SNIFFER® NETWORK ANALYZER OPERATIONS — VERSION 4.3

Network General Corporation

SNIFFER® NETWORK ANALYZER OPERATIONS

✓

Network General Corporation

SNIFFER® NETWORK ANALYZER

OPERATIONS

DISCLAIMER OF WARRANTIES

The information in this document has been reviewed and is believed to be reliable; nevertheless, Network General Corporation makes no warranties, either expressed or implied, with respect to this manual or with respect to the software and hardware described in this manual, its quality, performance, merchantability, or fitness for any particular purpose. The entire risk as to its quality and performance is with the buyer. The software herein is transferred "AS IS."

Network General Corporation reserves the right to make changes to any products described herein to improve their function or design.

In no event will Network General Corporation be liable for direct, indirect, incidental or consequential damages at law or in equity resulting from any defect in the software, even if Network General Corporation has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of implied warranties or liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Document prepared by Network General Technical Publications.

March 1993

P/N: 20028-004

Table of Contents

List of Figures

Chapter 1. Sniffer Network Analyzer Overview

Chapter 2. Defining System Options

Chapter 3. Capturing Frames

Chapter 4. Displaying Interpreted Frames

Chapter 5. Managing Names and Working with Files

Chapter 6. Using Protocol Forcing

Chapter 7. Generating Traffic

Chapter 8. The Sniffer–LM2000 Conversion Utility

Chapter 9. Using the Sniffer Analyzer Files

List of Procedures

Chapter 1. Sniffer Network Analyzer Overview

Chapter 2. Defining System Options

Chapter 3. Capturing Frames

Chapter 5. Managing Names and Working with Files

Chapter 6. Using Protocol Forcing

Chapter 7. Generating Traffic

PREFACE

Preface

About This Manual

This manual describes the functions and operations of the Sniffer® analyzer, a software component of the Sniffer Network Analyzer™ . It also provides recommendations on how to use the analyzer effectively to detect and solve network problems.

The Sniffer Network Analyzer observes the local or wide area network to which it is attached, and displays the monitored activity.

Manuals for the Sniffer Network Analyzer

Figure i lists the manuals that accompany the Sniffer Network Analyzer. These manuals describe normal operations.

If the product shipment includes release notes or README files on disks, the information in the notes or files supersedes the information in this manual.

For Information On....	Read...
Installing and configuring the Sniffer Network Analyzer.	*Sniffer Network Analyzer: Model xx Installation Guide*
Operating the Classic features of the Sniffer Network Analyzer. General information on the Sniffer Network Analyzer.	*Sniffer Network Analyzer Operations* (this manual)
Operating the Expert features of the Sniffer Network Analyzer.	*Expert Sniffer Network Analyzer Operations*
Accelerated overview of Expert analyzer operations. For those who don't like to read documentation.	*Quickstart*
Operating the monitor functions on an Ethernet network. Using the monitor features effectively to detect network abnormalities.	*Sniffer Network Analyzer: Ethernet Monitor Operations*
Operating the monitor functions on a token ring network. Using the monitor features effectively to detect network abnormalities.	*Sniffer Network Analyzer: Token Ring Monitor Operations*
Operating the monitor functions on an FDDI network. Using the monitor features effectively to detect network abnormalities.	*Sniffer Network Analyzer: FDDI Monitor Operations*

Figure i. Manuals for the Sniffer Network Analyzer.

For Information On....	Read...
Various network and protocol types.	*Sniffer Network Analyzer: Network and Protocol Reference*
Remote^2 Manager.	*DCA Remote2 Supplement*

Figure i. Manuals for the Sniffer Network Analyzer.

Organization of This Manual

Figure ii describes the organization of this manual.

Chapter/Appendix	Contents
Table of Contents List of Figures List of Procedures Preface	For many tasks, the manual includes a step-by-step procedure. Procedures are listed in the *List of Procedures*.
Chapter 1, "Sniffer Network Analyzer Overview."	Provides an overview of the Sniffer Network Analyzer and describes its capabilities. Also defines key terms, lists new functions, and provides an introduction to the user interface.
Chapter 2, "Defining System Options."	Describes global options that apply to all networks, as well as options for particular networks or platforms.
Chapter 3, "Capturing Frames in Classic Mode."	Describes how to prepare for capture, including setting capture filters, screen format options during capture, and a trigger to stop capture.
Chapter 4, "Displaying Interpreted Frames."	Describes the procedures for filtering, interpreting, displaying, and printing captured frames. Also provides general background information about protocol analysis.
Chapter 5, "Managing Names and Working With Files."	Describes the analyzer's name table and how to use data (trace) and setup files.
Chapter 6, "Using Protocol Forcing."	Describes the **Protocol forcing** function of the analyzer.
Chapter 7, "Generating Traffic	Describes the traffic generator for Ethernet and token ring networks.
Chapter 8, "The Sniffer—LM2000 Conversion Utility."	Describes how to convert saved data files between LM2000 and Sniffer Internetwork Analyzer format.
Chapter 9, "Using the Sniffer Analyzer Files."	Describes the network analyzer's directory structure and the types and formats of files it uses.
Appendix A, "Overview of Menu Options."	Provides a graphic representation of the complete menu system of the Sniffer analyzer.

Figure ii. Scope of each chapter or appendix in this manual.

Chapter/Appendix	Contents
Appendix B, "Troubleshooting."	Provides a list of solutions to common problems.

Figure ii. Scope of each chapter or appendix in this manual.

Audience of This Manual

The Analyzer Operations manual has been prepared with the following assumptions:

- You are a network manager or troubleshooter who understands your network's operation.
- You are familiar with DOS.
- You have properly started the Sniffer Network Analyzer.

Navigational Aids Used in This Manual

To help you find procedures easily, a separate list of procedures is provided in this manual in addition to the Table of Contents and List of Figures. Also, the "Recommendation" entries in the Index point you to suggestions for getting the most from your Sniffer Network Analyzer.

This manual uses icons in the margin to help you locate information as explained below:

IMPORTANT INFORMATION. Next to this icon is information that is especially important; you should be certain to read it carefully before you proceed. This icon also indicates useful and valuable ways of using the product.

CAUTION. Next to this icon is information that you must know to avoid damage to data files, program files, or hardware devices. This icon also indicates information that you must know to avoid possible injury to yourself or others.

PROCEDURE. Next to this icon is a series of steps you must follow to accomplish a particular task.

Conventions Used in This Manual

Special Notations

The following describes the conventions used in this manual:

Bold Menu options and menu names are in bold type. For example:

Move to **Display** and press Enter.

Move to the **Report\Print** menu.

UPPERCASE — The filenames and command names you type at a DOS prompt are in uppercase. For example:

Modify the AUTOEXEC.BAT file if necessary. To duplicate the file, use the COPY command.

Bold italics — Variables, for which you insert values, are in bold italics. For example:

Type the number of minutes and seconds in the ***mm:ss*** format.

`Screen font` — Screen messages are printed in monospaced font. For example:

```
You must stop monitoring before you can use this feature.
```

Terminology

Hexadecimal numbers mentioned in the manual are followed by "(hex)"; numbers without any notations are decimal. For example, "The maximum number of stations is 75. The default memory address is D8000 (hex)."

The term "application" refers to a software component (that is, the monitor or analysis program) running on the Sniffer Network Analyzer.

This manual sometimes uses abbreviated names for the various components of the Sniffer Network Analyzer. The term "analyzer" stands for the analysis application. The term "Expert analyzer" stands for the analyzer capturing or displaying in the Expert window.

Screen Displays

The screen displays in this manual may not exactly match what you see on your screen. There may be minor differences that do not affect the functions of the displays.

Other Sources of Information

Network General Corporation (NGC) provides other sources of information that can help you become familiar with the Sniffer Network Analyzer.

On-Line Help

After highlighting an item in the analyzer or monitor menu, a phrase or sentence in a panel near the bottom of the screen explains the meaning of the highlighted item.

If you want to obtain general information on a particular feature of the Sniffer Network Analyzer, press F1(**Help**) whenever its key label appears on the screen. A window containing a list of topics opens. Note that in the Expert window the key label for F1 reads **Explain**. Explain screens provide context-sensitive solutions to specific network problems highlighted in the Expert window. Help screens provide general description and instruction for the items in the analyzer's menus.

Technical Support

If you have problems with the Sniffer Network Analyzer, refer to the troubleshooting section of this manual for the procedure to contact Network General's technical support. The Troubleshooting Guide is in Appendix B.

Training

NGC offers a comprehensive set of training courses focused on hands-on network analysis and troubleshooting using the Sniffer Network Analyzer. For more information, contact your sales representative.

CHAPTER ONE: SNIFFER NETWORK ANALYZER OVERVIEW 1

Sniffer Network Analyzer Overview

Overview

This chapter summarizes the major new and enhanced features of Network General's Sniffer analyzer, describes how the system works, and lists the major benefits of the product. This chapter does not cover the procedures for invoking various Sniffer functions or explain in detail the various menu items. That information is provided in later chapters.

Scope of this Manual

This manual describes the operation of the Sniffer analyzer in Classic mode. For information on operating the Sniffer analyzer in Expert mode, see the *Expert Sniffer Network Analyzer Operations* manual.

Major Components of the Sniffer Network Analyzer

The Sniffer analyzer is a software component of the Sniffer Network Analyzer. Figure 1–1 summarizes the major software components of the Sniffer Network Analyzer.

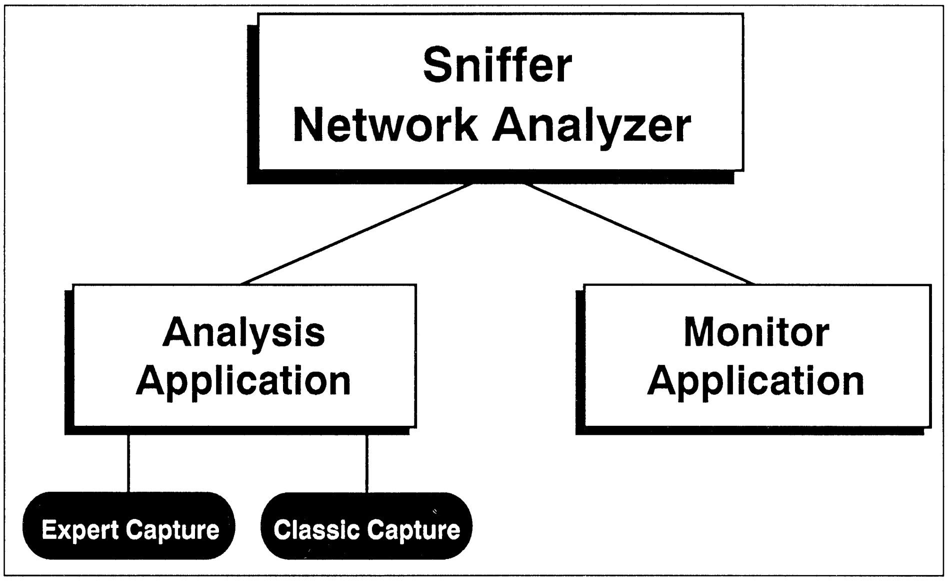


Figure 1–1. Major software components of the Sniffer Network Analyzer.

Depending on the network topologies installed in your Sniffer Network Analyzer, you can capture in either Expert or Classic mode. Expert functionality is available on the following topologies:

- Ethernet
- Token ring

- WAN/Synchronous (the Expert Sniffer Internetwork Analyzer)

When this manual mentions the "Expert Sniffer analyzer," it is referring to the Sniffer analyzer capturing or displaying in Expert mode. Similarly, the term, "Classic Sniffer analyzer," refers to the Sniffer analyzer capturing or displaying in Classic mode.

This manual describes the operations of the Sniffer Network Analyzer in Classic mode. The manual also includes general information, such as description of the file and directory structure of the Sniffer Network Analyzer. This manual does not desribe the operation of the analyzer in Expert mode. For information on operating the Sniffer Network Analyzer in Expert mode, see the companion publication *Expert Sniffer Network Analyzer Operations.*

Conceptual Overview of Sniffer Network Analyzer Functions

An analyzer —that is, the network analyzer program installed in the Sniffer Network Analyzer— records and interprets network transmissions. The work of the analyzer occurs in two main stages:

Capture The analyzer records network traffic for later interpretation. Capture can be filtered to record only traffic that meets certain criteria. Network data can be saved to disk when a user-definable trigger event occurs. This assures that the frames of interest are saved without requiring that capture be stopped. Alternatively, triggers can be specified so that capture stops when the trigger event is detected.

During capture in Expert mode, frames are analyzed as they are stored in the buffer. The various Expert displays are dynamically updated as capture proceeds, allowing you to navigate between various levels of detail to solve network problems in real time.

While capturing frames, the analyzer software maintains and displays graphs or tables that summarize recorded traffic.[1]

Display The analyzer interprets the recorded traffic. In the Classic window, the analyzer decodes the various layers of protocol in the recorded frames and displays them as English abbreviations or summaries. The analyzer can filter the display to show only those frames that meet certain criteria.

You can also display the captured frames in the Expert window. In the Expert window, you can investigate the symptoms and diagnoses the Expert analyzer detected. In the Expert window, all the views available during capture are also available during display. You can toggle display between the Classic and Expert windows by pressing the function key F3.

[1] The analyzer's displays during capture resemble some of the displays produced by the monitor. Don't confuse this mini-monitoring during capture with the full-blown monitor application, which is separate.

The Analyzer as (Mostly) Passive Observer

The Sniffer analyzer "hears" all traffic that passes over the segment it is observing. On a WAN/Synchronous link, it hears traffic in both directions ("from DTE" and "from DCE"). On a LAN, it hears all traffic that passes over the segment or subnet that it is monitoring. It is characteristic of a LAN that every station physically receives every transmission. Ordinarily, each station ignores all messages except broadcast messages and those addressed to it. The Sniffer analyzer not only hears all transmissions, but, while in "capture" mode, it can record them, regardless of how they're addressed.

In general, the Sniffer analyzer observes, tabulates, analyzes, or captures, but contributes no traffic to the network it is observing. However, when the analyzer is observing a LAN, it may contribute to the LAN's traffic as follows:

- On Ethernet, token ring, FDDI, PCnet, ARCnet, and StarLAN, an analyzer can generate test frames. In this mode, it repeatedly transmits the single test packet you specify.
- On Ethernet, the analyzer can emit a pulse to test for cable defects.
- On token ring, every station must participate in the ring by forwarding traffic from its upstream neighbor to its downstream neighbor. The Sniffer analyzer does that in the same way as other stations. However, the analyzer does not reply to the poll for standby monitors, and never acts as the ring's active monitor. It is thus invisible to most other stations.

  Note: During traffic generation, however, the token ring analyzer may act as the active monitor if no other station is transmitting.
- On token ring, the analyzer periodically transmits a frame addressed to "LAN Manager" announcing "trace tool present." The LAN Manager can force such a station to leave the ring immediately.
- On FDDI, the analyzer participates in the ring when it is set to SMT Active mode and forwards traffic from its upstream neighbor to its downstream neighbor. When set to SMT Passive mode, the analyzer forwards traffic but will not appear in an SMT ring map. When set up as a beam splitter, the analyzer is completely passive and doesn't affect the ring in any way.

A Map of the Analyzer's Functions

The analyzer's activities are divided into the set of functions described below. The diagram in Figure 1–2 represents schematically the route by which information flows between the various functions. Following the path of the frames as they are captured, they are affected by the analyzer's principal functions as follows:

- Capture filters determine which frames are discarded and which are captured.
- Capture views show the capture's progress, in one of two tabular formats or in the skyline format.

- Trigger detector scans arriving frames for a user-defined pattern or event. When it detects this pattern or event, it stops capture so that frames preceding or following the event are retained. Alternatively, you can configure **Disk Snapshot** so that the frames preceding or following the trigger event are saved to disk. This way, capture need not be stopped.
- Capture buffer is the storage area for frames that have been accepted. From here they are subsequently interpreted and displayed.
- Object database is the storage area for Expert information, such as network objects, symptoms, and diagnoses.
- Protocol interpreters identify the protocols nested within each frame and interpret their contents.
- Display filters determine which frames in the capture buffer are displayed.
- Frames that pass the display filters are displayed in three views:

  — Summary

  — Detail

  — Hex with ASCII or EBCDIC

Output of the display can be saved to a file, sent to a printer, or imported into spreadsheets.

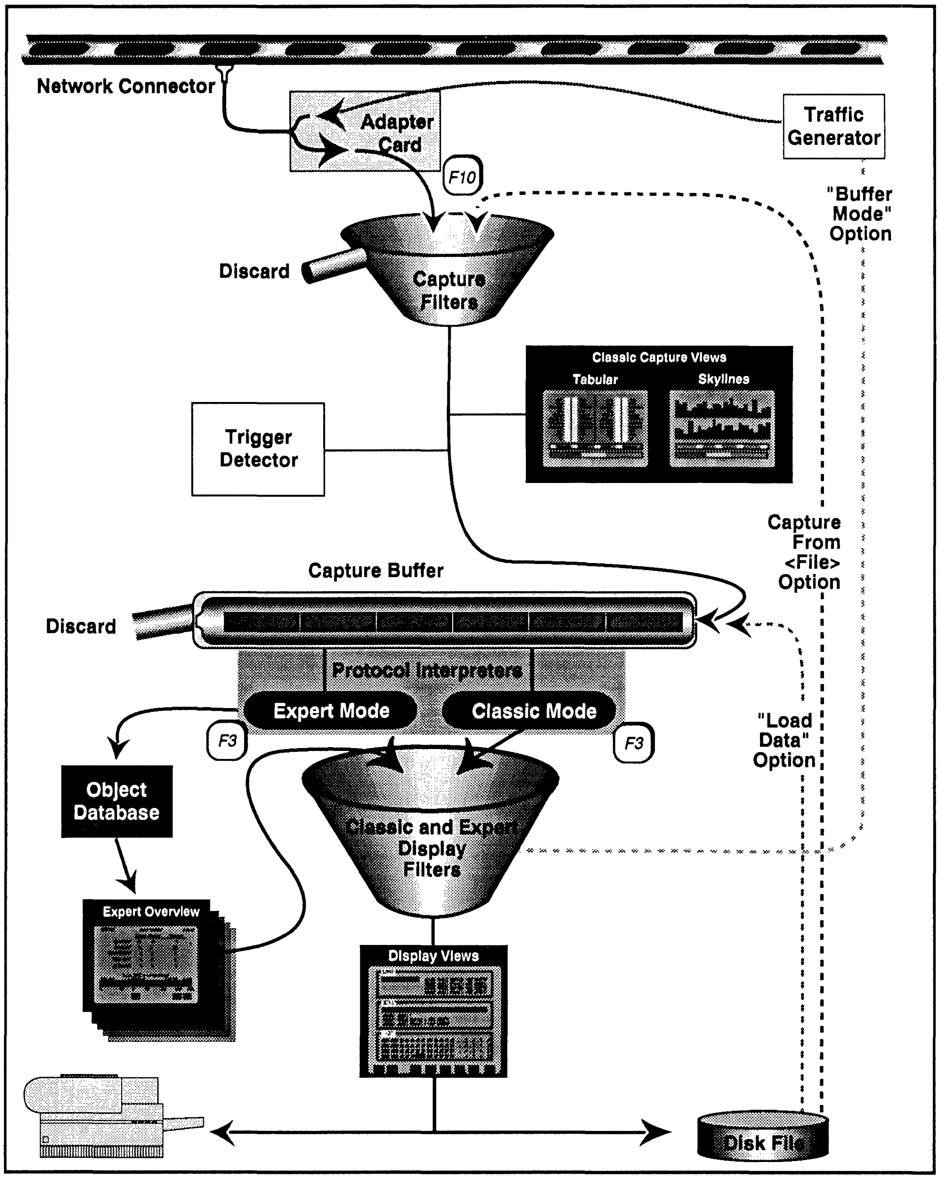


Figure 1–2. Overview of Sniffer analyzer functions.

Features of the Sniffer Network Analyzer

The Sniffer analyzer can generate traffic on various networks, filter frames when capturing, and display frames in a variety of formats. Figure 1–3 lists some of the features of the Sniffer analyzer.

Proprietary HDLC decodes	The new high-speed Internetwork Analyzer supports traffic rates up to T1/E1, and can decode proprietary versions of HDLC from a variety of router/bridge vendors.
Frame editing	This feature lets you edit a frame to change its size, content, or timing. If you have an Ethernet-II adapter card, you can also create bad CRC frames. By using this feature with the Traffic generator, you can specify the contents of generated frames.
Traffic generator buffer mode	On Ethernet, token ring, and FDDI networks, this option lets you transmit the contents of the capture buffer during traffic generation. By using this feature together with the Frame editing feature, you can build and send complex buffers.
Protocol forcing	This feature is an advanced tool for decoding encapsulated protocols, primarily seen on bridges and routers.
Global toggle for filters and triggers	This feature allows you to temporarily disable any capture filters, display filters, or triggers you defined. This allows you to disable filters or triggers as a group, without having to disable them individually.
Capture and display filters	The filter for Known stations is useful for detecting intruders. The Selected frames filter checks for frames that you flag. If you have an Ethernet-II adapter card, you can also filter for Collision frames.
Disk snapshot	This feature automatically saves to disk the portion of the capture buffer that contains the frames that interest you.
ASCII parity option	This feature lets you strip the 8th bit from each byte.
Dynamic mode option	This option automatically adjusts interpretation to ASCII or EBCDIC, depending on the types of frames received. This option is now available for all topologies.
Flags	An automatic flag for edited frames is provided. You can also manually apply the Selected frame flag to identify (and then filter and save, if desired) any frames you choose. If you have an Ethernet-II adapter card, an automatic flag for Collision frames is available.
Parameter reset	This option reverts all user-defined settings back to the factory defaults, shown in Appendix A. When you use this option, you can always start from a known state.

Figure 1–3. Features of the Sniffer analyzer.

Figure 1–4 outlines some of the new features provided by the Expert analyzer:

Documentation of Expert analyzer features is found in the *Expert Sniffer Network Analyzer Operations* manual.

Analysis during capture	The Expert analyzer can analyze network traffic and generate diagnostic messages while capturing frames from the network or a file. It can also capture traffic in Classic or Highspeed mode and then perform Expert analysis on the frames in the capture buffer later. (Highspeed mode for Ethernet and PC-Net only.)
Explain screens	In the Expert window, you can pause capture and press F1 to show a detailed context-sensitive Explain screen pertaining to a symptom, diagnosis, or network object that is highlighted.
Multiple-layer analysis	The Expert analyzer can analyze problems at the Application, Connection, Network Station, and DLC Station layers. On a token ring network, it can also analyze problems at the Medium Access Control (MAC) layer. You can specify that the analyzer perform Expert analysis on only those layers that interest you.
Expert triggers	You can specify one or more network events as trigger events. For example, you can configure the analyzer to stop capturing (or, to save the capture buffer to disk) immediately after detecting a duplicate network address.
Network object filters	After capture, you can automatically filter out frames that are irrelevant to a particular symptom, diagnosis, or network object. After filtering, the analyzer displays only those frames related to the selected object, making it easy for you to concentrate on one problem at a time.
Display with symptoms	You can elect that the Classic data display window show a one-line description of any symptom associated with a frame.
Filter on symptoms	You can elect to display only those frames exhibiting symptoms.

