable format. If the frame contains no identifiable protocol after a certain layer, the rest of the frame is displayed as a raw dump in the last list box, labelled User Data.

Viewing a Single Protocol Layer Using Zoom Mode

Select **Zoom** using the Change Mode selection button in the Protocol Decode window to see a full-window display of any of the protocol layers contained in the current frame. The Zoom window lets you scroll forward or backward through the protocol layers by selecting the **Next Layer** or **Prev Layer** selection buttons, respectively. The display wraps from the highest-layer decode back to the lowest layer decode, and vice versa.

You can examine new frames by using any of the techniques described earlier to scroll through the frames displayed in the Summary Mode window.

Filtering Previously Captured Data Using Post-Capture Filters

Sometimes you may want to filter previously captured data to isolate protocol information you need. You can do this using the Post-Capture Filters. To use these filters:

Step 1 Load the data capture file (see "Decoding Captured Data Using Protocol Decode").

Step 2 Select **Post-Capture Filtering** from the Protocol Decode window. The Post-Capture Filters window appears.

Step 3 Select the filter definition you want to use.

Step 4 Select **Apply**. The Summary Mode list box on the Protocol Decode window now contains only packets that have passed your Post-Capture Filter definition.

The selection fields simplify specification of the parameters for post-capture filtering. These fields contain toggle buttons that you can click to indicate your preferences. The following describes each selection field and its contents.

Selection Button	What it Does
Address Type	You can specify the address type as either MAC or IP. The address or symbol entered in the Source and Destination Address field are interpreted according to this setting. A valid MAC address, valid IP address, or valid Name is allowed. Use these addresses to create more specific filters related to the source or destination of the data to be captured.
Source/Destination Address	Select **Source Address** or **Destination Address** to specify source and destination addresses for filtering.
Both Directions	Determines whether to capture traffic from source-to-destination only, or in both directions. Select **Yes** to filter data in both directions, **No** to filter data in only one direction.
Filter Type	Can be either inclusive or exclusive. Inclusive means capture all traffic if the specified condition is matched. Exclusive means capture all traffic that does not specify the specified condition.