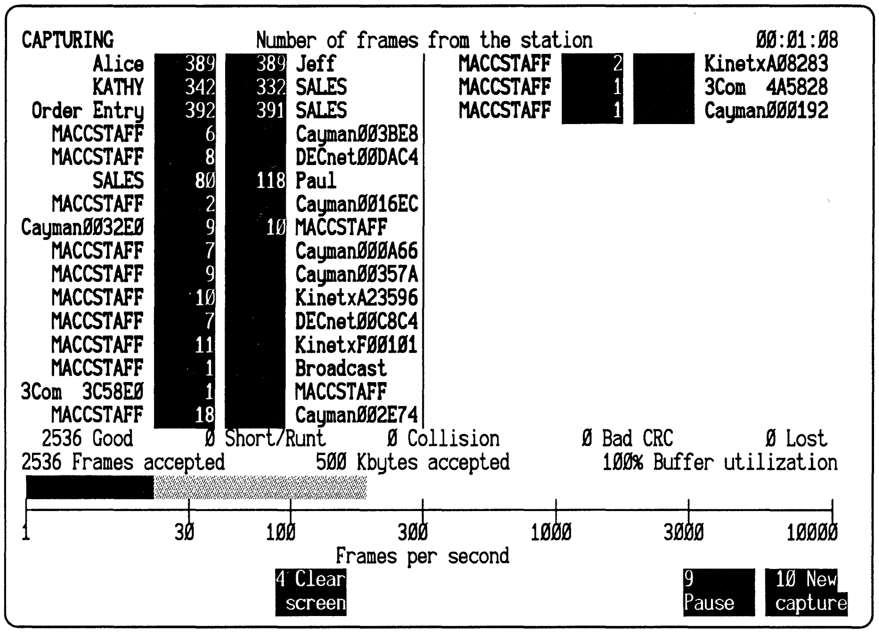
Figure 1–4. New features of the Expert Sniffer analyzer.

Overview of the User Interface

You interact with the Sniffer analyzer through its menus and function keys. In some cases, a menu item and a function key have the same function. For example, you can either choose Capture from the main menu or press F10 (**New capture**) to start the capture process.

Using the Function Keys

In most cases, however, function keys are specific to whatever is displayed. During capture, for example, only those function keys that you might need are displayed. In Figure 1–5, F4 (**Clear screen**) clears the screen (although the capture buffer is not affected), F9 (**Pause**) pauses capture and displays additional function keys for additional options, and F10 (**New capture**) starts the capture. The function keys relevant to various procedures are discussed with those procedures.



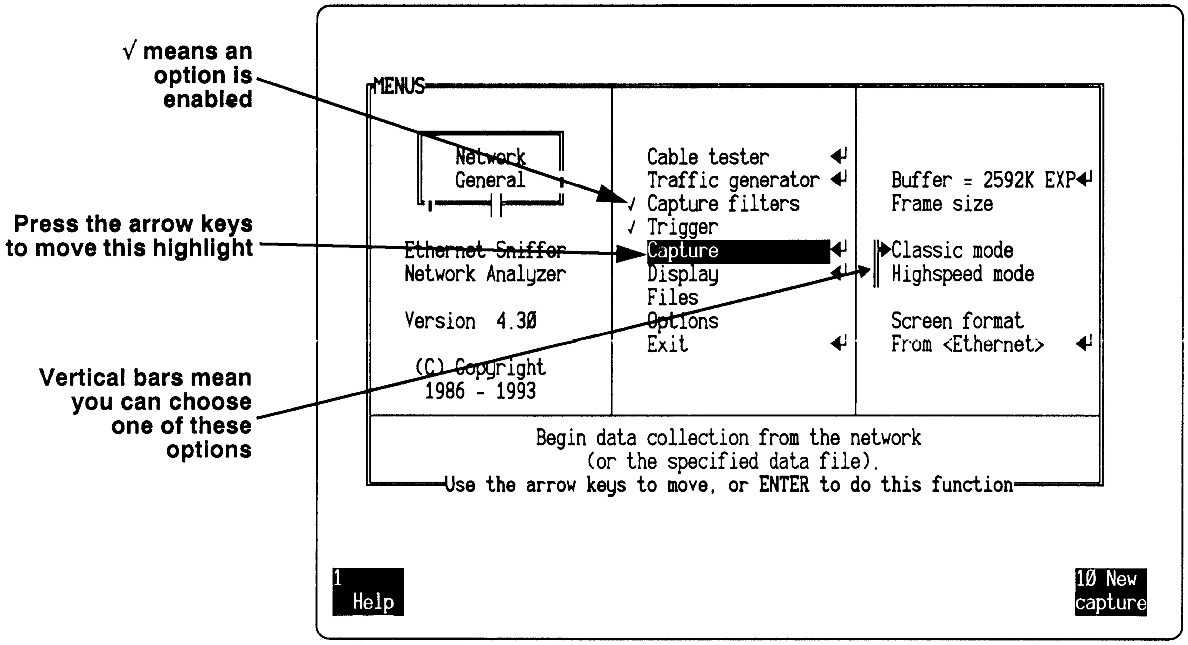
```
CAPTURING                Number of frames from the station                00:01:08
        Alice   389   389 Jeff        |   MACCSTAFF      2        KinetxA08283
        KATHY   342   332 SALES       |   MACCSTAFF      1        3Com  4A5828
  Order Entry   392   391 SALES       |   MACCSTAFF      1        Cayman000192
    MACCSTAFF     6       Cayman003BE8|
    MACCSTAFF     8       DECnet00DAC4|
        SALES    80   118 Paul        |
    MACCSTAFF     2       Cayman0016EC|
 Cayman0032E0     9    10 MACCSTAFF   |
    MACCSTAFF     7       Cayman000A66|
    MACCSTAFF     9       Cayman00357A|
    MACCSTAFF    10       KinetxA23596|
    MACCSTAFF     7       DECnet00C8C4|
    MACCSTAFF    11       KinetxF00101|
    MACCSTAFF     1       Broadcast   |
 3Com  3C58E0     1       MACCSTAFF   |
    MACCSTAFF    18       Cayman002E74|
  2536 Good         0 Short/Runt     0 Collision       0 Bad CRC        0 Lost
 2536 Frames accepted       500 Kbytes accepted        100% Buffer utilization

1             30      100        300       1000       3000        10000
                           Frames per second
                    4 Clear                                    9       10 New
                     screen                                   Pause    capture
```

Figure 1–5. Function keys available during capture.

Using the Sniffer Analyzer Menus

When you first start the Sniffer analyzer, the main menu appears (see page 2–3). Depending on your network, the options in this menu may vary slightly. However, the process of working with the menus is the same for all networks and platforms.

Figure 1–6 shows the options associated with the main menu, through which you can access all other functions. For an overview of *all* menu items and associated options, see Appendix A.



√ means an option is enabled

Press the arrow keys to move this highlight

Vertical bars mean you can choose one of these options

```
MENUS
  Network              Cable tester      ↵
  General              Traffic generator ↵   Buffer = 2592K EXP↵
                     √ Capture filters       Frame size
                     √ Trigger
 Ethernet Sniffer      Capture           ↵  ▶Classic mode
 Network Analyzer      Display           ↵  ▶Highspeed mode
                       Files
 Version  4.30         Options               Screen format
                       Exit              ↵   From <Ethernet>   ↵
   (C) Copyright
   1986 - 1993

             Begin data collection from the network
                  (or the specified data file).
     Use the arrow keys to move, or ENTER to do this function

1                                                        10 New
  Help                                                   capture
```

Figure 1–6. The Sniffer analyzer main menu.

To work with the Sniffer analyzer menus:

1. Press one of the four arrow keys to move the highlight to the desired menu item. Note that any options associated with that item appear in the panel to the item's right. As you move the highlight, the relevant options are displayed, while those associated with another option disappear.
2. For options followed by a ↵ symbol, pressing Enter when the option is highlighted either executes the command or it displays a listing or dialog box. From this display, you can either choose an option or enter information. In Figure 1–6, for example, pressing Enter when the **From <Ethernet>** option is highlighted results in a listing of files from which you can choose one as the capture source.
3. For options connected by a vertical bar (radio control), you can choose an option by moving the highlight to that option and pressing Spacebar. All other options connected by the bar are automatically disabled. In the main menu, for example, you can choose between capturing in **Classic mode** or in **Highspeed mode** (not applicable for the FDDI Sniffer Network Analyzer).
4. For options preceded by √ or x symbols, you can enable or disable those options by moving the highlight to them and pressing Spacebar. Any such options are always either enabled (√) or disabled (x); pressing Spacebar toggles between the two states.

CHAPTER TWO: DEFINING SYSTEM OPTIONS 2

Defining System Options

Overview

To work with system options, you should have successfully started your Sniffer analyzer and attached it to the network. If you have not done so, refer to the *Sniffer Network Analyzer: Model xx Installation Guide* for information on installation and initial setup of the Sniffer analyzer.

This chapter explains how to configure the system options found in the Options menu of the Sniffer analyzer. System options include general network characteristics or general preferences related to how the Sniffer analyzer works. Some options apply to all networks while others apply only to specific architectures, such as token ring, or to specific platforms, such as the IBM Model 70.

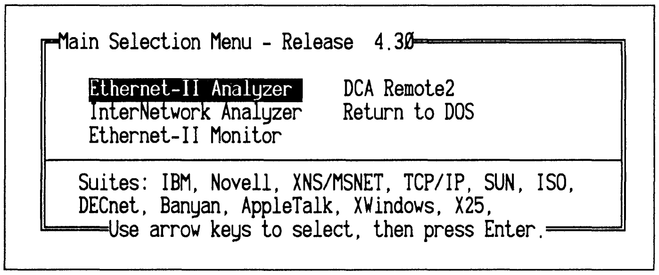
System options for all networks include:

- Audible clicks
- Use defaults
- Interpret RI bit
- Language

This chapter also explains the special options available for Ethernet, for token ring, for the IBM PS/2 Model P/70, for the Sniffer Internetwork Analyzer (the Sniffer analyzer for WAN/Synchronous), and for fiber distributed data interface (FDDI) networks.

Starting the Analyzer Application

When you first start the Sniffer analyzer, the Main Selection Menu appears. Figure 2–1 shows the Main Selection Menu for a Sniffer analyzer with an Ethernet II adapter card.



```
Main Selection Menu - Release 4.30

   Ethernet-II Analyzer    DCA Remote2
   InterNetwork Analyzer   Return to DOS
   Ethernet-II Monitor

  Suites: IBM, Novell, XNS/MSNET, TCP/IP, SUN, ISO,
  DECnet, Banyan, AppleTalk, XWindows, X25,
       Use arrow keys to select, then press Enter.
```

Figure 2–1. The Sniffer Network Analyzer Main Selection Menu.

This menu shows the release version, the protocol suites available for your network, and the various Sniffer analyzer functions, which include:

- Ethernet (or other network) Analyzer: this program captures and analyzes frames. This manual discusses all the features associated with the Sniffer analyzer program.

  Note: "Internetwork Analyzer" refers to the Sniffer analyzer for WAN/Synchronous networks.

- Ethernet (or other network) Monitor: this program monitors traffic and provides an accurate picture of network activity at any moment. For instructions, refer to the *Advanced Network Monitor User's Manual* for your network.

- DCA Remote2: this program allows you to run the Sniffer analyzer remotely, from another computer via modem. The analyzer's serial port transmits the analyzer's screen to the remote controller and it receives keystrokes from the controller. For complete information, refer to the *DCA Remote2 Supplement,* shipped with your system.

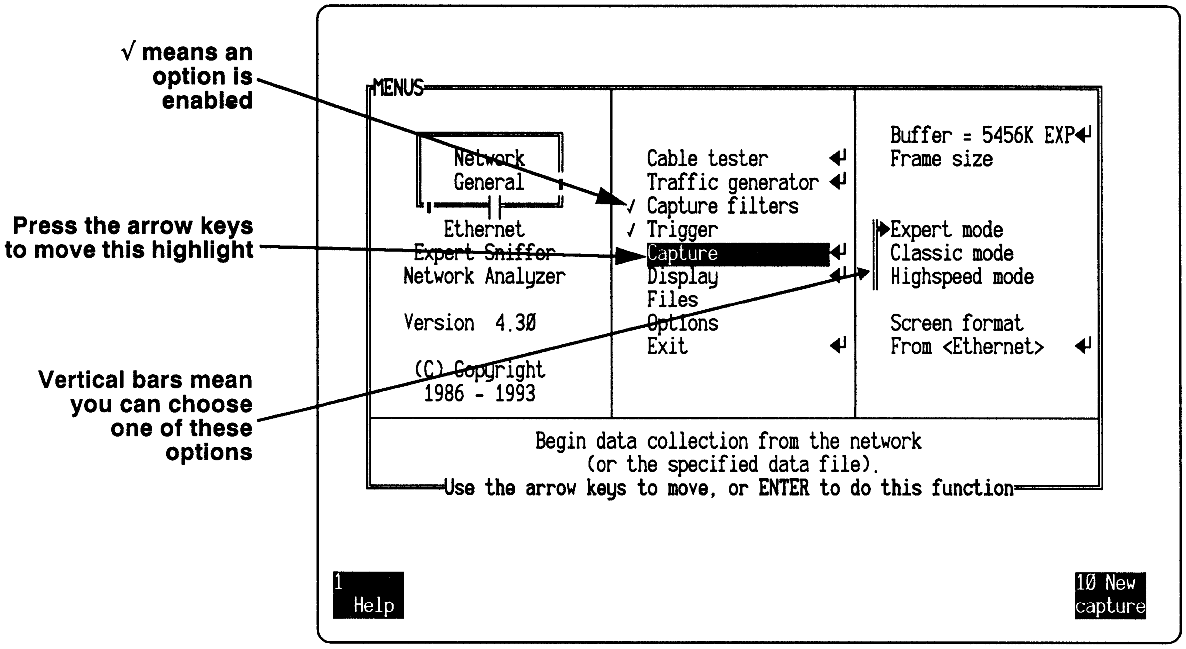
  Note: To use this feature, you should start the Remote2 application (that is, make it memory-resident) before starting either the Sniffer analyzer or the Sniffer monitor.

- Return to DOS: this function terminates the application and displays the DOS **C:** prompt.

To start the Sniffer analyzer:

1. Move to *xx* **Analyzer** and press Enter.

   In response, an initialization screen appears, followed by the main menu (Figure 2–2), which may vary slightly depending on the options available for your network. From this menu, you can reach any of the Sniffer analyzer's functions.



√ means an option is enabled

Press the arrow keys to move this highlight

Vertical bars mean you can choose one of these options

```
MENUS
  Network           Cable tester       ↵   Buffer = 5456K EXP↵
  General           Traffic generator  ↵   Frame size
                  √ Capture filters
  Ethernet        √ Trigger                ▶Expert mode
  Expert Sniffer    Capture            ↵    Classic mode
  Network Analyzer  Display            ↵    Highspeed mode
                    Files
  Version  4.30     Options                 Screen format
                    Exit               ↵    From <Ethernet>  ↵
  (C) Copyright
  1986 - 1993
              Begin data collection from the network
                   (or the specified data file).
      Use the arrow keys to move, or ENTER to do this function
1                                                      10 New
 Help                                                  capture
```

Figure 2–2. The Sniffer analyzer main menu.

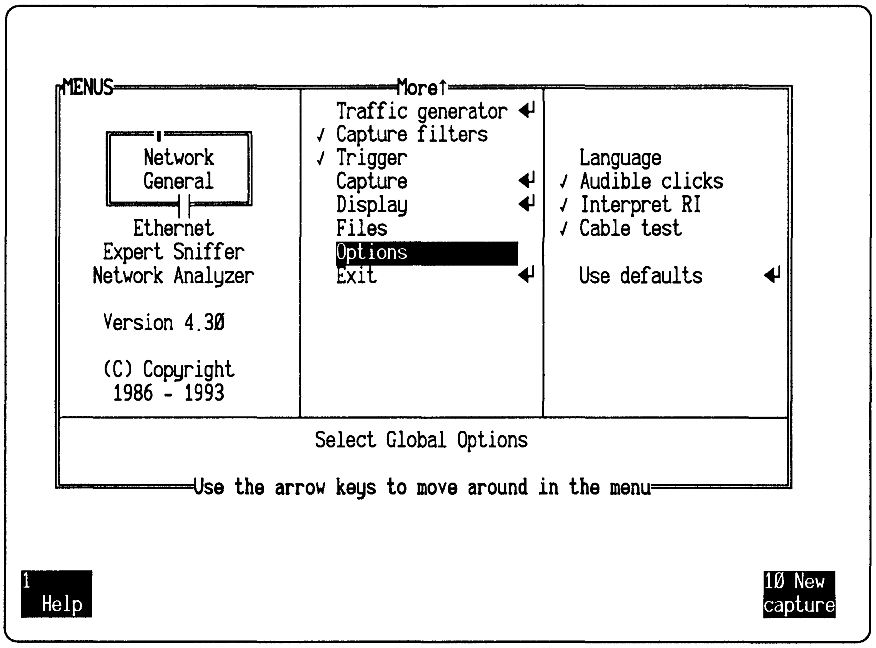
Options Menu Overview

The Options menu is located near the bottom of the main menu's first panel. Figure 2–3 provides an overview of the menu items associated with the Options menu for Ethernet networks.

Note: For the IBM PS/2 Model P/70, the menu includes an additional option for choosing either the external or internal transceiver. The Options menus for token ring, WAN/Synchronous, and FDDI networks are shown later in this chapter.

This chapter provides an overview of the basic menu items associated with the Options menu. Many of these items, in turn, are associated with additional options. As with all other Sniffer analyzer menu options, you first press the Cursor keys to move the highlight to the desired option. You can then define that option.

- For options marked with the √ and x symbols, you can press Spacebar to enable (√) or disable (x) the option. To reverse all settings, press Alt-Spacebar.
- For options connected with a vertical bar (radio control), you can choose one of those options by moving to it and pressing Spacebar.
- For options where you must define a specific value, you can choose that value from a list or enter the desired value into a dialog box.



```
MENUS                        More↑
                        Traffic generator ↵
   Network            √ Capture filters
   General            √ Trigger                 Language
                        Capture         ↵     √ Audible clicks
                        Display         ↵     √ Interpret RI
   Ethernet             Files                 √ Cable test
 Expert Sniffer         Options
Network Analyzer        Exit            ↵       Use defaults      ↵

 Version 4.30

 (C) Copyright
  1986 - 1993

                     Select Global Options

         Use the arrow keys to move around in the menu

1                                                            10 New
 Help                                                        capture
```

Figure 2–3. The Options menu: Ethernet Sniffer analyzer.

Setting the Language Option

Depending on the configuration you ordered, you may be able to change the language in which the analyzer presents the help and Explain files. Currently available languages include:

- English
- German
- French
- Italian

To set the Language option:

1. Move to **Options\Language**.
2. Highlight the desired language and press Spacebar. The analyzer will now display all help and Explain files in this language.

Setting the Audible Clicks Option

The **Audible clicks** option determines whether the Sniffer analyzer "clicks" each time it accepts a frame into the capture buffer. The clicks provide an impression of the general level of traffic, which makes it easy to detect sudden lulls or bursts in traffic without looking at the screen.

With the **Audible clicks** option enabled, the analyzer also clicks each time it transmits a frame during traffic generation.

The default is ✓**Audible clicks** enabled.

To set or clear the Audible clicks option:

1. Move to **Options\Audible clicks.**
2. Press Spacebar to enable (✓) or disable (x) the option.

About the Interpret RI Option

On LAN networks that use six-byte addressing (including token ring and Ethernet), this option determines how the Sniffer analyzer treats data link connection (DLC) addresses.

Some networks reserve one bit—the RI bit— in the source address to indicate that the frame includes a field called the *"source routing information"* (RI) field. On networks that recognize the RI bit, an address really consists of only 47 bits. The 48th bit is used in the destination address to indicate "broadcast" or "multicast" and in the source address to indicate "RI present." The broadcast/multicast bit is the bit that is physically transmitted first.[1]

RI Fields and "Data Relative" vs. "Frame Relative" Options

IBM introduced source routing on token ring networks, which remains the context in which it is most frequently found. In principle, source routing information can be used not just on token ring but on any LAN that uses six-byte station addresses, including Ethernet, FDDI, StarLAN, and PC Network.

The RI field is a variable-length field inserted after the DLC destination and source fields and before the frame's data field. As a result, the data field is increased by the total length of the RI field. To allow for the varying size of the RI field, you can describe a pattern by either its frame relative or its data relative offset. For more information, refer to "Defining a Pattern Match Filter" on page 3–45.

The RI field contains an identifier for each of the bridges that forwarded the frame. As it retransmits a frame, each bridge appends its own two-byte identifier[1] to the RI field. As a result, the ultimate recipient has a record of all intermediate stations that forwarded the frame.

To request that each intermediary insert its identifier, the originating station turns on the RI bit. In response, each receiving station interprets the first two data bytes as the RI header, perhaps followed by a list of route designator fields.

The originating station sets up the RI header. Five bits in the RI header record the total length of the RI field (including the header). Initially, before the frame is forwarded, the RI field's total length is two bytes. As each bridge forwards the frame it appends its own two-byte identifier, increasing the RI length by two.

Effects of Enabling "Interpret RI"

The default is **Interpret RI** enabled, which means:

- The Sniffer analyzer treats DLC addresses as 47 bits.
- The analyzer calls the RI interpreter to interpret the RI field of frames that contain this bit in the source address.

A few networks treat all 48 bits as part of the address. On such a network, the 48th bit is simply part of the address—it does not mean that there is an RI field. When analyzing frames from such a network, it is important to disable the **Interpret RI** option. Otherwise, the Sniffer analyzer may try to interpret part of the frame's data field as an RI field.

[1] This situation occurs because rules for converting bits-on-the-wire to bits-in-memory differ between networks. The broadcast bit is the high-order bit of a token ring address, but in an Ethernet, StarLAN, or PC Network address, it is the low-order bit of the first byte.

[1] The identifier is composed of a 12-bit ring number and a 4-bit bridge number. These are arbitrary numbers assigned by the network administrators. The RI identifier is unrelated to the bridge's station address.

Effects of Disabling "Interpret RI"

If this option is disabled:

- The Sniffer analyzer treats addresses as 48 bits.
- The analyzer does *not* call the RI interpreter and assumes that there is *never* an RI field.
- The **Destination class** filter continues to recognize the broadcast bit in a destination address. As a result, the filter treats a station whose address includes a one in that position as if it were a broadcast or multicast address.

Setting the Interpret RI Option

The default is √**Interpret RI** enabled.

To determine whether to treat the high-order bit of the source address as part of the address or an RI indicator:

1. Move to **Options\Interpret RI**.
2. Press Spacebar to enable (√) or disable (x) the option.

Resetting all Options

The **Use defaults** option restores the Sniffer analyzer's default factory settings to all options, including the capture and display filters, triggers, and other options. These settings are stored in the file DEFAULTS.*xx*S, where *xx* is the network abbreviation (such as EN, TR, or FD). For an overview of the factory default settings of all options, refer to the overview of menu items in Appendix A.

Note: *Do not* alter the settings in this file—it allows you to always start from a known state. If you want to apply the settings you define at system startup, you can save them to the STARTUP.*xx*S file in the C:\CAPTURE directory.

To restore the default configuration:

1. Move to **Options\Use defaults** and press Enter.

Caution: This option clears any settings you may have defined. If you want to use those settings later, save the current settings as a Setup file. For details, refer to "Using Setup Files to Define System Options" on page 5–14.

Setting the Cable Test Option for Ethernet

When you first start capture on an Ethernet Sniffer analyzer, the analyzer checks to see if it is connected to an Ethernet cable by performing a time-domain reflectometer (TDR) test. The TDR test actually transmits a packet on the cable to verify that it exists. In some isolated cases, this packet may disturb other network activities. You can use the **Cable test** option to disable the initial TDR test.

To determine whether the Ethernet analyzer should perform a TDR cable test upon the start of capture:

1. Move to Options\Cable test.
2. Press Spacebar to enable (✓) or disable (x) the option.

Setting the Transceiver Option for the IBM PS/2 Model P/70

On an Ethernet Sniffer analyzer, IBM's Microchannel technology makes it possible to use software to change between BNC and AUI ports, without having to remove the adapter card and change a jumper block.

If you run the Sniffer analyzer with an Ethernet-II adapter card on the Model 70, you can choose whether to use the external transceiver attached to the DB-15 connector, or the internal transceiver that uses the thin Ethernet BNC connector. Therefore, if you use the AUI ports, choose the External transceiver option; if you use the BNC port, choose the Internal transceiver option. If you want to switch between the two options, connect to the appropriate port.

Do not physically connect to both ports simultaneously and then try to switch between ports by using this option. If you do so, you risk crosstalk between the segments attached to each port, or even network failure.

The default is **External transceiver** selected.

To choose between ports on the Model 70:

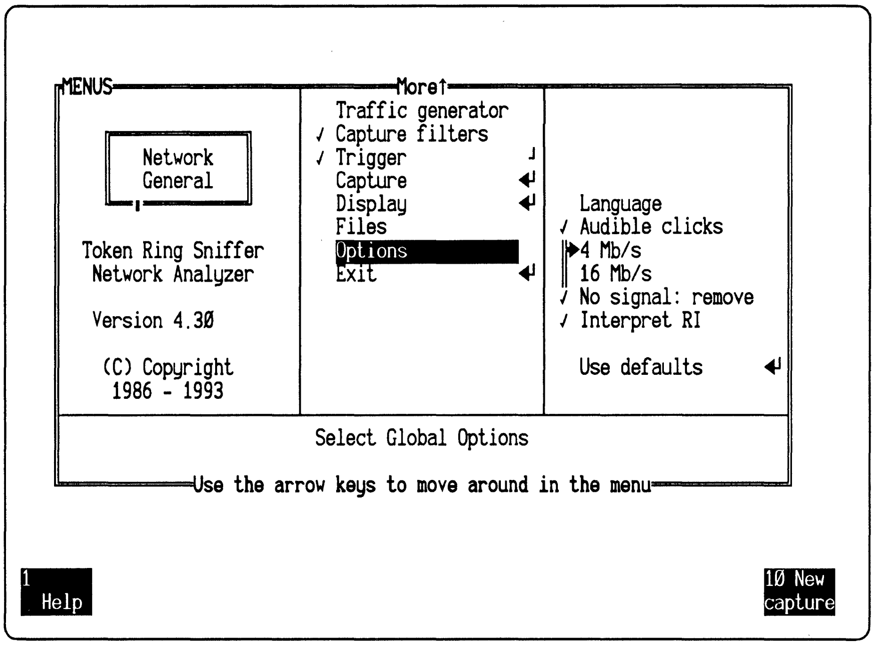
1. Move to **Options** and then to the desired transceiver and press Spacebar.

   ▸External transceiver
   Internal transceiver

Setting the Token Ring Options

On a token ring Sniffer analyzer, the **Audible clicks**, **Interpret RI**, and **Use defaults** options operate as they do on an Ethernet network, as described in the previous section. Token ring networks include two additional system options: the network speed and the option to remove from the ring if there is no signal.

Figure 2–4 shows the system options associated with a token ring analyzer.



```
MENUS                        More↑
                     Traffic generator
  Network          ✓ Capture filters
  General          ✓ Trigger            ┘
                     Capture            ↵
                     Display            ↵    Language
                     Files                 ✓ Audible clicks
Token Ring Sniffer   Options                ▶4 Mb/s
Network Analyzer     Exit               ↵    16 Mb/s
                                           ✓ No signal: remove
Version 4.30                               ✓ Interpret RI

(C) Copyright                                Use defaults       ↵
1986 - 1993

                      Select Global Options
             Use the arrow keys to move around in the menu

1                                                          10 New
 Help                                                      capture
```

Figure 2–4. The Options menu: token ring Sniffer analyzer.

Setting the Token Ring Speed

The token ring adapter card is capable of capturing from networks running at speeds of either 4 or 16 Mbits/s. If the wrong speed is selected, the ring will be disrupted, although you can minimize the disruption by enabling the **No signal: remove** option, as described in the next section.

If you move the Sniffer analyzer to another network, you can use the speed options to select the appropriate speed.

To set the network speed used by the analyzer's adapter card:

1. Move to **Options** and then to the desired speed and press Spacebar.

   ▶4 Mb/s
   16 Mb/s

Note: You can choose from the menu the speed at which you want to capture. On the Model 70, you can also select the speed for traffic generation from the menu. For other Sniffer analyzer platforms, however, you must set a switch on the token ring adapter card for the correct transmission speed.

Setting the Token Ring Remove Option

With a token ring network, you can determine how the Sniffer analyzer responds if it receives no signal when it inserts itself into the ring. There are two choices: it can remove itself from the ring immediately or remain in the ring.

Removing the analyzer minimizes disruption if you inadvertently connect an analyzer configured for one transmission speed to a ring that operates at a different speed.

However, operating without automatic removal has two advantages:

- When the ring is broken, you can connect to a portion of the ring and await signals as you make other changes to the ring.
- On a functioning ring, you can disconnect temporarily and reconnect without having to reset the Sniffer analyzer adapter card.

If you are certain that the Sniffer analyzer's speed matches the speed of the network, you can remove this protection.

The default is ✓ **No signal: remove** enabled.

To change the token ring No signal:remove protection option:

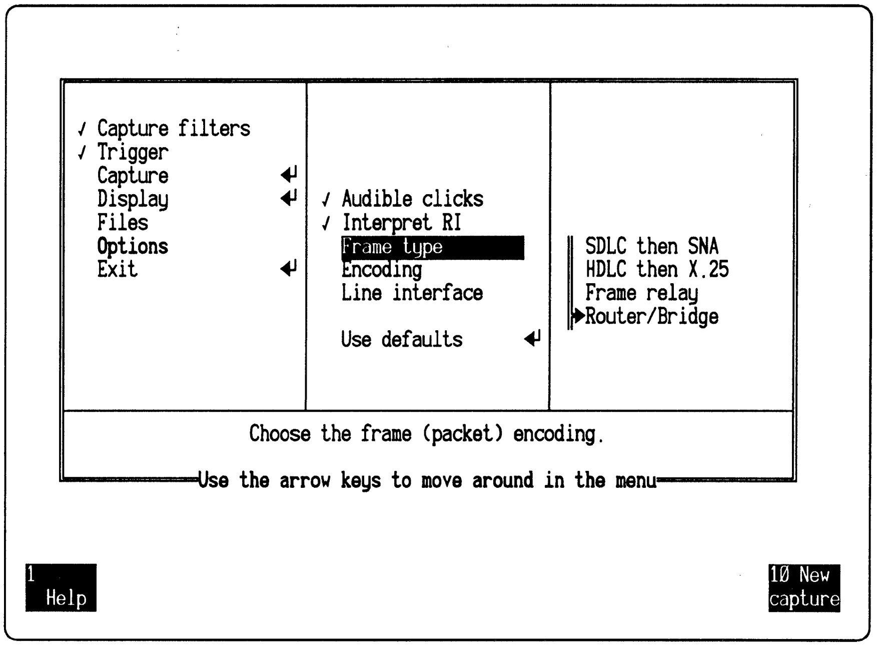
1. Move to **Options\No signal: remove.**
2. Press the Spacebar to enable (✓) or disable (X) the protection.

Setting the Sniffer Internetwork Analyzer Options

On a Sniffer Internetwork (WAN/Synchronous) analyzer, the **Audible clicks, Interpret RI**, and **Use defaults** options operate as they do on an Ethernet network, described in the previous sections. The Sniffer Internetwork Analyzer includes several additional system options:

- Frame type options
- Encoding method options
- Physical line interface options.

Figure 2–5 shows the system options associated with the Sniffer Internetwork Analyzer. Each is described in the sections below.



Choose the frame (packet) encoding.

Use the arrow keys to move around in the menu

Figure 2–5. The Options menu: Sniffer Internetwork (WAN/Synchronous) analyzer.

Frame Type Options

If you have a WAN/Synchronous network, you will need to define the lower-level protocols used by the synchronous link. This includes defining the frame type and the encoding method used to transmit the frame across the WAN.

The **Frame type** options let you define the access protocols, including Frame relay, Router/Bridge, SDLC/SNA (IBM's Synchronous Data Link Control protocol), and HDLC/X.25 (High-level Data Link Control). None of these protocols affect which of the higher-level protocols are embedded within their frames.

Of these protocols, the most widely used are SNA (System Network Architecture) over SDLC at IBM installations, and X.25 over HDLC, which is widespread in Europe and is used increasingly in the United States. The Frame relay frame type is widely used for LAN interconnectivity, as are proprietary versions of HDLC (decoded by the **Router/Bridge** option). For examples of how these options determine what is displayed during capture, see "Frame Counts Display During Capture: WAN/Synchronous" on page 3–20.

The default frame type is **Router/Bridge**. The **Router/Bridge** option lets the analyzer decode proprietary versions of HDLC during capture. Many leased-line internetworks use proprietary versions of HDLC. The Sniffer Internetwork Analyzer can recognize and interpret data within many versions of HDLC. These include the Point-to-Point (PPP) standard router/bridge frame format and also a variety of others, including proprietary versions of HDLC from the following router/bridges:

- Wellfleet (Versions 3.1, 3.3, and 3.7)
- Cisco
- Vitalink
- Proteon
- IBM source routing bridges (Versions 2.2 and 2.3, token ring only)
- Microcom

  Note: for Microcom bridges, **Encoding** must be set to **Modulo-128** rather than **Modulo-8**.
- Ungermann-Bass
- ACC
- Banyan Vines

Note: If your analyzer has a color display, the Sniffer Internetwork Analyzer displays proprietary router/bridge information in black.

If the Sniffer Internetwork Analyzer does not automatically recognize the bridge/router in use, you can use the analyzer's **Protocol forcing** feature to force the interpretation of non-standard protocols. For more information on this feature, see Chapter 6, "Using Protocol Forcing."

Encoding Options

Associated with the **Frame type** options are the schemes for encoding frames and the data bits within frames of transmitted data. This includes whether or not to invert the data bits, the method for generating the sequence number of the frames, and the decoding method itself.

Inverting Data Bits

Some WAN/Synchronous networks invert data bits as they come off the wire (changes binary 0 to 1, and vice versa). To make sure the Sniffer analyzer reads the data correctly, you can enable the **Invert** option, which corrects for inversion to read the data correctly.

About WAN/Synchronous Frame Numbering

There are two methods for generating frame sequence numbers. Which of these methods is used is not readily distinguishable by inspection. The method that uses three bits (Modulo 8) is widely used in the United States and in Europe. The method that uses seven bits (Modulo 128) is often used in Japan and in international satellite links.

The default is √ **Modulo 8** enabled.

About WAN/Synchronous Data Signaling

The two most common encoding methods for SDLC and HDLC are NRZ (Non-return to zero) and NRZI (Non-return to zero inverted). To decode transmitted data correctly, you should define the encoding method.

The default is √ **NRZ** enabled.

Line Interface Options

The Sniffer Internetwork (WAN/Synchronous) analyzer provides several options for the physical line interface, including:

- RS232 interface via a DB25 cable
- RS422 interface via a DB15 cable
- RS423 interface via a DB15 cable
- V.10 interface via a DB15 cable
- V.11 interface via a DB15 cable
- V.35 interface via a DB15 cable
- T1 interface via the Network General T1-POD

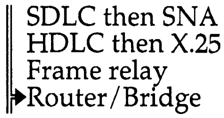
  Note: The Network General T1-POD is supplied separately. It is not included with the Internetwork Analyzer. For more information on the T1-POD, see the documentation accompanying it.

The default is the V.35 interface via a DB15 cable. For complete information on the physical line interfaces supported by the Sniffer Internetwork Analyzer, see the *Sniffer Network Analyzer: Model xx Installation Guide* accompanying your documentation set.

Setting the Sniffer Internetwork Analyzer Options

To define the Sniffer Internetwork Analyzer options:

1. Choose the frame type to determine how the frame itself is encoded. Move to **Options\Frame type**. Move to the desired frame type and press Spacebar.

   SDLC then SNA
   HDLC then X.25
   Frame relay
   ▶Router/Bridge

2. To determine whether to invert the data bits, move to **Options\Encoding\Invert** and press Spacebar to enable (√) or disable (x) the option.
3. To choose the physical line interface for your Internetwork analyzer, move to **Options\Line interface** and highlight the option corresponding to your physical interface. Press spacebar to enable that option.

4. To choose the encoding method determining the level at which data bits are encoded, move to **Options\Encoding** and then to the desired encoding methods and press Spacebar.

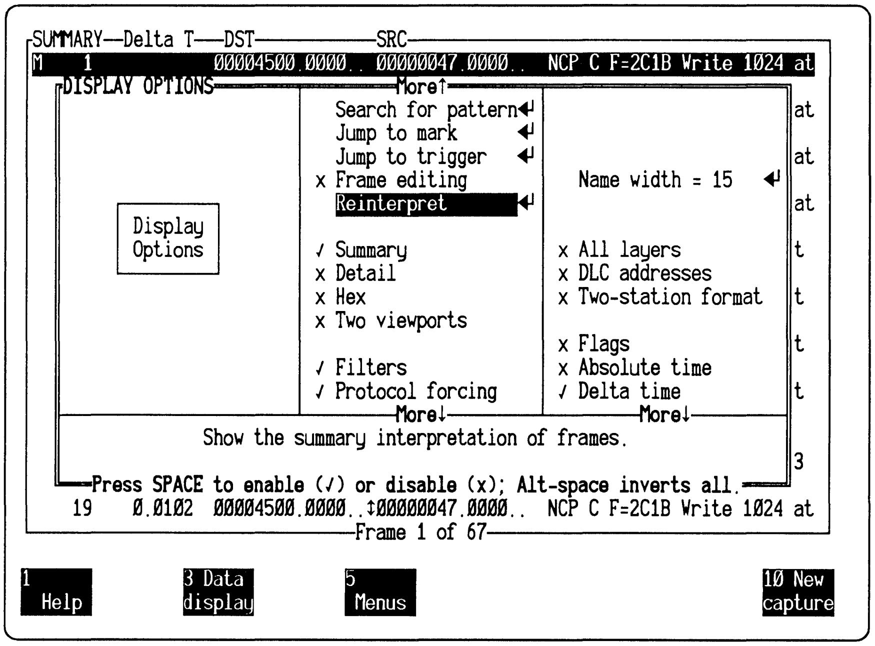
   ▶Modulo 8 (default)
   Modulo 128

   ▶NRZ (default)
   NRZI

Note: If you notice during display that the wrong frame type is displayed, return to the **Options\Frame type** menu and choose the correct frame type. To apply the new interpretation to a set of captured frames, you must reinterpret the frames. The procedure for reinterpreting a set of captured frames is described below.

To reinterpret displayed frames:

1. Press F6 (**Display options**). Figure 2–6 shows the Display Options menu.



```
SUMMARY—Delta T—DST————————SRC——————————————————————————————
M    1          00004500.0000..  00000047.0000..   NCP C F=2C1B Write 1024 at
 DISPLAY OPTIONS—————————————More↑——————————————————————————
                      Search for pattern↵                        at
                      Jump to mark      ↵
                      Jump to trigger   ↵                        at
                    x Frame editing          Name width = 15  ↵
                      Reinterpret       ↵                        at
       Display
       Options      ✓ Summary              x All layers          t
                    x Detail               x DLC addresses
                    x Hex                  x Two-station format  t
                    x Two viewports
                                           x Flags               t
                    ✓ Filters              x Absolute time
                    ✓ Protocol forcing     ✓ Delta time          t
                    ——————More↓——————————————————More↓——————
              Show the summary interpretation of frames.
                                                                 3
  —Press SPACE to enable (✓) or disable (x); Alt-space inverts all.—
   19    0.0102  00004500.0000..↕00000047.0000..  NCP C F=2C1B Write 1024 at
  ———————————————————————Frame 1 of 67————————————————————————
```

Figure 2–6. Reinterpreting frames with the Display Options menu.

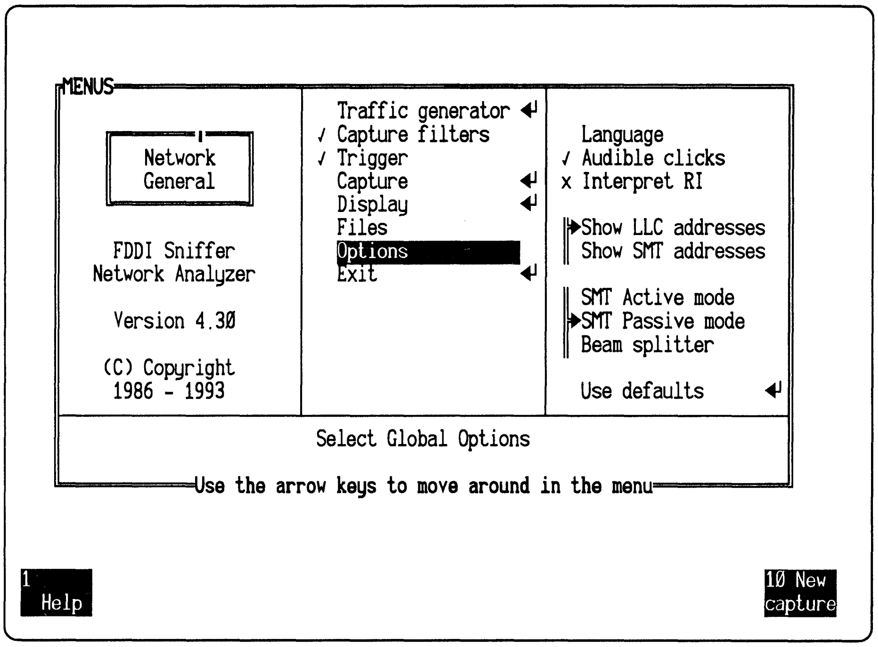
2. In the menu that appears, move to **Reinterpret** and press Enter. Then press F3 (**Data display**) again.

   Result: The frames in the capture buffer are reinterpreted and displayed in accordance with the various parameters set in the Sniffer analyzer menus.

Setting the FDDI Options

On an FDDI Sniffer analyzer, the **Audible clicks, Interpret RI**, and **Use defaults** options operate as they do on an Ethernet network, described in the previous sections. FDDI networks include two additional system options: the station mode and the option to invert addressing.

Figure 2–7 shows the system options associated with an FDDI analyzer.



```
MENUS
                        Traffic generator ↵
   Network            ✓ Capture filters          Language
   General            ✓ Trigger                ✓ Audible clicks
                        Capture            ↵   x Interpret RI
                        Display            ↵
                        Files                   ▶Show LLC addresses
 FDDI Sniffer           Options                  Show SMT addresses
Network Analyzer        Exit               ↵
                                                 SMT Active mode
 Version 4.30                                   ▶SMT Passive mode
                                                 Beam splitter
 (C) Copyright
 1986 - 1993                                     Use defaults       ↵

                        Select Global Options

            Use the arrow keys to move around in the menu

1                                                              10 New
 Help                                                          capture
```

Figure 2–7. FDDI options

Setting the Station Mode

You can set the FDDI analyzer as an SMT Active station, an SMT Passive station, or a beam splitter on the FDDI ring.

Setting the analyzer as an SMT Active station means that it participates in the FDDI network activity. It periodically sends out neighbor information frame (NIF) announcements and responds to its upstream neighbor's NIF requests. A monitoring station can use these announcements to construct an SMT ring map.

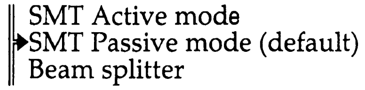
Setting the analyzer as an SMT Passive station means it has a more limited involvement with the ring. It participates at the MAC and CMT levels, and forwards frames, but it does not send NIF announcements and responses, and thus it will not appear in an SMT ring map.

Setting the analyzer as a beam splitter means that it is completely passive and does not participate in any ring activity. You must connect your analyzer to the network via a beam splitter in order to use this setting.

When a beam splitter is used, the maximum length between FDDI stations is considerably less than the standard 2km for multimode fiber. This is due to the signal loss caused by splitting the beam. The vendor of the beam splitter device should specify the signal loss.

To change the station setting:

1. Choose the option you want and press Spacebar.



```
 SMT Active mode
▸SMT Passive mode (default)
 Beam splitter
```

Inverting Addresses

From the perspective of the FDDI analyzer, each station uses two logical addresses to communicate. One form of the address is the canonical form of the assigned DLC address. The other is the most significant bit (MSB) form. When a station transmits LLC frames, the Sniffer analyzer sees the canonical form of its assigned DLC address. However, when the same station transmits SMT or MAC frames, the Sniffer analyzer sees the MSB form of its DLC address.

The **Show LLC addresses** or **Show SMT addresses** option allows you to display the FDDI station addresses using one of the two logical addresses. This option affects all displays except the HEX view where data is presented as provided by the FDDI interface card (that is, with MAC and SMT frame addresses in MSB form and LLC frame addresses in canonical form– see the paragraph below).

Note: The FDDI interface card used by the Sniffer analyzer presents LLC frame addresses to the Sniffer analyzer in canonical form. Consequently, in the HEX view, all LLC frame DLC addresses will be shown in canonical form regardless of the **Options** setting. MAC and SMT frame DLC addresses are always displayed in the HEX view in MSB form.

The default is **Show LLC addresses** enabled —display station addresses using LLC addresses. This option only affects the way DLC addresses are displayed in the Summary and Detail views. The HEX view is unaffected by the setting of this option.

Figure 2–8 illustrates how this feature works. In this example, the assigned IEEE burned-in DLC address is 01-01--01-01-01-01 (the canonical form).

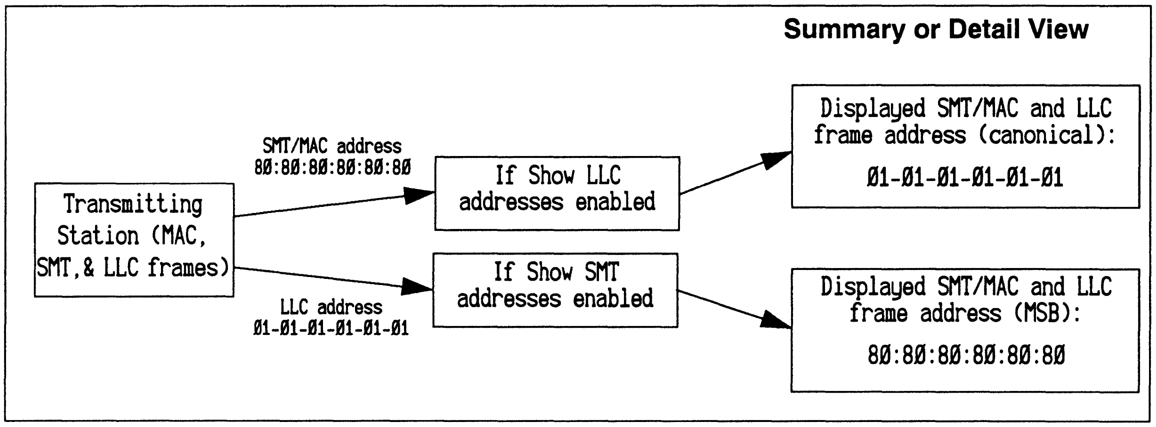

Summary or Detail View
Transmitting Station (MAC, SMT,& LLC frames)
SMT/MAC address
80:80:80:80:80:80
LLC address
01-01-01-01-01-01
If Show LLC addresses enabled
If Show SMT addresses enabled
Displayed SMT/MAC and LLC frame address (canonical):
01-01-01-01-01-01
Displayed SMT/MAC and LLC frame address (MSB):
80:80:80:80:80:80

Figure 2–8. Show LLC or SMT addresses option.

To change the address inversion option:

1. Choose the option you want and press Spacebar.

   ▶Show LLC addresses (default)
   Show SMT addresses

Caution: If you set a capture or display filter or a trigger, make sure that the DLC address you enter matches the option setting you selected. If not, your filter or trigger will not work. For example, if the canonical form of a station address is 00-00-65-0A-00-01 (SMT address is 00:00:A6:50:00:80), and the option is set to Show LLC addresses, make sure you use the canonical form of the DLC address for any station capture or display filter or trigger. If you use the SMT address, the Sniffer analyzer will assume that you are entering an LLC address, and the filter or trigger will not work.

CHAPTER THREE: CAPTURING FRAMES 3

Capturing Frames

Overview

During capture, the Sniffer analyzer passes those frames that pass its capture filters to the capture buffer. As frames are captured, the analyzer displays the results of the capture process in displays that are updated continuously. These displays show either a skyline view that shows traffic density over time, or tables that show station addresses. For ARCNET and LocalTalk, there is also a display that shows a Matrix view.

Before you start capture, you can customize the process to make sure the frames that interest you are captured. To do this, you can prepare for capture by defining various associated options that determine *how* frames will be captured, *which* frames will be captured, and how the capture will be *stopped.*

In addition to describing the **Cable test** feature for Ethernet networks, this chapter describes the options related to capturing frames. This includes:

- Preparing to capture frames

  - Displaying information about the capture buffer

  - Choosing a capture mode

  - Defining capture options

  - Defining capture filters

  - Defining a trigger to stop capture

- Starting the capture

- Options after you stop capture

When capture is complete, the captured frames are interpreted by the protocol interpreters, which interpret and decode the higher-level protocols within the frames. You can then examine the frame-by-frame results in various displays. These topics are discussed in Chapter 4, "Displaying Interpreted Frames."

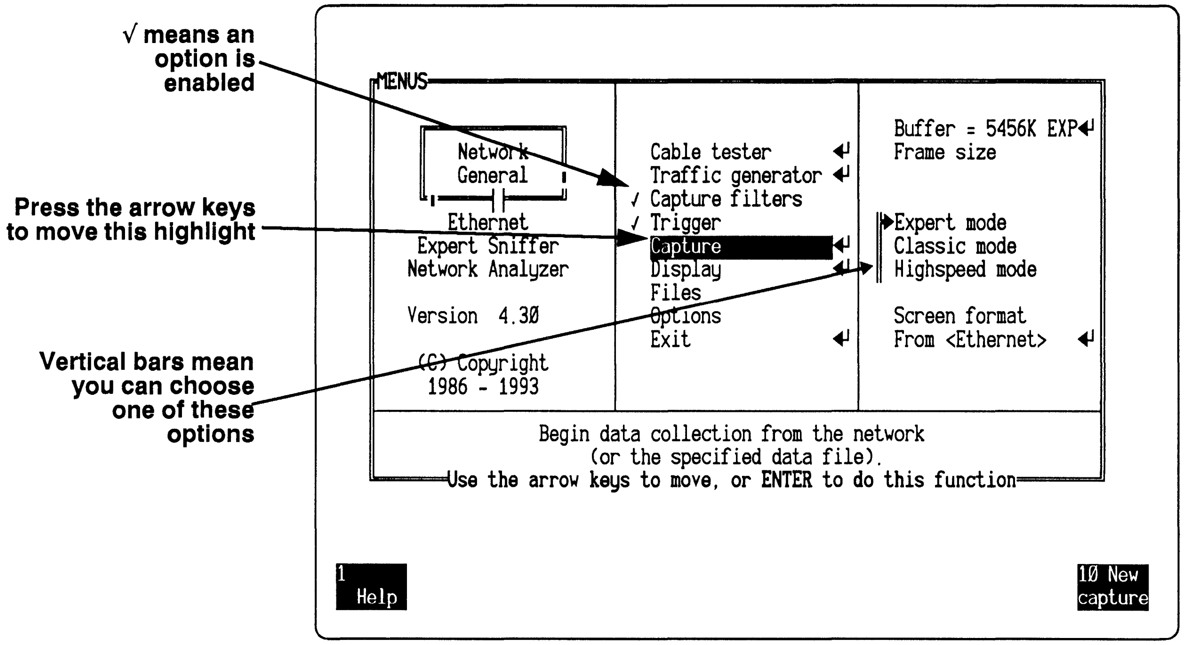
Capture Menu Overview

Figure 3–1 provides an overview of the basic menu items associated with the Capture menu. Many of these items, in turn, are associated with additional options. Although Figure 3–1 shows the menu as it appears on an Ethernet Sniffer analyzer, the basic Capture menu items are similar for all networks.

As with all other menu options, you first press the Cursor keys to move the highlight to the desired option. You can then define that option.

- For options marked with the √ and x symbols, you can press Spacebar to enable (√) or disable (x) the option. To reverse all settings, press Alt-Spacebar.

- For options connected with a vertical bar (radio control), you can choose one of those options by moving to it and pressing Spacebar.
- For options where you must define a specific value, such as an address, you can choose a value from a list or enter the desired value into a dialog box.



Begin data collection from the network
(or the specified data file).
Use the arrow keys to move, or ENTER to do this function

Figure 3–1. Overview of the Capture menu options.

Ethernet Cable Tester

On Ethernet, the Sniffer analyzer provides a cable tester: a means to check and report cable faults. The analyzer's main menu includes an option labeled **Cable tester** (Figure 3–1). The cable test uses the network analyzer's interface card as a time-domain reflectometer. During the test, the analyzer repeatedly emits a pulse and listens for the echo characteristic of certain types of faults.

To test the Ethernet segment for cable faults:

1. In the analyzer's main menu, move the highlight to **Cable Tester** and press Enter (Figure 3–1).

   Result: The analyzer repeatedly emits a test signal on the Ethernet segment to which the network analyzer's interface card is attached. The analyzer overlays a display reporting what faults —if any— have been detected, and updates it as the test is repeated.

2. To terminate the test, press Esc.

The cable tester keeps testing until you terminate it by pressing Esc. While the test is running, the analyzer does not perform any of its other functions.

As long as the tester is active, the Sniffer analyzer repeatedly updates the display so that it shows the cable's current status. As long as it detects no fault, it displays the message `No cable fault found.`

The analyzer can detect a cable fault located between the adapter card and the transceiver that connects it to the network. It can also detect an open line or a short in the network cabling beyond the transceiver. The Sniffer analyzer cannot test for faults, open lines, or shorts on cable segments separated by a bridge or repeater from the segment on which it is located.

Automatic Test at First Capture

Under some circumstances, when you start capture, the analyzer first runs a brief cable test. It does this automatically, without being asked. It runs the automatic test only when this is the first live capture since the analyzer program started.

If the automatic test discovers no fault, there is no display and the analyzer proceeds directly with capture.

If the automatic test detects a cable fault, the analyzer reports it, and gives you the choice to proceed with capture or to halt.

The automatic test sends a packet out onto the Ethernet cable. If you do not want this test run, you can disable it with the **Cable test** option in the analyzer's Options menu. For more information on this option, see Chapter 2, "Defining System Options."

Messages Provided by the Cable Tester

The Cable Tester will generate the following messages:

Cable OK	Means the cable is OK.
Cable short	Means there is a short somewhere on the cable.
Cable open	Means the cable is not terminated on at least one end.

In addition, the analyzer may generate the "Cable fault," or "Cable unknown fault," messages. This usually means that one of the following conditions exists:

1. The transceiver is not connected to the AUI port.
2. There isn't a BNC cable or valid LAN connection to the transceiver.
3. The BNC cable is open at both ends (no terminators).

Limitations of the Cable Tester

- The Sniffer analyzer readily detects an open line and produces a steady diagnostic display. The reflection characteristic of a short circuit between the center conductor and ground is harder to discriminate from a normal signal, so the analyzer sometimes misses it.
- Certain intermittent defects can produce a jittering display. As it continuously updates the display, the Sniffer analyzer may assign different diagnoses to a continuously changing situation.
- When a collision anywhere on the network coincides with a test pulse, the resulting signal is similar to the pattern produced by an open line. However, a collision produces no more than a momentary flicker.
- Transceivers vary in the way they transmit the test pulse and its echo. This variation in turn produces variation in the behavior of the cable tester. Most transceivers produce useful results, but some do not.
- The procedure for converting time estimates to distance is subject to numerous unpredictable sources of variation.
- Under heavy traffic loads, the cable tester will occasionally report "Cable open," when it is actually not. This is because the analyzer needs enough "room" on the wire to send out its test pulse. As traffic subsides, the display will change to read, "Cable OK."

Displaying Information About the Capture Buffer

Before you start a capture, you may want to display information about the size of the capture buffer and detailed memory statistics that include memory allocation for the capture buffer.

The Capture menu shows the number of kilobytes the computer has allocated to the capture buffer. In Figure 3–1, for example, the buffer size is 2592 Kbytes.

To check the size of the capture buffer:

1. Move to **Capture** and look at the **Buffer=** item.

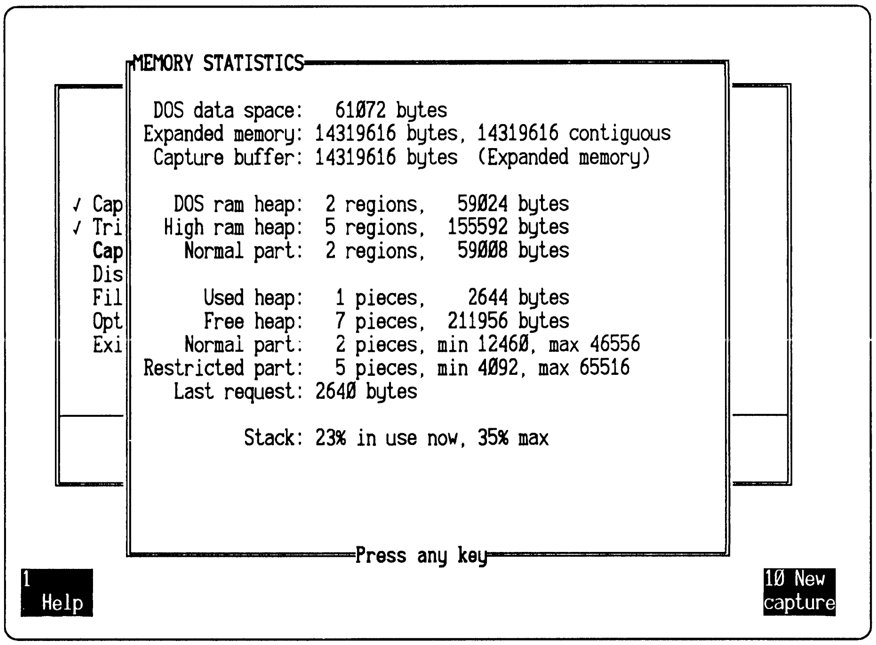
   Note the buffer size (in kilobytes). If the buffer makes use of expanded memory, the number of kilobytes is followed by the letters EX.

You can also display other details about the Sniffer analyzer's memory usage.

To display a summary of memory statistics:

1. Move to **Capture\Buffer** and press Enter.

   The Sniffer analyzer displays a summary of memory utilization statistics, including DOS data space, expanded memory, and various components of the system heap, as shown in Figure 3–2.



```
MEMORY STATISTICS

   DOS data space:   61Ø72 bytes
  Expanded memory: 14319616 bytes, 14319616 contiguous
   Capture buffer: 14319616 bytes  (Expanded memory)

     DOS ram heap:  2 regions,   59Ø24 bytes
    High ram heap:  5 regions,  155592 bytes
      Normal part:  2 regions,   59ØØ8 bytes

        Used heap:   1 pieces,    2644 bytes
        Free heap:   7 pieces,  211956 bytes
      Normal part:   2 pieces, min 1246Ø, max 46556
  Restricted part:   5 pieces, min 4Ø92, max 65516
     Last request: 264Ø bytes

            Stack: 23% in use now, 35% max

                      Press any key
```

Figure 3–2. Displaying memory statistics.

Preparing to Capture Frames: An Overview

Before you start to capture, you can specify how the system captures frames, which frames you want to capture, how to display information during the capture, and how to stop the capture.

In general, you should set these options before you start capturing. For each option, you can accept the predefined settings (defaults) or change them according to your needs. You can also save combinations of these options (setups) and apply these setups to later captures with the same criteria. For procedures for saving and loading a setup file, see "Saving the Current Options in the STARTUP File" on page 5–15. You can also disable most options temporarily or revert to the Sniffer analyzer's default options.

Figure 3–3 provides an overview of the tasks involved in preparing for capture. Not all options are listed in the table. Each task is described in more detail in the sections that follow.

Preparing to Capture Frames

Choose a capture mode	Classic mode	
	Expert mode	
	Highspeed mode*	
Define capture options	Frame size	
	Capture source	Live network or data (trace) file
	Screen format	Units of measurement (frames or Kbytes)
		Tabular format (individual or pair counts)
		Skyline format (at defined intervals)
		Matrix format**
Define capture filters	Known/unknown stns	
	Destination class	
	Address match	
	Protocol	
	Pattern matches	
	Defective frames*	
Define stop of capture	Stop when full	
	Stop at trigger	Defective frames*
		External trigger
		Pattern trigger
		Trigger position (delay)
Define disk snapshot	Save at trigger or when full?	
	Size of snapshot files?	
	Number of files?	
	Overwrite files?	

*Ethernet, PC Network only
**ARCNET LocalTalk only
***FDDI only

Figure 3–3. Preparing for capture: an overview.

Choosing a Capture Mode

When your Sniffer Network Analyzer is shipped, it is set up to capture and display in **Expert mode**[1], with all options preset to reasonable default values. In addition to this mode, you can choose **Classic mode**. **Highspeed mode** is also available on PC Network or Ethernet analyzers to avoid losing frames during heavy traffic.

Note: This manual describes the operations of the Sniffer analyzer in Classic mode. For information on features associated with Expert mode, see the companion publication, *Expert Sniffer Network Analyzer Operations*.

To choose a capture mode and the associated options:

1. Move to the desired option and press Spacebar.

   ▸ Expert mode (default)
   Classic mode
   Highspeed mode

2. Define the associated options, which are described in the sections that follow.

Defining the Basic Capture Options

In addition to defining the capture filters and the trigger that stops the capture, you can define the following basic options.

- The size of captured frames
- The capture source (live or from a file)
- The screen format of the views during capture

Defining Frame Size during Capture

You can choose to truncate frames that exceed a certain length to fit more frames into the capture buffer, thus extending the time covered by the capture and reducing the size of the capture data file and saving disk space (if you choose to save that file to disk). On a very busy network, truncation may also help avoid losing frames, since a longer frame takes slightly more time to store. The default is to capture the entire frame.

When each high-level frame is entirely contained within a lower-level frame, truncation leaves the headers and discards part of the high-level data. Since the headers usually contain the information you need for analysis, little is lost by discarding the later parts of the frame.

However, some high-level protocols—such as TCP—are byte-oriented rather than frame-oriented, while others—such as ISO or X Window—permit very long messages. As a result, a single ISO or X message may span several lower-level TCP frames.

[1] The FDDI Analyzer does not support the Expert or Highspeed modes.

Figure 3–4 shows how a sequence of variable-length higher-level frames may be sliced arbitrarily and packed into frames of an intermediate byte-oriented protocol such as TCP. The start of a new spanned frame is not required to force a new lower-level frame. Thus, an X header (for example) may occur at any position in a TCP frame's data field.

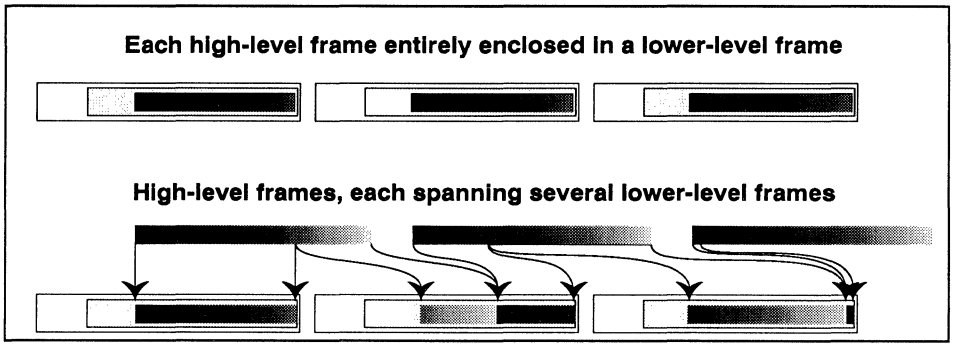

Each high-level frame entirely enclosed in a lower-level frame
High-level frames, each spanning several lower-level frames

Figure 3–4. Effect of high-level frames spanning multiple DLC frames.

If your analysis requires keeping track of the headers of high-level spanned frames, it is *essential* to save whole frames. Otherwise, the headers and boundaries of the highest levels may be lost.

See the *Expert Analyzer Operations* manual for information about how frame slicing affects the Expert analysis.

To limit capture to the first n bytes of a frame:

1. Move to **Capture\Frame size**.
2. Move to the desired maximum length and press Spacebar to choose that option.

```
   32 bytes
   64 bytes
  128 bytes
  256 bytes
  512 bytes
▸ Whole frame (default)
```

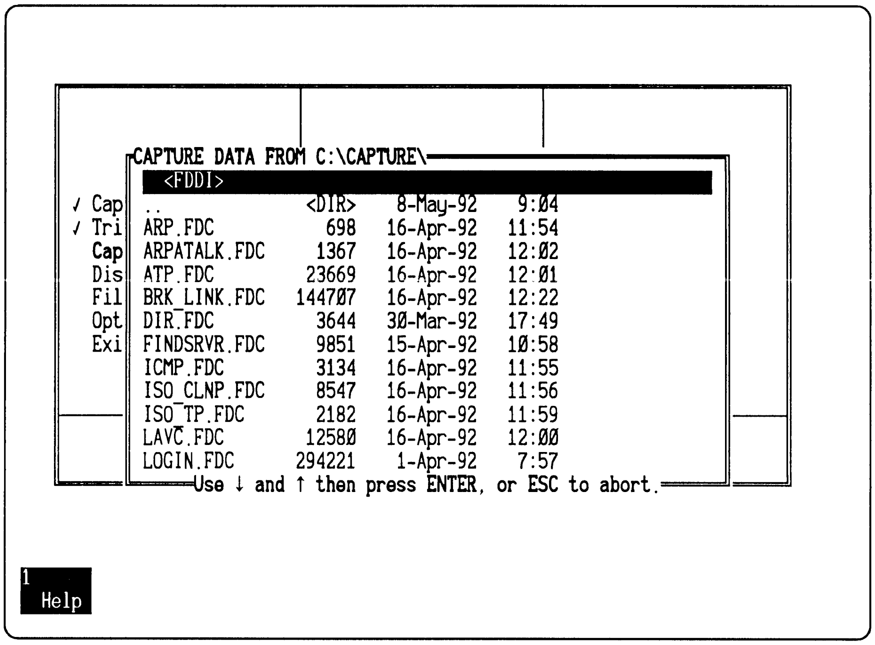
Defining the Capture Source: Live Network or Data File

You can determine whether data is captured from a live network or played back from a file. The capture option labeled **From <xxx>** determines the capture source. The default is to capture from the network, as indicated by the **<From Ethernet>**, **<From Token Ring>**, **<From FDDI>**, or **<From Synchronous>** items, as appropriate. After you set up a capture from a file, **From** is followed by the name of that file.

To capture from a file:

1. Move to **Capture\From <xxx>** and press Enter. (**From** is at the bottom of the menu; if necessary, scroll down to display it.)

A dialog box appears that shows the files that contain saved frames (trace files) in the CAPTURE directory of the Sniffer's hard drive (Figure 3–5).



```
         CAPTURE DATA FROM C:\CAPTURE\
           <FDDI>
✓ Cap   ..                <DIR>    8-May-92    9:Ø4
✓ Tri   ARP.FDC             698   16-Apr-92   11:54
  Cap   ARPATALK.FDC       1367   16-Apr-92   12:Ø2
  Dis   ATP.FDC           23669   16-Apr-92   12:Ø1
  Fil   BRK_LINK.FDC     1447Ø7   16-Apr-92   12:22
  Opt   DIR.FDC            3644   3Ø-Mar-92   17:49
  Exi   FINDSRVR.FDC       9851   15-Apr-92   1Ø:58
        ICMP.FDC           3134   16-Apr-92   11:55
        ISO_CLNP.FDC       8547   16-Apr-92   11:56
        ISO_TP.FDC         2182   16-Apr-92   11:59
        LAVC.FDC          1258Ø   16-Apr-92   12:ØØ
        LOGIN.FDC        294221    1-Apr-92    7:57
             Use ↓ and ↑ then press ENTER, or ESC to abort.

1
 Help
```

Figure 3–5. Choosing the capture source.

2. Move to the file from which you want to capture and press Enter.

   Note that the name of the selected file now appears after **From < xxx>**. The Sniffer analyzer reads this file into the adapter card and then sends the file to the capture buffer. All filters and the trigger are applied as the file contents are captured.

3. To move to a subdirectory other than the CAPTURE directory, move to **<DIR>**, press Enter, and then select the desired directory.

Limitations of Capturing from a Saved Trace File

When you capture frames from a trace file, the analyzer cannot emulate the speed at which frames were captured from the network due to limitations enforced by the time required to access the disk drive (where the trace file is stored). Depending on your platform, capturing from a trace file is at least 20 times slower than the real captured traffic. That is, statistics relating to traffic rates will be at least 20 times slower during playback than they were during actual capture.

To capture from the network:

When the currently selected capture source is a file, you must reselect the appropriate network if you want to capture from the network.

1. Move to **Capture\From <xxx>** and press Enter.
2. In the dialog box that appears, move to the network name (at the top of the screen) and press Enter.

Defining Screen Format During Capture: An Overview

You can observe the capture process in different formats, depending on whether you are working with a LAN or a WAN/Synchronous network and on the **Screen format** options you define.

Screen Formats for LANs During Capture

For LANs, you can choose between various screen format options to display data as it is captured, including:

- Tabular views (called **Counts**), as either individual or pair counts.
- Skyline view, at one of three intervals between updates.
- Matrix view (ARCNET and LocalTalk only), which shows the running totals by source, arranged without labels in a 16x16 matrix.

For all views, you can define the count units used (frame counts, Kbyte counts, or network usage) and the scale of the bar graph that shows real-time traffic density (linear or logarithmic).

Figure 3–6 summarizes the LAN **Screen format** options for most LANs.

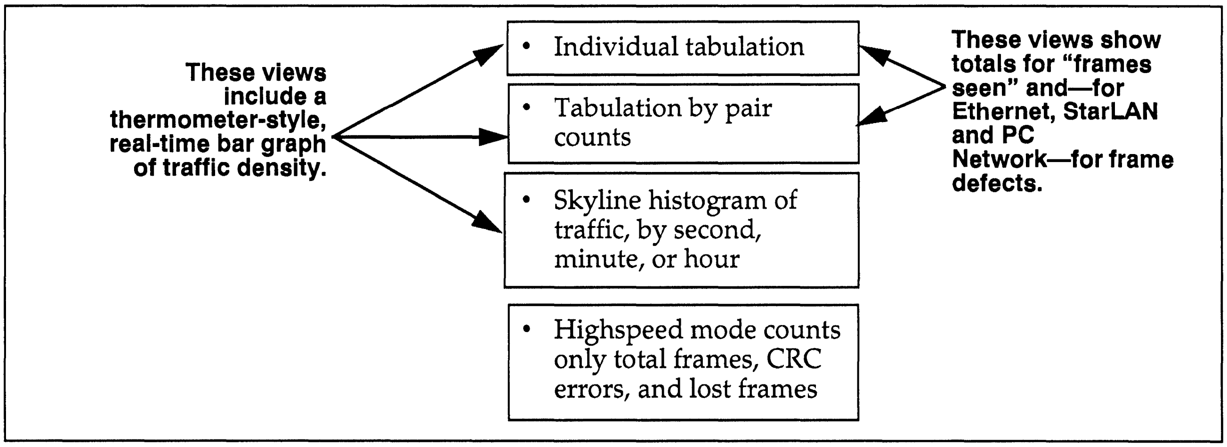

These views include a thermometer-style, real-time bar graph of traffic density.
• Individual tabulation
• Tabulation by pair counts
• Skyline histogram of traffic, by second, minute, or hour
• Highspeed mode counts only total frames, CRC errors, and lost frames
These views show totals for "frames seen" and—for Ethernet, StarLAN and PC Network—for frame defects.

Figure 3–6. Summary of screen formats for most LANs.

Figure 3–7 illustrates these options.

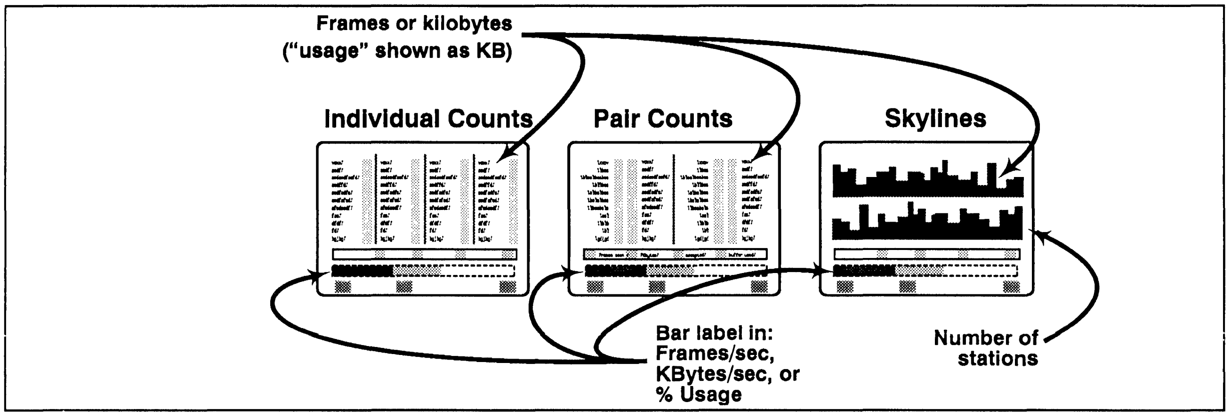


Figure 3–7. Effect of various screen format options.

Screen Formats for WAN/Synchronous Networks During Capture

On the Sniffer Internetwork Analyzer, you can further define the following options associated with each of the screen formats:

- Tabular view: whether to display all stations or active stations only
- Skyline view: the interval between updates (the default)
- Both views: the units used to measure the capture (frame counts or Kbyte counts) and the scale of the bar graph that shows real-time traffic density (linear or logarithmic).

Note: Although the tabular view (**Counts**) is available when the **Router/Bridge** option is enabled, the screen will remain blank (except for the DTE/DCE counters and the various counters at the bottom of the screen). This is because the **Router/Bridge** option tells the analyzer to expect proprietary versions of HDLC. These versions do not conform to the traditional HDLC standard, and as such, traffic cannot be tallied according to the types of frames sent (such as Info, RR, RNR, REJ, and so on). When capturing with **Router/Bridge** enabled, it is best to leave the Skylines view (the default) enabled.

Defining the Screen Format During Capture: Procedure

Defining a screen format includes choosing between one of two tabular formats and the Skyline format. For all formats, you can define whether data is shown as frame counts, Kbyte counts, or in terms of network usage. You can also determine the scale of the bar graph at the bottom of the display.

Each option is explained in more detail after the procedure.

To select the screen format for most LANs:

1. Move to **Capture\Screen format** and choose desired units of measure.

```
▸Show frame counts (default)
 Show Kbyte counts
 Show NW usage
```

2. Choose the desired scale of the bar graph.

   Linear bar scale
   ▶Log bar scale (default)

3. Choose the desired display format.

   Individual counts
   ▶Pair counts (default)
   Skylines

   If you chose Skylines, define the interval at which the screen is updated.

   ▶1 second update (default)
   1 minute update
   1 hour update

To select the screen format for a WAN/Synchronous link:

1. Move to **Capture\Screen format** and choose desired units of measure.

   ▶Show frame counts (default)
   Show Kbyte counts

2. Choose the desired scale of the bar graph.

   Linear bar scale
   ▶Log bar scale (default)

3. Choose the desired display format.

   Counts
   ▶Skylines (default)

   If you chose Skylines, define the interval at which the screen is updated.

   ▶1 second update
   1 minute update (default)
   1 hour update

   If you chose Counts, define which stations are shown.

   Display all
   ▶Display active (default)

Units of Measure

You can select the units of measure in which capture activity is reported. The choices and their effects on individual counts, total counts, and the bar graph are shown in Figure 3–8. The default is to show frame counts.

Units of measure include:

- Frame counts
- Kilobytes
- Network usage (LAN only)

	Tabular units	Skyline units	Bar graph units	Counters
Frame counts	Frames	Frames	Frames	both
Kilobytes	Kilobytes	Kilobytes	Kilobytes	both
Network usage (LAN)	Kilobytes	Kilobytes	Percentage of bandwidth	both

Figure 3–8. Capture menu options for frames, kilobytes, and usage.

Traffic Density Bar Graph

As capture proceeds, the Sniffer analyzer displays a thermometer-style horizontal bar graph that shows real-time variations in traffic density (Figure 3–9). If the **Audible clicks** option (Options menu) is enabled, the intensity of the clicks corresponds to the traffic density.

For LAN traffic, a single bar is updated several times a second. The bar shows a moving average of the last half-second's activity and the "high water" mark—the maximum activity recorded during the current capture session. Figure 3–9 shows a sample bar graph, with the Frames option enabled, for a LAN.

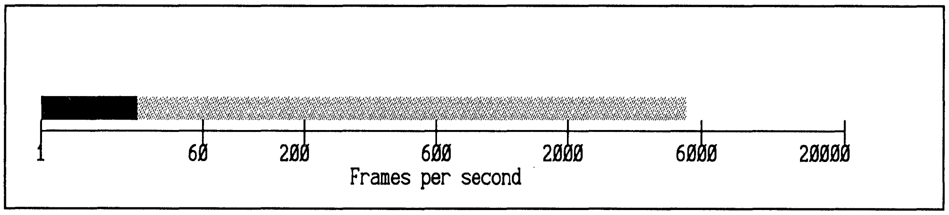


Figure 3–9. Traffic density bar graph for LANs (logarithmic scale).

For WAN/Synchronous traffic, there are two bar graphs; one for the DTE and one for the DCE counters, as shown in Figure 3–10.

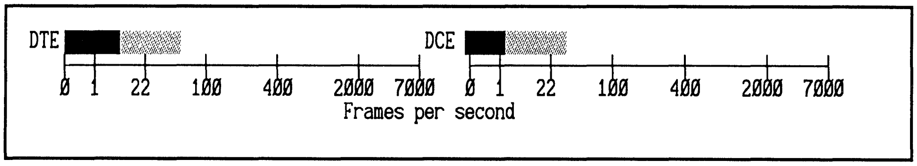


Figure 3–10. Traffic density bars for WAN/Synchronous link.

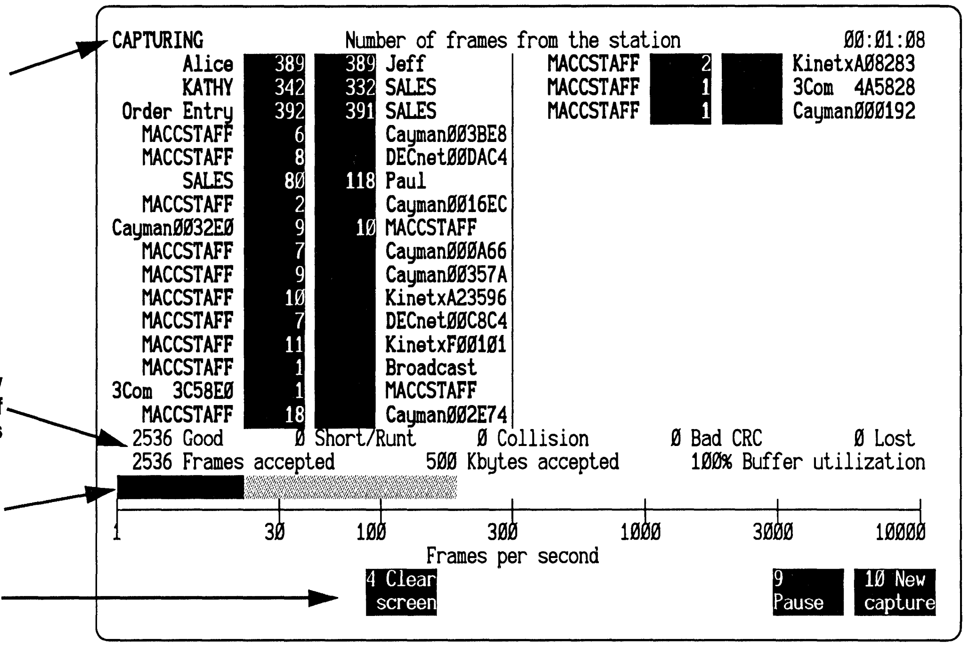
You can select either a logarithmic or a linear horizontal scale for the traffic density bar graph.

Linear	A fixed distance (for example, 1 centimeter) corresponds to an absolute change in traffic density (for example, 10,000 frames).
Logarithmic	A fixed distance (for example, 1 centimeter) corresponds to a relative change (for example, 10 percent).

When the overall density is low, small variations are easier to see on a logarithmic scale (the default).

Information in the Tabular Views

In addition to the counters that provide information about the frames seen and the buffer utilization, the tabular displays show details about which stations are active. You can display this information as pair counts (transmitting and receiving stations) or as individual counts (transmitting stations only). Figure 3–11 shows a sample pair count display for Ethernet.



```
CAPTURING               Number of frames from the station                 ØØ:Ø1:Ø8
       Alice  389  389 Jeff         |  MACCSTAFF   2        KinetxAØ8283
       KATHY  342  332 SALES        |  MACCSTAFF   1        3Com  4A5828
 Order Entry  392  391 SALES        |  MACCSTAFF   1        CaymanØØØ192
   MACCSTAFF    6      CaymanØØ3BE8
   MACCSTAFF    8      DECnetØØDAC4
       SALES   8Ø  118 Paul
   MACCSTAFF    2      CaymanØØ16EC
CaymanØØ32EØ    9   1Ø MACCSTAFF
   MACCSTAFF    7      CaymanØØØA66
   MACCSTAFF    9      CaymanØØ357A
   MACCSTAFF   1Ø      KinetxA23596
   MACCSTAFF    7      DECnetØØC8C4
   MACCSTAFF   11      KinetxFØØ1Ø1
   MACCSTAFF    1      Broadcast
3Com  3C58EØ    1      MACCSTAFF
   MACCSTAFF   18      CaymanØØ2E74
  2536 Good        Ø Short/Runt     Ø Collision       Ø Bad CRC        Ø Lost
  2536 Frames accepted        5ØØ Kbytes accepted       1ØØ% Buffer utilization

1            3Ø        1ØØ        3ØØ        1ØØØ        3ØØØ        1ØØØØ
                          Frames per second
                4 Clear                                   9        1Ø New
                  screen                                  Pause    capture
```

"CAPTURING" indicates that capture is in progress

Counters show breakdown of frames

Bar graph shows traffic density

Function keys provide access to other functions

Figure 3–11. Sample tabular Ethernet display: pair counts.

Counters

As capture proceeds, you can see the total number of frames (whether or not they passed the capture filters) and the total number of kilobytes they contained. On token ring and FDDI networks, these totals are reported directly as "frames seen" and "kilobytes seen."

On other networks, there is no single total for "frames seen," but separate counts for various subtotals. On Ethernet, for example, there are totals for the total numbers of good frames, short/runt frames, bad CRC frames, and lost frames, as shown in Figure 3–11. On analyzers with Ethernet-II adapter cards, there is also a counter for collision frames.

On an FDDI analyzer, there are three counters whose function is not entirely self-evident — Error, Beacon, and RingOp.

- The Error counter is active only when capturing error frames. When the counter is active, the analyzer pre-scans all frames to derive the error count, regardless of how the other capture filters are set. The count includes frame fragments and all frames that have an invalid frame status field, a bad CRC, or the E-flag set.
- The Beacon counter applies to all frames regardless of how any of the capture filters are set. The analyzer pre-scans all the frames to derive the beacon frame count.
- The RingOp counter displays the RingOp value that is passed to the analyzer by the FDDI adapter. The count is updated once each second. This count indicates how many times the ring toggles from operational to non-operational status.

  When the analyzer is in beam splitter mode, the RingOp counter is also incremented when the analyzer's link is disconnected, even though there is no RingOp event on the ring being observed.

Buffer Utilization

During capture, the Sniffer analyzer continuously updates a counter that shows the percentage of the capture buffer that has been filled, up to 100 percent. When the buffer is full, the oldest frames are purged while capture continues.

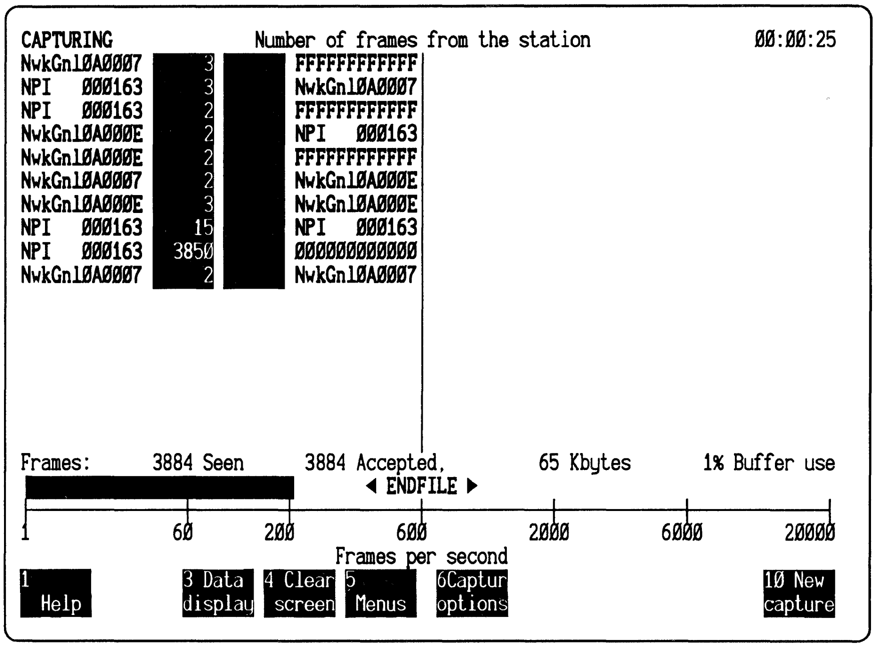
Station Names

If the current name table includes the symbolic names associated with various DLC addresses, the analyzer displays those names in the tabular displays. These names make the displays more meaningful and make it easy to identify stations—and suspected intruders. If a symbolic name is not in this table, the analyzer displays only the DLC address.

On startup, the Sniffer analyzer loads the name table from the STARTUP.*xx*D file (where *xx* is a two-letter abbreviation for the analyzer's topology). To include symbolic names in the displays, you can edit this table to assign names to the addresses you expect to see during the capture. You can also capture for a while to detect unnamed addresses and then edit the table to include the corresponding names. For more information about making optimal use of the name table, see "Managing Names" on page 5–3.

Pair Counts During Capture: LAN

When displaying pair counts during capture, detected pairs fill the available screen positions until the screen is full (Figure 3–12). For each pair of stations, there is one counter for traffic in the direction first detected and another for traffic in the reverse direction, in either frames or kilobytes. The number closest to the station's name describes transmissions *from* that station *to* the other station.



```
CAPTURING                Number of frames from the station                00:00:25
NwkGn10A0007      3      FFFFFFFFFFFF
NPI   000163      3      NwkGn10A0007
NPI   000163      2      FFFFFFFFFFFF
NwkGn10A000E      2      NPI   000163
NwkGn10A000E      2      FFFFFFFFFFFF
NwkGn10A0007      2      NwkGn10A000E
NwkGn10A000E      3      NwkGn10A000E
NPI   000163     15      NPI   000163
NPI   000163   3850      000000000000
NwkGn10A0007      2      NwkGn10A0007

Frames:       3884 Seen       3884 Accepted,        65 Kbytes        1% Buffer use
                                  ◀ ENDFILE ▶
```

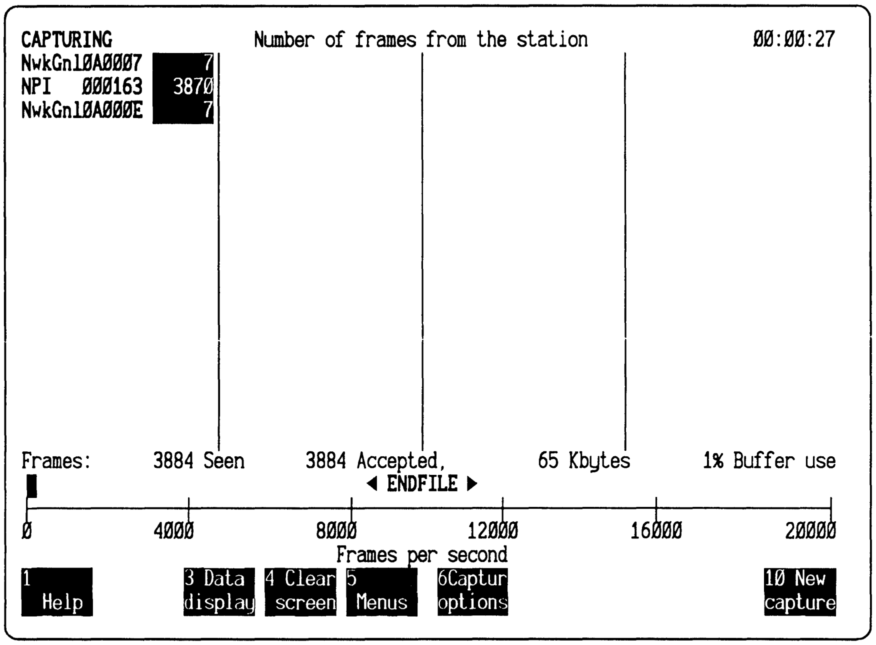
Figure 3–12. Sample tabular view: pair counts.

When all available screen slots are filled, new pairs are not added to the screen. However, the counters that list the total and various subtotals continue to be updated. To clear the screen and start a new tabulation, press F4 (**Clear Screen**).

Note: Clearing the screen has no effect on the frames in the capture buffer.

Individual Counts During Capture: LAN

As with pair counts, the Sniffer analyzer adds an entry for each station that transmits, in the order detected (Figure 3–13). Because these entries record the source but not the destination, there is more room for possible entries.



```
CAPTURING             Number of frames from the station              00:00:27
NwkGnl0A0007       7
NPI   000163    3870
NwkGnl0A000E       7

Frames:      3884 Seen     3884 Accepted,        65 Kbytes       1% Buffer use
                                ◀ ENDFILE ▶
0            4000          8000          12000         16000         20000
                              Frames per second
```

Figure 3–13. Sample tabular view: individual counts.

When all slots on the screen are filled, grand total and detail counts are updated, although new stations that are detected are not listed. To clear the screen and start a new tabulation, press F4 (**Clear screen**). Frames in the capture buffer are not affected.

Because ARCNET and LocalTalk use one-byte DLC addresses, there are exactly 256 possible addresses. For these networks, you can display individual counts in a matrix of 16 rows and 16 columns, labeled 0 through F. In the Matrix view, there is no room for symbolic names.

In the **Matrix** view on ARCNET networks, you can "probe" all stations, to find out which stations are on the network. Each station responds with one of the following replies, which appears at each station's slot in the display:

New — The station that responded to the probe did not appear in previous tallies.

Gone — The station appeared in previous tallies but did not respond to this probe.

n — A number indicates a station already known to be present. (0 indicates that no frames were transmitted, but the station responded to an earlier probe).

. — A dot serves as a place holder that represents an address that has neither transmitted nor responded to the probe.

To "probe" an ARCNET network:

1. With the Matrix view displayed, press F2 (**Probe network**).

In addition to the indicators that show new, gone, and current stations, the top of the screen shows the number of stations that responded since the last probe and whether or not they are still on the network. The totals below the columns show totals for the entire capture session.

Function Keys Available in the LAN Tabular Views

While observing a capture in one of the tabular views, the following function keys are available.

F2 (ARCNET only) **Network probe**. Pauses capture and "probes" all stations. Each station responds with "New," "Gone," "n," or "."

F4 **Clear screen**. Clears the screen and resets all counters to 0.

F9 **Pause.** Temporarily stops screen updates and displays a new set of function keys, listed as follows:

> F1 **Help.** Displays the main Help menu.
>
> F3 **Data display.** Interprets the frames in the capture buffer and displays them in the default (or chosen) display format.
>
> F4 **Clear screen.** Clears the screen and resets all counters to 0. (This has no effect on the frames in the capture buffer.)
>
> F5 **Menus.** Displays the main menu.
>
> F6 **Capture options.** Displays the options for choosing the screen format.
>
> F9 **Resume.** Resumes the display of the tabular views. If you changed any options, the views change accordingly.

F10 **Stop capture**. Stops the capture and redisplays the main menu.

Frame Counts Display During Capture: WAN/Synchronous

On a Sniffer Internetwork Analyzer, the tabular view shows counters for the X.25, HDLC, SNA, and Frame relay protocols, as well as a listing of detected calls. How screens are displayed depends on how you defined the **Frame type** option when defining system options with the Options menu. For more information, see "Frame Type Options" on page 2–12.

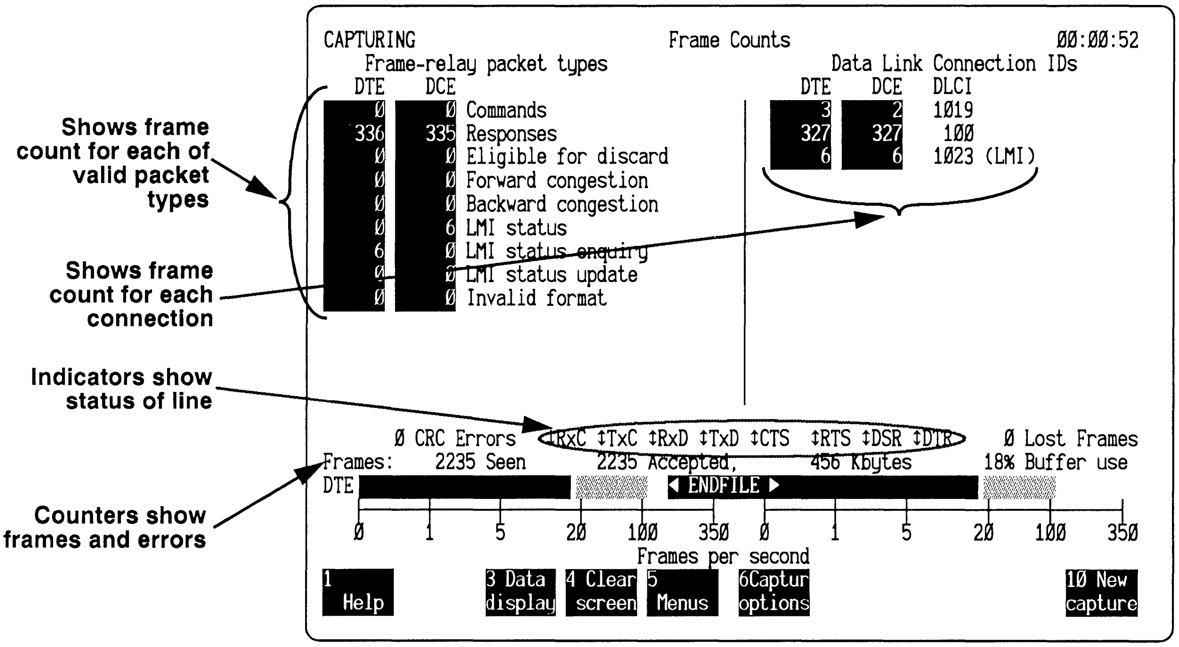
As with the tabular views for a LAN, these views show various counters near the bottom of the screen, including CRC errors, lost frames, total frames seen, and the percentage of the buffer used. Also note that there are two bar graphs that show traffic density, one for DTE and another for DCE.

In addition, a one-line summary shows the status of the line, using the RS232 indicators RxC, TxC, RxD, TxD, CTS, DSR, and DTR. The condition of each indicator is shown with an up arrow (for a logical 1), a down arrow (for a logical 0), and ↕, which means the indicator's status changed in the last second.

Note: Although the tabular view is available when the **Router/Bridge** option is enabled, the screen will remain blank (except for the DTE/DCE counters and the various counters at the bottom of the screen). This is because the **Router/Bridge** option tells the analyzer to expect proprietary versions of HDLC. These versions do not conform to the traditional HDLC standard, and as such, traffic cannot be tallied according to the types of frames sent (such as Info, RR, RNR, REJ, and so on). When capturing with **Router/Bridge** enabled, it is best to leave the Skylines view (the default) enabled.

Note: If you do capture in the tabular view with the **Router/Bridge** option enabled, the message, "This screen intentionally left blank" appears. The paragraph above explains why.

Figure 3–14 shows a capture using the **Frame relay** access protocol.



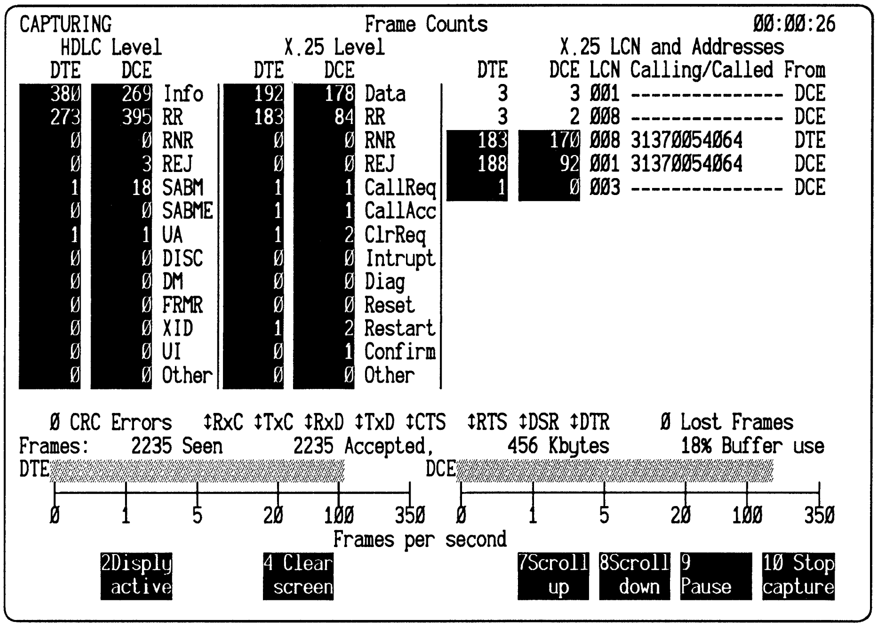
Shows frame count for each of valid packet types
Shows frame count for each connection
Indicators show status of line
Counters show frames and errors

```
CAPTURING                          Frame Counts                            ØØ:ØØ:52
    Frame-relay packet types                            Data Link Connection IDs
   DTE    DCE                                         DTE    DCE   DLCI
     Ø      Ø Commands                                  3      2   1Ø19
   336    335 Responses                               327    327    1ØØ
     Ø      Ø Eligible for discard                      6      6   1Ø23 (LMI)
     Ø      Ø Forward congestion
     Ø      Ø Backward congestion
     Ø      6 LMI status
     6      Ø LMI status enquiry
     Ø      Ø LMI status update
     Ø      Ø Invalid format

      Ø CRC Errors  ↕RxC ↕TxC ↕RxD ↕TxD ↕CTS  ↕RTS ↕DSR ↕DTR    Ø Lost Frames
Frames:   2235 Seen      2235 Accepted,      456 Kbytes         18% Buffer use
DTE                          ◀ ENDFILE ▶
  Ø     1     5    2Ø    1ØØ   35Ø  Ø     1     5    2Ø    1ØØ   35Ø
                          Frames per second
1          3 Data  4 Clear 5        6Captur                         1Ø New
  Help     display  screen  Menus   options                         capture
```

Figure 3–14. Internetwork Analyzer capture view: Frame relay access protocol.

The left side of the screen shows the valid packet types supported by the Frame relay protocol, as well as the number of frame types detected during capture. The right side shows the number of connections during the capture. Each connection is identified by a unique number; the Data Link Connection ID (DLCI). Each DLCI can be assigned a particular type of connection—DLCI 1023, for example, is reserved for Frame Relay network management information (Local Management Interface).

Figure 3–15 shows a capture using the **X.25/HDLC** access protocol.



```
CAPTURING                            Frame Counts                      ØØ:ØØ:26
   HDLC Level              X.25 Level                X.25 LCN and Addresses
  DTE    DCE            DTE    DCE           DTE     DCE LCN Calling/Called From
  38Ø    269 Info     | 192    178 Data    |   3       3 ØØ1 --------------- DCE
  273    395 RR       | 183     84 RR      |   3       2 ØØ8 --------------- DCE
    Ø      Ø RNR      |   Ø      Ø RNR     | 183     17Ø ØØ8 3137ØØ54Ø64     DTE
    Ø      3 REJ      |   Ø      Ø REJ     | 188      92 ØØ1 3137ØØ54Ø64     DCE
    1     18 SABM     |   1      1 CallReq |   1       Ø ØØ3 --------------- DCE
    Ø      Ø SABME    |   1      1 CallAcc |
    1      1 UA       |   1      2 ClrReq  |
    Ø      Ø DISC     |   Ø      Ø Intrupt |
    Ø      Ø DM       |   Ø      Ø Diag    |
    Ø      Ø FRMR     |   Ø      Ø Reset   |
    Ø      Ø XID      |   1      2 Restart |
    Ø      Ø UI       |   Ø      1 Confirm |
    Ø      Ø Other    |   Ø      Ø Other   |

   Ø CRC Errors    ↕RxC ↕TxC ↕RxD ↕TxD ↕CTS  ↕RTS ↕DSR ↕DTR      Ø Lost Frames
Frames:    2235 Seen       2235 Accepted,      456 Kbytes        18% Buffer use
DTE                                    DCE
   Ø     1     5     2Ø   1ØØ   35Ø  Ø     1      5      2Ø     1ØØ    35Ø
                            Frames per second
```

Figure 3–15. Internetwork Analyzer capture view: X.25/HDLC access protocol.

The upper area of the screen consists of three main zones.

- The left zone shows the counters for each of twelve HDLC types, totaled separately by direction (from DTE and from DCE).
- The center zone shows the counters at the next protocol level, either X.25 or SNA. Because only data frames have SNA or X.25 content, the total number of frames in this panel may be lower than the total in the left panel.
- The right zone shows a table of logical calls, built in the order each call is detected within the traffic. Each call is identified by its call address (if known) and its logical call number (LCN), which is composed of a logical channel group number and the logical channel number. For calls that are not visible on the screen, you can use the Cursor keys or the function keys to scroll. The logical call table includes both calls that are still active and calls that have been completed. The counts for active calls are highlighted.

  A logical call's address is contained in the first frame. If a call was initiated before the Sniffer analyzer started to capture, its LCN is known, but the information is not in its address. Instead, this address is shown as a row of dashes, indicating an unknown address.

The column at the far right shows whether each call originated from DTE or from DCE. For each call, the analyzer tabulates traffic for that connection in each direction.

Active vs. Completed Calls

You can restrict the display to show only completed calls by pressing F2 (**Display active**). Pressing F2 again restores the display to all calls. Once a call has been completed, its logical call number can be reused. As a result, inactive calls can include multiple instances of the same LCN.

Naming Addresses

As with LANs, you can supply names for the source or destination of a logical call. The analyzer substitutes the name for the remote address (the source on a call from DCE, the destination on a call from DTE). Names for addresses are visible in the right panel. For information about how to add names to the name table, refer to "Managing Names" on page 5–3.

Function Keys Available in the Sniffer Internetwork Analyzer Tabular Views

F2 **Display active/Display all**. Toggles the display between showing all stations or active stations.

F4 **Clear screen**. Clears the screen and resets all counters to 0.

F7 **Scroll up**. Scrolls the list of logical calls toward the top of the list.

F8 **Scroll down**. Scrolls the list of logical calls toward the bottom of the list.

F9 **Pause.** Temporarily stops screen updates and displays a new set of function keys that allow you to access the Help system, change the screen format, or interpret captured frames.

While paused, the following function keys are available:

F1 **Help.** Displays the main Help menu.

F2 **Display active/Display all**. Toggles the display between showing all stations or active stations.

F3 **Data display.** Interprets the frames in the capture buffer and displays them in the default (or chosen) display format.

F4 **Clear screen**. Clears the screen and resets all counters to 0. (This has no effect on the frames in the capture buffer.)

F5 **Menus.** Displays the main menu.

F6 **Capture options.** Displays the options for choosing the screen format.

F7 **Scroll up**. Scrolls the list of logical calls toward the top of the list.

F8 **Scroll down**. Scrolls the list of logical calls toward the bottom of the list.

F9 **Resume.** Resumes the display of the tabular views. If you changed any options, the views change accordingly.

F10 **Stop capture**. Stops the capture and redisplays the main menu.

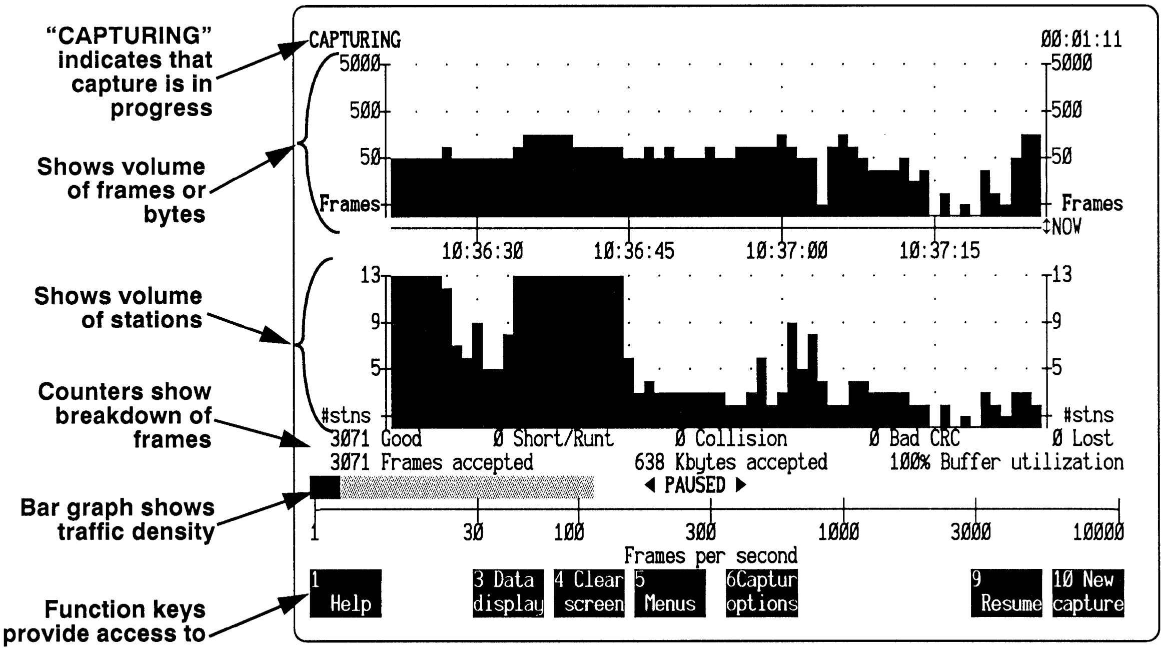
Information in the Skyline View

The skyline view (Figure 3–16) shows traffic density during capture. Each view consists of two histograms, one above the other, with a common horizontal time scale. The top histogram shows the number of frames (or bytes) and the bottom shows the number of stations detected. You can manipulate the scale of each histogram to adjust the level of detail to the network's volume.

Note: If you are using a larger screen, the skyline views automatically expand to take advantage of the additional space. As a result, up to five histograms may be displayed.

Counters

The counters in the skyline view are the same as those in the tabular views. As capture proceeds, they show the total number of frames (whether or not they passed the capture filters) and the total number of kilobytes they contained. On token ring and FDDI networks, these totals are reported directly as "frames seen" and "kilobytes seen."



"CAPTURING" indicates that capture is in progress

Shows volume of frames or bytes

Shows volume of stations

Counters show breakdown of frames

Bar graph shows traffic density

Function keys provide access to other functions

```
CAPTURING                                                00:01:11
3071 Good      0 Short/Runt      0 Collision      0 Bad CRC       0 Lost
3071 Frames accepted      638 Kbytes accepted      100% Buffer utilization
                          ◀ PAUSED ▶
```

Figure 3–16. Sample LAN skyline view.

On other networks, there is no single total for "frames seen," but separate counters for various subtotals. For example, on Ethernet, there are totals for the total numbers of good frames, short/runt frames, bad CRC frames, and lost frames. On networks with an Ethernet-II adapter card, there is also a counter for collision frames.

Buffer Utilization

During capture the Sniffer analyzer continuously updates a counter that shows the percentage of the capture buffer that has been filled.

Skyline Views for LAN Networks

On a LAN, the upper histogram shows either the number of frames or the number of kilobytes transmitted during the interval you specified, as shown in Figure 3–16. If you chose the **Show NW usage** option, the upper histogram shows the number of kilobytes and the bar graph shows the percentile of network usage. The lower histogram shows the number of stations active during the interval.

These histograms are updated with a new column at the right at the specified interval (1 second, 1 minute, or 1 hour). The Skyline view also provides a running count of total frames, but no itemization of traffic by individual stations.

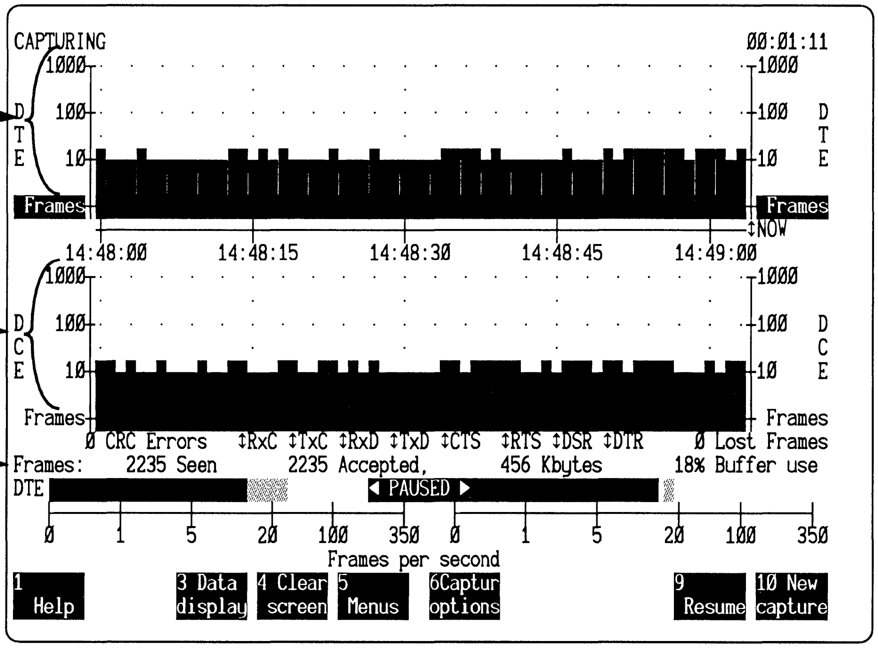
Skyline Views for WAN/Synchronous Networks

On a WAN/Synchronous link (Figure 3–17), the upper histogram shows traffic from DTE, while the lower histogram shows traffic from DCE. Beneath the histograms are the counters that show the total number of frames (whether or not they passed the capture filters) and the total number of kilobytes they contained. In addition, there is a one-line summary that shows the status of the line, using the RS232 indicators RxC, TxC, RxD, TxD, CTS, DSR, and DTR. The condition of each indicator is shown with an up arrow (for a logical 1), a down arrow (for a logical 0), and ↕, which means the indicator's status changed in the last second.

Shows volume of DTE frames

Shows volume of DCE frames

Counters show frames and errors



```
     Ø CRC Errors   ↕RxC ↕TxC ↕RxD ↕TxD ↕CTS  ↕RTS ↕DSR ↕DTR    Ø Lost Frames
Frames:   2235 Seen      2235 Accepted,     456 Kbytes        18% Buffer use
```

Figure 3–17. Sample WAN/Synchronous skyline view.

Depending on traffic volume, you may want to manipulate the vertical scales of the two histograms to show the optimal level of detail. You can also manipulate the horizontal scale to show earlier intervals that are no longer in the view, as though backspacing through the display. You can adjust each histogram independently of the other.

To adjust the vertical scales to the best level of detail:

1. Press F2 (**Select display**) or the Tab key to select the histogram you want to scale.
2. To decrease the scale (larger bars related to a smaller range), press F6 (**Scale down).**
3. To increase the scale (shorter bars related to a larger range), press F5 (**Scale up**).

To adjust the horizontal scales to view earlier intervals:

1. Press F2 (**Select display**) or the Tab key to select the histogram you want to scale.
2. To view intervals that occurred earlier during the capture, press F7 (**View earlier**) repeatedly until you reach the desired interval.
3. After viewing earlier intervals, press F8 (**View later**) repeatedly until you reach any interval up to the current interval.

Function Keys Available in Skyline View

F2 **Select display** (or the **Tab key).** Toggles between the two histograms.

F4 **Clear screen.** Clears the screen and resets all counters.

F5 **Scale up.** Increases the current histogram's scale to show a larger number of stations or frames. As the scale increases, the bars become shorter.

F6 **Scale down.** Decreases the current histogram's scale to show a smaller number of stations or frames. As the scale decreases, the bars become taller.

F7 **View earlier.** Allows you to view the number of stations, bytes, or frames at earlier intervals.

F8 **View later.** If you used function key F7 to view earlier intervals, this key returns you to later intervals, up to the current interval.

F9 **Pause.** Temporarily stops screen updates and displays a new set of function keys that allow you to access the Help system, change the screen format, or interpret captured frames.

While paused, the following function keys are available:

F1 **Help.** Displays the main Help menu.

F3 **Data display.** Interprets the frames in the capture buffer and displays them in the default (or chosen) display format.

F4 **Clear screen**. Clears the screen and resets all counters to 0.

F5 **Menus.** Stops capture and displays the main menu.

F6 **Capture options.** Displays the options for choosing the screen format.

F9 **Resume.** Resumes the skyline display. If you changed any options, the display changes accordingly.

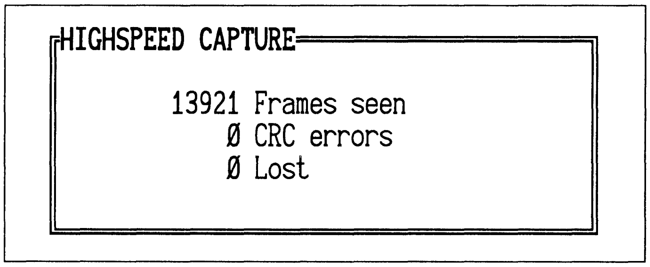
F10 **Stop capture**. Stops the capture and redisplays the main menu.

Choosing Highspeed Capture Mode

When capturing "live" from Ethernet or PC Network, choosing **Highspeed mode** speeds up processing. During sustained high-speed traffic under certain conditions, the analyzer might not be able to capture every frame while simultaneously displaying it. Because the adapter card provides programmable access to the local buffer, you can store frames in the adapter card's temporary buffers instead of in the area of main storage dedicated to the Sniffer analyzer's capture buffer. Because the analyzer only counts frames instead of processing them, this speeds up the capture considerably.

Although the chosen screen format appears on the screen, it is not updated. Instead, a rectangle that shows the highspeed counts is superimposed on the center of the screen. As capture proceeds, only the central rectangle is updated, as shown in Figure 3–18. Note that the capture filters and the trigger options disappear from the menu when you choose **Highspeed mode**.

Note: If you are not using the Ethernet-II adapter card, storage is limited to the adapter card's buffer memory.



```
HIGHSPEED CAPTURE

        13921 Frames seen
            Ø CRC errors
            Ø Lost
```

Figure 3–18. Information displayed during capture in Highspeed mode.

If you are using an Ethernet-II adapter card, frames are transferred directly to the capture buffer as they are captured. Otherwise, pressing F10 (**Stop capture**) or F9 (**Pause**) transfers the accumulated frames in the adapter card's buffer to the Sniffer analyzer's capture buffer and displays the accumulated statistics.

To select Highspeed mode:

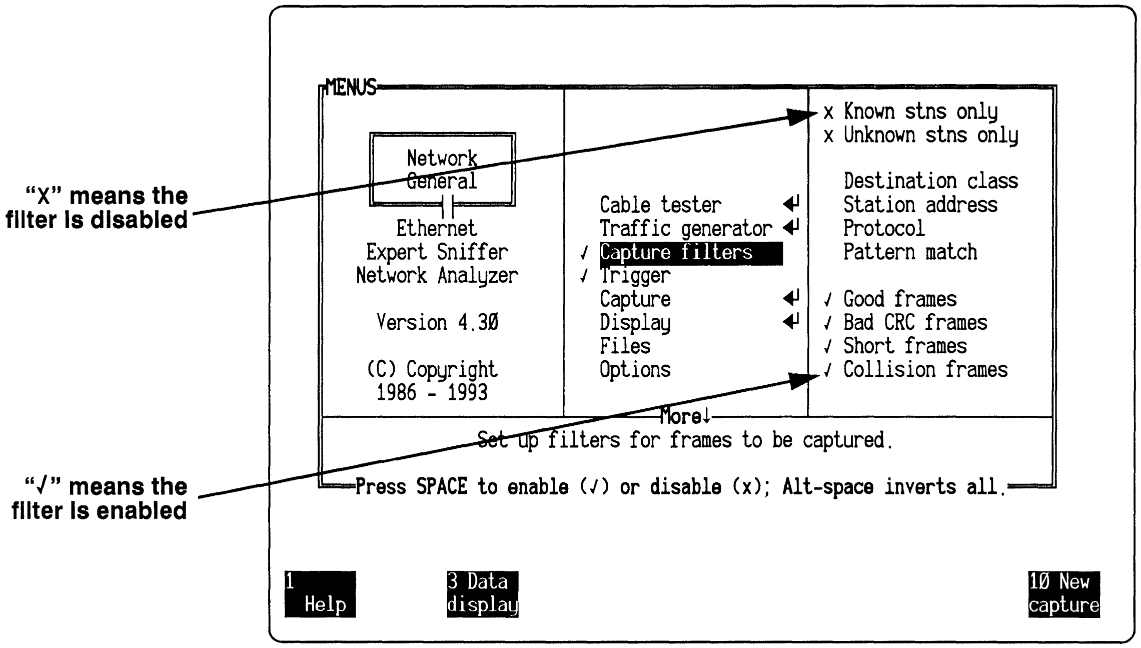
1. Move to **Capture\Highspeed mode** and press Spacebar.

   Note that the **Capture filters** and **Trigger** options disappear from the menu. When you return to **Classic** mode, these options reappear, with the settings (enabled or disabled) intact.

Setting the Capture Filters

To limit the number of captured frames to those of interest, you can define filters that eliminate other frames, such as particular low-level DLC addresses or unknown stations. As a result, only those frames that pass the filters are captured. Which filters are available depends on your network.

Figure 3–19 shows the capture filters available for Sniffer analyzers with an Ethernet-II adapter card. The options associated with some of these filters will appear on the right when you move to a particular filter.



"X" means the filter is disabled

"√" means the filter is enabled

```
MENUS
                                                  x Known stns only
                                                  x Unknown stns only
     Network
     General                                        Destination class
                        Cable tester         ↵      Station address
     Ethernet           Traffic generator    ↵      Protocol
  Expert Sniffer      √ Capture filters             Pattern match
 Network Analyzer     √ Trigger
                        Capture              ↵    √ Good frames
   Version 4.30         Display              ↵    √ Bad CRC frames
                        Files                     √ Short frames
  (C) Copyright         Options                   √ Collision frames
   1986 - 1993
                               More↓
                 Set up filters for frames to be captured.
Press SPACE to enable (√) or disable (x); Alt-space inverts all.

1       3 Data                                            10 New
 Help   display                                           capture
```

Figure 3–19. Setting the Ethernet capture filters.

Figure 3–20 summarizes the available LAN capture filters by network.

LAN	Filter	Test	Default
All	Known stations only	Does a stations's DLC address have a corresponding symbolic name in the name table?	x don't accept
All	Unknown stations only	Does a station's DLC address *not* have a corresponding name in the name table?	x don't accept
All	Destination class	Does the frame have a specific destination or is it a broadcast/multicast?	accept both
All	Station address	Does the frame match any of the user-specified source-and-destination pairs?	accept any
All	Protocol	Does the frame contain any of the low-level protocols disabled by the user?	accept any
All	Pattern match	Does the frame match up to four user-specified patterns?	accept any
FD	Void/Claim frames	Is the frame a void or claim frame (for live capture only)?	x don't accept
FD	Error frames	Is the frame an error frame (for live capture only)?	x don't accept
EN*	Good frames	Does the frame contain frames without defects?	√ accept
EN*	Bad CRC frames	Does the frame include a C flag?	√ accept
EN*	Short frames	Is the frame less than 60 bytes long (runt)?	√ accept
EN-II	Collision frames	Does the frame include a collision?	√ accept

*Also for StarLAN and PC Network

Figure 3–20. Overview of available LAN capture filters.

Figure 3–21 summarizes the available WAN/Synchronous capture filters.

WAN	Filter	Test	Default
	Pattern match	Does the frame match up to four user-specified patterns?	accept any
	From DTE	Does the frame include frames sent by the DTE?	accept any
	From DCE	Does the frame include frames sent by the DCE?	accept any
	RR frames	Does the frame include the RR (Receiver Ready) code?	accept any
	RNR frames	Does the frame include the RNR (Receiver not Ready) code?	accept any
	Info frames	Is the frame an SDLC/HDLC info frame?	accept any
	Good frames	Capture frames with good CRC?	accept any
	Bad CRC frames	Capture frames with bad CRC?	accept any

Figure 3–21. Overview of available Sniffer Internetwork Analyzer capture filters.

Using capture filters requires a certain amount of processing time. As a result, the more complex the capture filter, the more time is required. On networks with a light or moderate load, this processing time is not noticeable. On heavily loaded networks, however, complex capture filters limit the speed at which the Sniffer analyzer can accept frames, unless the filters significantly reduce the number of frames accepted. As a result, some frames may be lost. If this happens, the number of lost frames is recorded in the *lost frames* counter. If the number of lost frames increases, try using simpler capture filters or (on Ethernet and PC Network) capture in **Highspeed mode**.

To set up the capture filters:

1. Move to **Capture filters**. If necessary, press Spacebar to enable (√) the option.
2. Move to the desired filters and press Spacebar to enable (√) or disable (x) those filters.
3. For filters with associated options, define those options.

Saving Selected Capture Filters

The capture filters you select remain in effect only until you exit the analyzer or reboot the computer. When shipped, the **Capture filters** option is enabled. To use the settings you defined instead of the system defaults, you can save them to a setup file and then load that file after you start the analyzer. You can also save them to the STARTUP.*xx*S file to be applied automatically.

Note: Saving a setup saves *all* options as you define them, not just the capture filters.

To save the capture filters setup:

1. Move to **Files\ Save\Setups** and press Enter.
2. In the dialog box that appears, enter the desired filename, without an extension.

Disabling the Capture Filters

If you observe a high number of lost frames, you may want to disable the capture filters or reduce their complexity. You may also find that the frames that interest you are not captured and suspect that a capture filter is eliminating those frames. By disabling the capture filters, you can determine whether the capture filters are responsible.

You can always disable filters individually or press Alt-Spacebar to reverse all settings. There are also two general ways to disable any capture filters you may have enabled:

- Disable the **Capture filters** option.
- Use the **Use defaults** option.

By disabling the **Capture filters** option, you *temporarily* disable all capture filters. This allows you to see how capture proceeds with the filters disabled, without having to disable individual filters you may have spent considerable time setting up. After examining the results, you can fine-tune your capture filters.

To temporarily disable all selected capture filters:

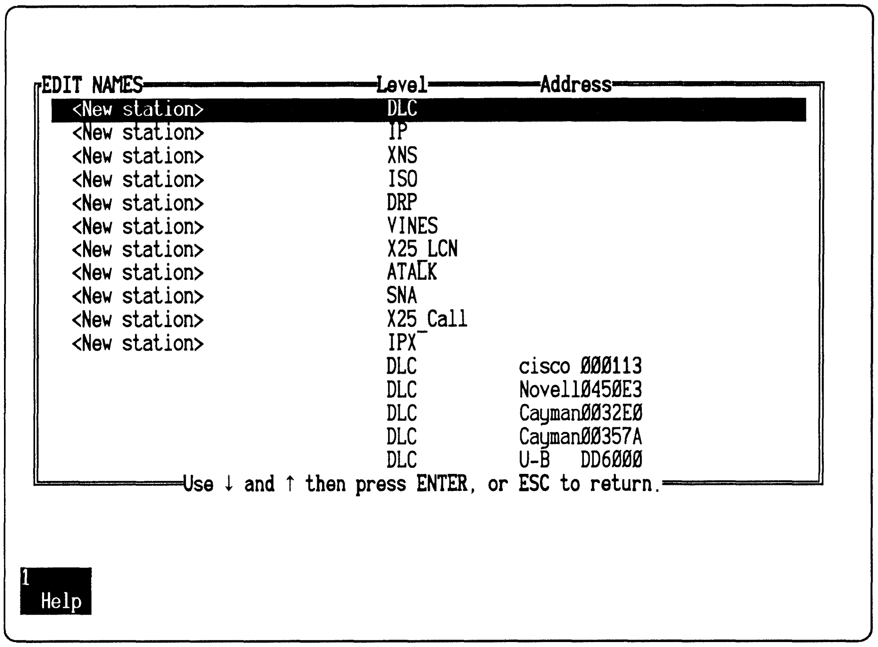
1. Move to **Capture filters** and press Spacebar to disable (x) the option.

If you choose the **Use defaults** option, all enabled capture filters *and* all other options are reset to the default settings (shown in Appendix A). Because you may have spent considerable time defining various options, *do not* use the **Use defaults** option unless you want to return to the system defaults. This command is described in more detail in "Setting the Cable Test Option for Ethernet" on page 2–8.

Capture Filters and the Name Table

Several capture filters—**Known stations only**, **Unknown stations only**, and **Destination class**—use information contained in the name table. To use these filters efficiently, you must maintain this table.

The permanent name table is contained in the file STARTUP.*xx*D, which is read at system startup. This table includes any addresses that were previously detected and then named. In addition to this permanent name table, the Sniffer analyzer creates a current name table for each new capture by scanning the capture buffer for addresses that are not in the name table. If such addresses are found, the analyzer inserts them at the top of the name table. The working name table thus includes all the information in the permanent name table, as well as newly detected addresses (Figure 3–22).



```
EDIT NAMES                          Level          Address
  <New station>                     DLC
  <New station>                     IP
  <New station>                     XNS
  <New station>                     ISO
  <New station>                     DRP
  <New station>                     VINES
  <New station>                     X25_LCN
  <New station>                     ATALK
  <New station>                     SNA
  <New station>                     X25_Call
  <New station>                     IPX
                                    DLC         cisco 000113
                                    DLC         Novell0450E3
                                    DLC         Cayman0032E0
                                    DLC         Cayman00357A
                                    DLC         U-B   DD6000
              Use ↓ and ↑ then press ENTER, or ESC to return.

1
 Help
```

Figure 3–22. The working name table.

Until you name the newly detected addresses, the Sniffer analyzer considers them "unknown." If the **Look for names** option is enabled (**Display\Manage names\Look for names**), the analyzer automatically updates the working name table with any detected addresses. Any unnamed addresses are deleted from the name table when you exit the Sniffer analyzer application. For additional information about working with the name table, refer to "Managing Names" on page 5–3.

Known Stations Only Filter

When you enable **Known stns only**, the analyzer captures only those frames that contain a "known," or named, DLC address (source or destination). To effectively use this filter, you must update your name table to name any detected addresses.

The default is x **Known stns only** disabled.

To restrict capture to frames from known stations:

1. Move to **Capture filters\Known stns only**, and press Spacebar to enable the option (✓).

Unknown Stations Only Filter (LAN)

When you enable **Unknown stns only**, the Sniffer analyzer captures only those frames that contain an "unknown" DLC address (source or destination). The analyzer considers an address to be unknown either when its address isn't in the current name table or when the address is not named.

The cause of such traffic could be illegal hackers, bad data frames, faulty software in the application or on the network, or adapter cards that were replaced without notifying the system manager.

The default is x **Unknown stns only** disabled.

To restrict capture to frames from unknown stations:

1. Move to **Capture filters\Unknown stns only**, and press Spacebar to enable the option (✓).

Destination Class Filter

On a LAN, you can specify whether to capture frames from a specific address, from a generic address, or from both. When you enable the **Broadcast** option, only frames transmitted to the generic address that includes several—or perhaps all—stations will be captured. When you enable only the **Specific** option, only frames transmitted to a specific address will be captured. Because there are no such transmissions over wide area networks, there is no **Destination class** filter for WAN/Synchronous links.

In the name table, you can assign a name to a generic address, such as "Error Monitor" or "LAN Manager." Of course, a generic address can only be the destination, not the source, of a frame. Each type of network has prescribed formats for generic addresses, which are different from any possible individual addresses.

Formats of generic addresses are summarized in Figure 3–23.

Originating Network	Type	Description	Characteristic Address
Ethernet StarLAN PC Network	Multicast address (including Broadcast	A multicast address is a collective name for several stations. It may be a role played by one or more stations, or by all stations (for example, "Broadcast").	A DLC multicast address has a 1 in the low-order bit of the first byte, so that in hexadecimal its second character is odd (that is, 1, 3, 5, 7, 9, B, D, or F). No individual station has an address with that bit on.
Token Ring, FDDI	Functional address (including Broadcast)	A functional address is a collective name for a role played by one or more stations, (e.g. "Error monitor") or by all stations (e.g. "Broadcast").	A DLC functional address has a 1 in the high-order bit, so that in hexadecimal it appears as a number whose first digit is 8 or higher. No individual station has an address with that bit on.

Figure 3–23. Formats of generic addresses, by network of origin.

To select or exclude frames by destination class:

1. Note the meaning of broadcast or multicast address on your network.
2. Move to **Capture filters\Destination class** and press Spacebar to enable (√) or disable (x) the **Broadcast** and/or **Specific** options.

Station Address Filters

During capture, you can filter only for lower-level addresses. For these addresses, you can enable up to four different DLC address matches, where each match consists of the following information:

- The source and destination addresses
- Whether to include traffic that travels in both directions between those addresses
- Whether the filter includes or excludes this match

To make it easy to describe these matches, you can also assign a name to each match.

On a LAN, you can set filters for a frame's DLC destination. However, the DLC destination may describe only the current leg of a much longer journey. Because higher-level protocols embedded in the frame's data field have their own addresses, they may cause the recipient of the current frame to repack the data and retransmit it with a new address.

Note: Most topologies use six-byte addresses. ARCNET and LocalTalk, however, use one-byte addresses. On ARCNET, you can also enter addresses in octal rather than hexadecimal format or display DLC addresses in the octal format.

Defining Station Address Matches: Some Considerations

By defining station address matches, you can exercise considerable control over which frames are captured. The Sniffer analyzer evaluates the matches, starting with Match 1 (or the name you assign to Match 1) through Match 4. When a match succeeds, the analyzer stops testing for further matches. Whether or not the successful match is captured depends on whether you chose the **Include these** or **Exclude these** option associated with that match.

When none of the specified matches succeeds, the **Others** menu item determines whether the frames are captured anyway. **Include these** means the frames are captured; **Exclude these** means that they are not captured.

Using Fewer than Four Address Matches

It is not necessary to set all four matches; in fact, you may not want to set any at all. The analyzer disregards a match that contains only the default settings **From <any station>** and **To <any station>**. When all four matches are **From <any station> To <any station>**, the analyzer uses no address filters during capture.

Disabling Defined Address Matches

You can temporarily turn off the filter specified by a defined match by pressing Spacebar to disable (x) that match. The Sniffer analyzer checks only enabled matches marked with √.

Examples: Taking Advantage of Address Match Order

Suppose you are interested in all traffic to and from Server-1 except for the voluminous traffic between Server-1 and Gateway-A, which would quickly fill the capture buffer. Since the address filters are evaluated in sequence, you can define filters that first discard frames between Server-1 and Gateway-A and then accept frames between Server-1 and any other destination. The two sets of matches that would accomplish this are summarized in Figure 3–24.

	Match Name	Source Address	Destination Address	Reverse Direction	Include/ Exclude
Match 1	S1 to A	Server-1	Gateway A	yes	exclude
Match 2	S1 to others	Server-1	<any>	yes	include
Match 3	[Match 3]	<any>	<any>	[yes]	[include]
Match 4	[Match 4]	<any>	<any>	[yes]	[include]
Others					exclude

Figure 3–24. Address filter to capture all traffic—with one exception—from a station.

Another example shows traffic between stations George or Anita and Server-1, as well as any traffic to Gateway-A (but not the reverse). To capture these frames, you could specify three matches as shown in Figure 3–24.

	Match Name	Source Address	Destination Address	Reverse Direction	Include/ Exclude
Match 1	G's files	George	Server-1	yes	include
Match 2	A's files	Anita	Server 1	yes	include
Match 3	Outgoing	<any>	Gateway A	no	include
Match 4	[Match 4]	<any>	<any>	[yes]	[include]
Others					exclude

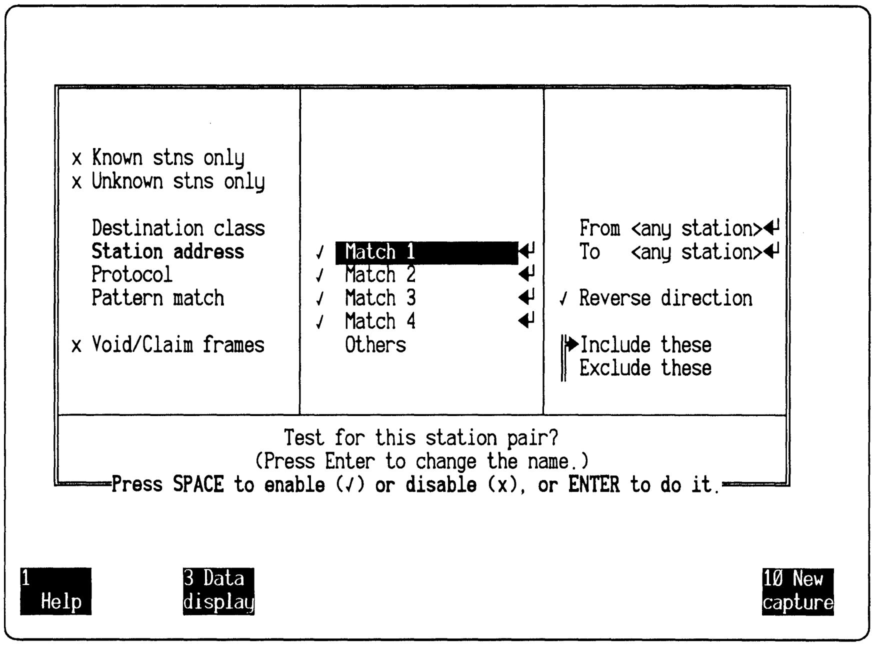
Figure 3–25. Example of a filter match on three address pairs.

Defining the Station Address Filters

After you determine what matches are required to capture the desired frames, you can define and name the matches that make up the station address filters.

To define station address capture filters:

1. Move to **Capture filters\Station address\Match 1** (Figure 3–26).



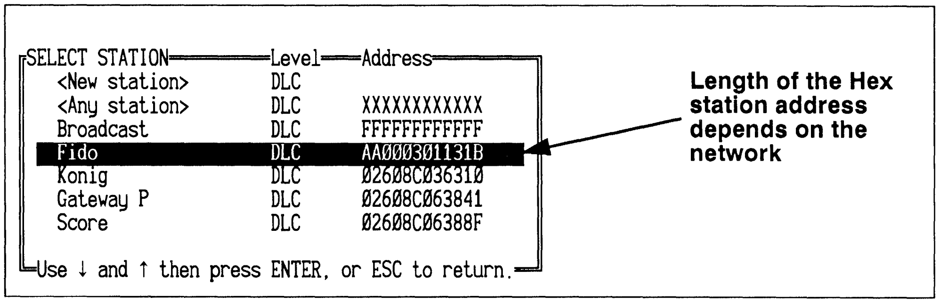
```
x Known stns only
x Unknown stns only

  Destination class                        From <any station>↵
  Station address      √ Match 1       ↵   To   <any station>↵
  Protocol             √ Match 2       ↵
  Pattern match        √ Match 3       ↵ √ Reverse direction
                       √ Match 4       ↵
x Void/Claim frames      Others            ▶Include these
                                            Exclude these

                   Test for this station pair?
                 (Press Enter to change the name.)
   Press SPACE to enable (√) or disable (x), or ENTER to do it.

1           3 Data                                        1Ø New
 Help       display                                       capture
```

Figure 3–26. Defining a station address capture filter.

2. If you want to name this match, press Enter. In the dialog box that appears, type a name and press Enter.

3. To specify a source address, move to **From** and press Enter.

   In the table that appears (Figure 3–27), move to the desired station and press Enter. If you enabled the **DLC addresses** option in the **Display\Summary** menu, the DLC address is automatically highlighted. If that option is disabled (the default) the highest level address is highlighted.



```
SELECT STATION          Level   Address
   <New station>        DLC
   <Any station>        DLC     XXXXXXXXXXXX
   Broadcast            DLC     FFFFFFFFFFFF
   Fido                 DLC     AAØØØ3Ø1131B
   Konig                DLC     Ø26Ø8CØ3631Ø
   Gateway P            DLC     Ø26Ø8CØ63841
   Score                DLC     Ø26Ø8CØ6388F

Use ↓ and ↑ then press ENTER, or ESC to return.
```

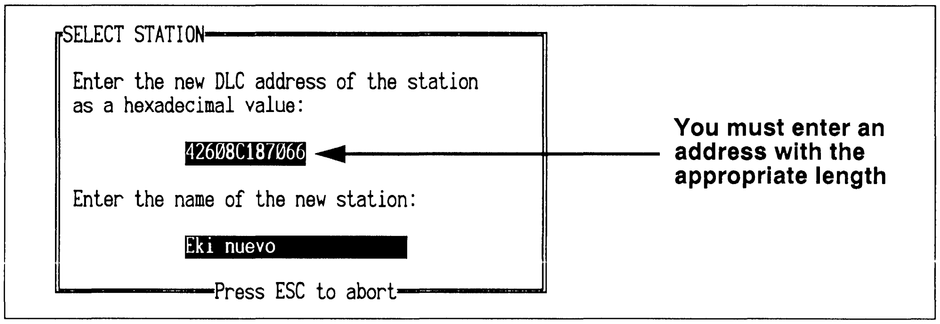
Length of the Hex station address depends on the network

Figure 3–27. Selecting a station for a station address filter.

   Note that the address—either its name, if it has one, or the DLC address—replaces **<any station>** in the **From** menu item.

4. If the address you want is not in the table, move to **<New station>** at the top of the table and press Enter.

In the dialog box that appears (Figure 3–28), type a new DLC address and a corresponding symbolic name and press Enter.



```
SELECT STATION

Enter the new DLC address of the station
as a hexadecimal value:

        42608C187066

Enter the name of the new station:

        Eki nuevo

               Press ESC to abort
```

You must enter an address with the appropriate length

Figure 3–28. Entering a new station address and name.

5. To specify a destination address, move to **To** and press Enter. Repeat the instructions in step 3 for selecting an address.

   As with the source address, the DLC address is automatically highlighted if you enabled the **DLC addresses** option in the **Display/Summary** menu. If that option is disabled (the default) the highest level address is highlighted. For ARCNET, you can enter the information as an octal value.

6. To specify whether this match also applies to traffic in the reverse direction, move to **Reverse direction** and press Spacebar to enable (√) or disable (x) the option.

7. To specify whether to include or exclude frames identified by this match, move to the appropriate option and press Spacebar to select the option you want.

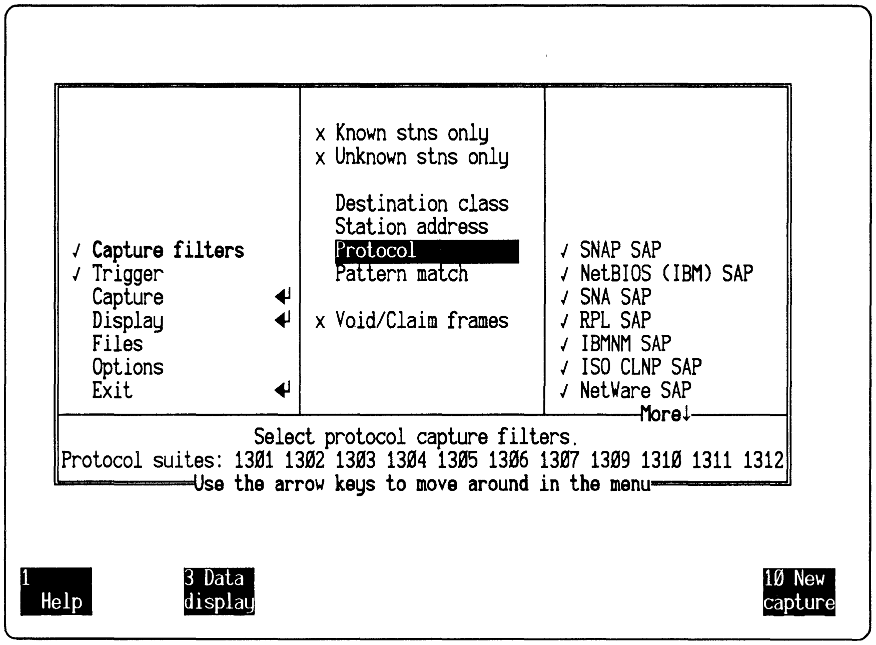
   ▶ Include these
   Exclude these

8. Repeat steps 1 through 7 for up to four matches.

Protocol Filter

On a LAN, each DLC frame includes a field that indicates the frame type. Depending on the network, this low-level classification is called a *SAP* ("service access point" per IEEE 802.2) or an *Ethertype* (for Ethernet and StarLAN). This is the lowest level at which protocols are identified, which is also the only level available for capture filters. (Because the analyzer can devote more time to processing filters during the Display process, the display filters can include tests for higher-level protocols or addresses.)

Figure 3–29 shows some of the protocols available for capture filters. Next to each protocol, a √ indicates that the capture filter accepts that protocol, and an "x" that it does not. The filter accepts a frame if it contains *any* of the protocols marked with a √. The default is all protocols enabled.



```
                       x Known stns only
                       x Unknown stns only

                         Destination class
                         Station address
√ Capture filters        Protocol               √ SNAP SAP
√ Trigger                Pattern match          √ NetBIOS (IBM) SAP
  Capture        ↵                              √ SNA SAP
  Display        ↵     x Void/Claim frames      √ RPL SAP
  Files                                         √ IBMNM SAP
  Options                                       √ ISO CLNP SAP
  Exit           ↵                              √ NetWare SAP
                                                          More↓
              Select protocol capture filters.
Protocol suites: 1301 1302 1303 1304 1305 1306 1307 1309 1310 1311 1312
           Use the arrow keys to move around in the menu

1 Help       3 Data display                          10 New capture
```

Figure 3–29. Defining the protocol capture filters.

Note: Specific protocols available for capture filters on your Sniffer analyzer are listed in the **Capture filters** menu. Some typical protocol lists are shown in Figure 3–30.

Token Ring with IBM, XNS/MSNET, ISO, X.25	**Ethernet with TCP/IP, Sun, DECnet, Banyan, AppleTalk, X-Windows**	**Ethernet with IBM, Novell, XNS/MSNET, ISO, X.25**	**FDDI**
√ MAC frames	√ LOOP Etype	√ LOOP Etype	√ Void/Claim frames
√ SNAP SAP	√ 3Com Netmap Etype	√ 3Com Netmap Etype	√ Other MAC frames
√ BPDU SAP	√ IP Etype	√ IBMRT Etype	√ SMT frames
√ NetBIOS (IBM) SAP	√ ARP Etype	√ NetWare Etype	√ SNAP SAP
√ SNA SAP	√ TRLR Etype	√ XNS Etype	√ NetBIOS (IBM) SAP
√ RPL SAP	√ PUP Etype	√ PUP Etype	√ SNA SAP
√ U-B SAP	√ PUP ARP Etype	√ 3Com NBP Etype	√ RPL SAP
√ IBMNM SAP	√ SNMP Etype	√ PUP ARP Etype	√ IBMNM SAP
√ NetWare SAP	√ MOP Etype	√ Other Etype	√ ISO CLNP SAP
√ ISO CLNP SAP	√ DRP Etype	√ SNAP SAP	√ NetWare SAP
√ XNS SAP	√ LAT Etype	√ BPDU SAP	√ XNS SAP
√ X.25 SAP	√ IP (VINES) Etype	√ Net BIOS (IBM) SAP	√ IP SAP
√ Other SAP	√ LOOP (VINES) Etype	√ SNA SAP	√ LLC (VINES) SAP
	√ Echo (VINES) Etype	√ RLP SAP	√ X.25 SAP
	√ ARP (Atalk) Etype	√ IBMNM SAP	√ Other SAP
	√ LAP (Atalk) Etype	√ ISO/NetWare SAP	
	√ Other Etype	√ X.25 SAP	
	√ SNAP SAP	√ Other SAP	
	√ BPDU SAP		
	√ LLC (VINES) SAP		
	√ Other SAP		

Figure 3–30. DLC protocols typically available for capture filters.

For most networks, the Sniffer analyzer's default setting is to accept every protocol.

To choose the protocols accepted during capture:

1. Move to **Capture filters\Protocol**.
2. Move to the protocols you want to disable. Press Spacebar to disable (x) and enable (√) the filter for a protocol.
3. If the protocol you want is not in the list, move to the last entry (**Other SAP**) and make sure that the option is enabled.

To reverse the settings for all protocols:

1. Press Alt-Spacebar.

Pattern Match Filter

A match consists of a pattern and the related offset. The pattern is a particular sequence of bits within a frame. The offset is the position of the bits within the data field of the frame. In a simple pattern, the bits occur at just one location. In a complex pattern, a set of up to eight simple component patterns is linked by AND / OR logic. The effect of NOT is achieved by choosing between **Match** and **Don't match**. The resulting set of patterns functions as a filter during capture.

Four Contexts for Pattern Matching

Setting up pattern matches as capture filters is only one of four contexts in which you specify a pattern as criteria for a function. The procedure for setting up these patterns is identical in all four contexts. However, a pattern established within one context has no effect on any other patterns.

The four contexts for pattern matching are:

Capture filter — The pattern that restricts which frames are accepted into the capture buffer during capture.

Trigger — The pattern that contains the "trigger" pattern, which stops the capture when it is detected.

Display filter — The pattern that restricts which frames in the capture buffer are displayed by the Display function.

Search — The pattern that specifies the search criteria for finding frames during display.

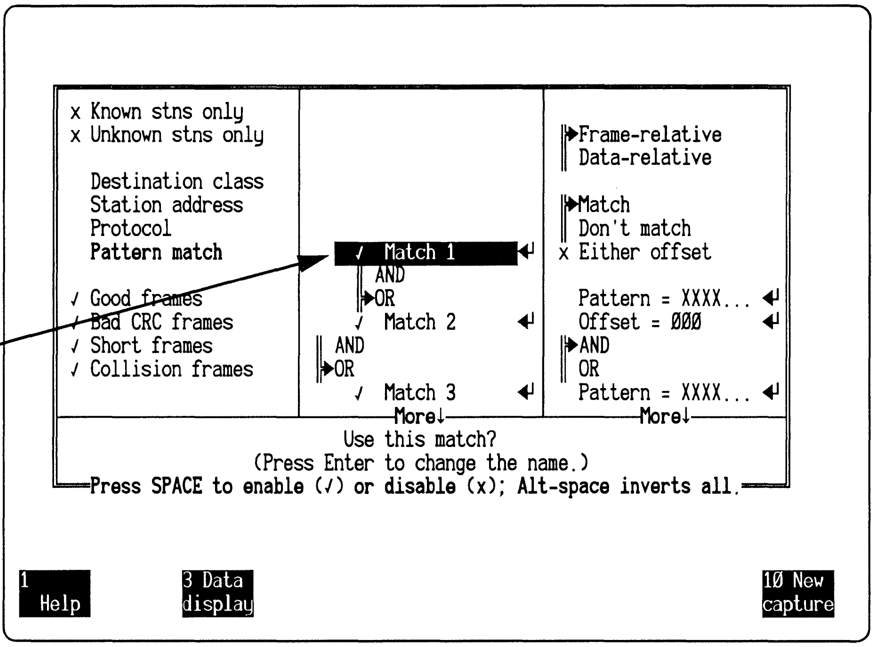
Because the Sniffer analyzer does not have time to invoke its interpreters for high-level protocols during capture, the analyzer cannot filter on high-level protocols or high-level addresses. However, it can execute fairly complex pattern matching. By experimenting with captured frames, you can often set up a pattern that, in effect, responds to a high-level embedded protocol.

Defining Complex Pattern Matches

By combining the four matches, you can define a complex pattern. The panel to the right of the **Pattern match** option contains the logical rules for combining the four component patterns into a set, as shown in Figure 3–31.

To help identify the four component patterns, you can assign each a name, which replaces the default names Match 1, Match 2, etc. Note that these names don't affect processing; they simply identify each component pattern. To assign a name, move to Match 1 (or any other match), press Enter, and type the name into the dialog box that appears.

You can name each match to identify it. You can also temporarily disable a match without changing its specifications



Use this match?
(Press Enter to change the name.)
Press SPACE to enable (✓) or disable (x); Alt-space inverts all.

Figure 3–31. Defining a pattern match.

Logical Combinations of the Four Matches

The four matches are combined by a logical AND or OR operator. The default is OR.

Matches are grouped into two sets of two, as shown in Figure 3–32. The analyzer first evaluates the relationship between Match 1 and Match 2, then between Match 3 and Match 4, and finally between the two pairs. Algebraically (with the symbol ⊗ standing for whichever relationship you set, either AND or OR), the relationship is summarized in this way:

$(\textit{Match 1} \otimes \textit{Match 2}) \otimes (\textit{Match 3} \otimes \textit{Match 4})$

The menu conveys this scheme by its pattern of indents.

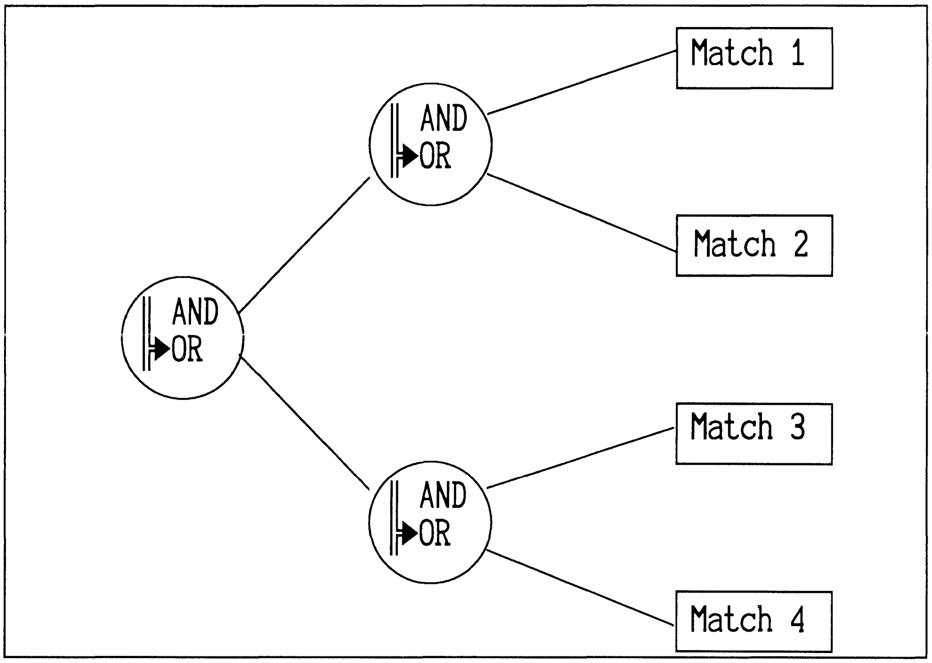


Figure 3–32. Combining four matches with AND and OR.

Pairs of Patterns within a Match

Each individual match is composed of a pair of patterns that is linked by AND or OR logical operators. When you highlight a match name, the panel to the right shows its pair of component patterns. Initially, the default for all the individual patterns is X (null) and all the offsets are 00.

A pattern that consists of X characters has no effect. Therefore, you should set up only those patterns and matches you need. If you set up some matches but not others, it doesn't matter which matches you define and which you leave at the default settings.

Temporarily Disabling a Match

By default, all matches are enabled, with nulls in the pattern fields. By moving to a match and pressing Spacebar, you can temporarily disable (x) that match without deleting the defined pattern.

A Match on a Pair of Patterns

A single match can involve a pair of patterns (you may prefer to think of this as a pattern in two parts). In the menu, the two patterns appear one above the other, each with its offset. You don't have to fill in both parts; any part you leave unspecified has no effect.

If you specify two patterns, you must also state the relationship between them: AND or OR. The default is OR. That is, to satisfy the match, the frame must contain *one* of the patterns.

For each pattern, you specify its location in the frame, which is called the "offset." Think of patterns as pattern A at offset *a*, and pattern B at offset *b*, resulting in the following match.

Pattern A at offset *a* AND Pattern B at offset *b*

Since these two patterns are in the same frame, a frame that meets this condition looks like Figure 3–33.

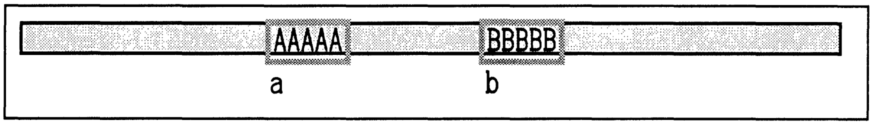


Figure 3–33. Frame containing both A at a *AND B at* b.

When the relationship is OR rather than AND, either or both frames are acceptable, as shown in Figure 3–34.

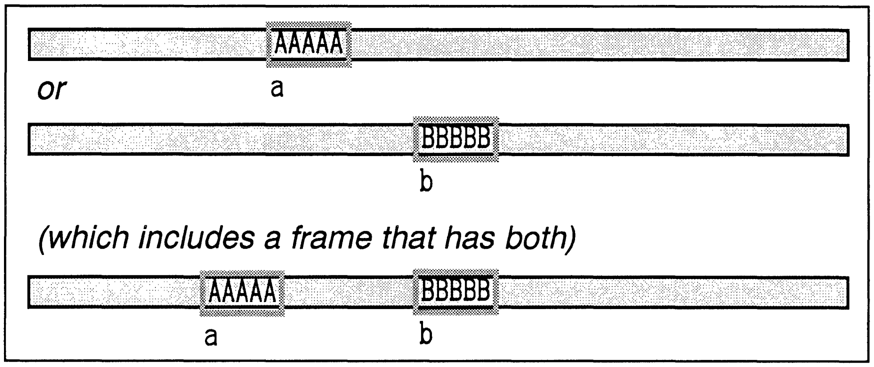


Figure 3–34. Frames containing either A at offset a OR B at offset b.

Effect of the Either Offset Option

When you specify a pair of patterns, you can also enable the **Either offset** option. This usually makes sense only when the two patterns are related by AND. Figure 3–35 illustrates this concept.

For example, an exchange between a client and a server over TCP might involve the "well known port" number of the server and a transient port number assigned to the client. In the exchange, the port numbers occur at two different positions, corresponding to *source port* and to *destination port*. If the **Either offset** option is enabled for the patterns related by AND, frames that pass between these ports, in either direction, will be captured.

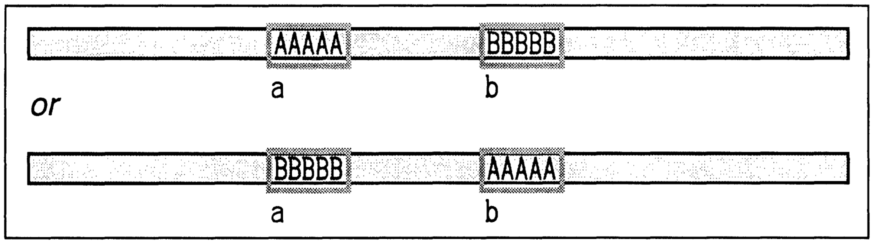


Figure 3–35. Effect of "Either offset" option when pairs are linked by AND.

In the unusual case that OR *and* the **Either offset** options are enabled, any of the four frames shown in Figure 3–36 is a match. The filter specified by this combination would accept all traffic to and from port A, as well as all traffic to and from port B. That would include traffic between ports A and B, as well as all traffic with any other ports.

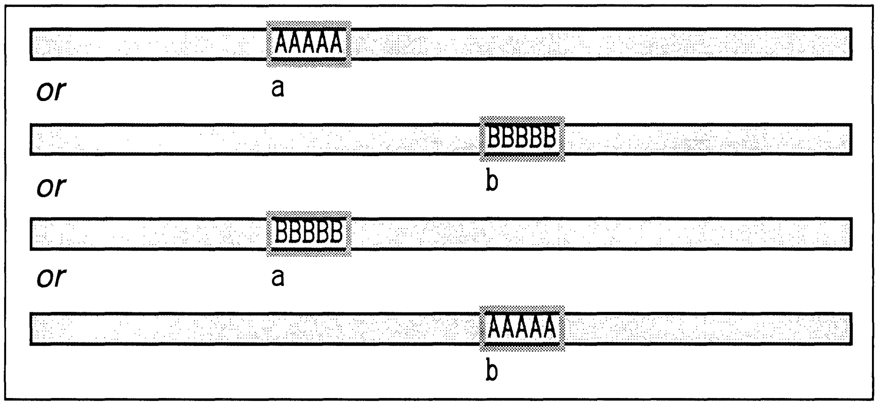


Figure 3–36. Effect of "Either offset" when pairs are linked by OR.

Effect of the Match/Don't Match Option

For each of the four matches, you can choose between the **Match** or **Don't match** options.

This setting reverses the evaluation of each pattern within a match. The **Don't match** option is evaluated *before* the **Either offset** option and *before* the AND / OR logic that combines the pair. To see the effect of **Don't match**, replace "AAAAA" by "Anything other than AAAAA" and replace "BBBBB" by "Anything other than BBBBB."

Whether the frame is accepted depends on the logic specified for combining the results of the four matches.

Examples

Suppose you describe a match as "pattern A at offset a." If you then enable **Don't match**, a frame should be accepted if, at offset a, it contains something *other than* pattern A.

When a match contains a pair of patterns linked by AND (for example, "Pattern A at offset a" *and also* "Pattern B at offset b"), enabling **Don't match** means that a frame should be accepted if it contains something *other than* pattern A at offset a *and* something *other than* pattern B at offset b.

When you specify a pair of patterns linked by OR (for example, "Pattern A at offset a" *or* "Pattern B at offset b"), enabling **Don't match** means that a frame should be accepted if it contains something *other than* "Pattern A at offset a" *or* something *other than* "Pattern B at offset b."

Characters and Offset in an Individual Pattern

Each individual pattern is defined by its position (offset) and the characters (or bits) it contains. A pattern may contain up to 32 characters.

Before you specify the pattern's content, first decide whether to enter it in hexadecimal, character, or binary format. The default is hexadecimal format.

Hexadecimal — Specify up to 16 bytes, each as a pair of hex digits 00 through FF.

Character — Specify up to 32 bytes, each as an ASCII character.

Binary — Specify up to 4 bytes as 32 binary bits, each a 0 or 1.

In hexadecimal or binary format, an X stands for anything at that position. In ASCII format, Alt-x has the same effect; when you press Alt-x, the corresponding position is shaded, like this: ▒.

Data-Relative vs. Frame-Relative Offset

The pattern's position within the frame is described by its *offset*. On token ring, FDDI, and certain other LANs, some frames contain a variable-length field called *source routing information* (RI). When this field is present, it appears after the DLC destination and source address, but before the regular data field.

As a result, the position of the data within a particular frame depends on whether that frame contains an RI field. When you specify the **Data relative** offset, the Sniffer analyzer adjusts the offset to compensate for the length of each frame's routing field. (For more information about the source routing field, see "Setting the Interpret RI Option" on page 2–8.)

If you are uncertain about whether a frame contains an RI field, you can define the offset in one of two ways:

Frame relative — Defines the offset as the number of bytes from the start of the frame.

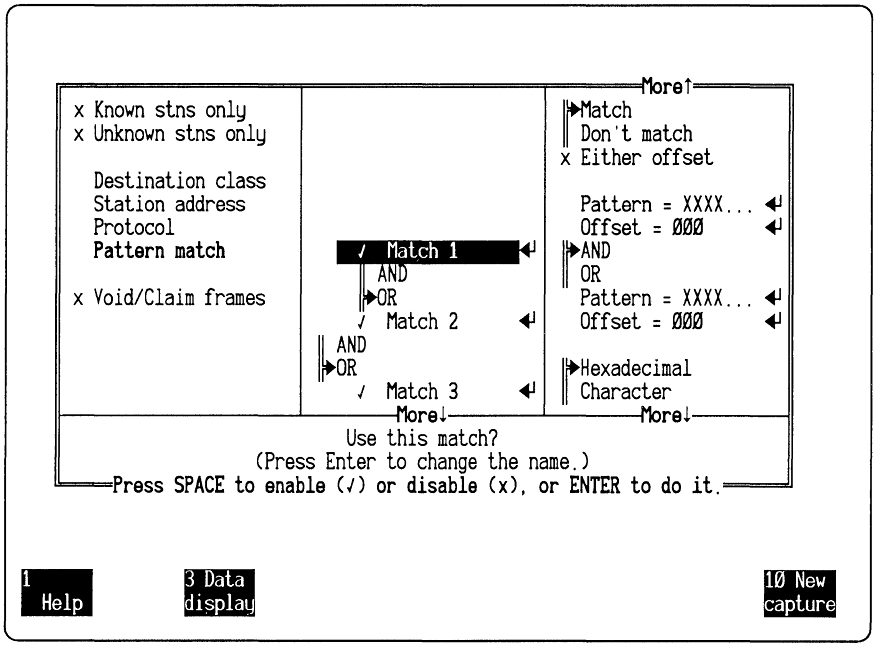
Data relative — Defines the offset as the number of bytes from the start of the frame's data segment; that is, from the start of the 802.2 frame data.

When a frame's source and destination stations are on the same network, it requires no forwarding and the routing field is frequently, but not universally, omitted. If you are confident that all frames of interest are in the same format (either all contain an RI field or none do), it is safe to enable the **Frame relative** offset option. Otherwise, enable the **Data relative** offset option. Figure 3–31 shows these options in the menu.

Defining a Pattern Match Filter

To review: you can link up to four matches by AND or OR logical operators. You can define each match in hexadecimal, character, or binary format and determine its location in the frame by defining the offset, which can be data or frame relative. In addition, you can further define the pattern by enabling or disabling the **Either offset** option. You can also specify whether to include or exclude matches with the **Match** and **Don't Match** options. For more information about each of these options, review the earlier material in this section, starting with "Defining Complex Pattern Matches."

Before defining a pattern match, first determine the pattern's logic with the options associated with the **Pattern match** filter. Figure 3–37 shows these options.



```
                                                          More↑
 x Known stns only                                    ▶Match
 x Unknown stns only                                   Don't match
                                                      x Either offset
   Destination class
   Station address                                     Pattern = XXXX... ↵
   Protocol                                            Offset = ØØØ      ↵
   Pattern match             √ Match 1         ↵      ▶AND
                               AND                     OR
 x Void/Claim frames          ▶OR                      Pattern = XXXX... ↵
                             √ Match 2         ↵       Offset = ØØØ      ↵
                          AND
                         ▶OR                          ▶Hexadecimal
                             √ Match 3         ↵       Character
                              More↓                    More↓
                          Use this match?
                 (Press Enter to change the name.)
 Press SPACE to enable (√) or disable (x), or ENTER to do it.

 1          3 Data                                         1Ø New
   Help     display                                        capture
```

Figure 3–37. Defining a pattern match.

To define a pattern match for a capture filter:

1. Move to **Capture filter\Pattern match\Match 1.**

2. If you want to name the match, press Enter and type the desired name into the dialog box that appears.

3. Define the pattern's logic. Move to each of the desired options and press Spacebar to select that option.

   a. Define whether to compensate for the pattern's offset, depending on the presence of a source routing field.

▶ Frame relative (default)
Data relative

b. Define whether this match captures frames that either match or don't match the specified pattern.

▶ Match (default)
Don't match

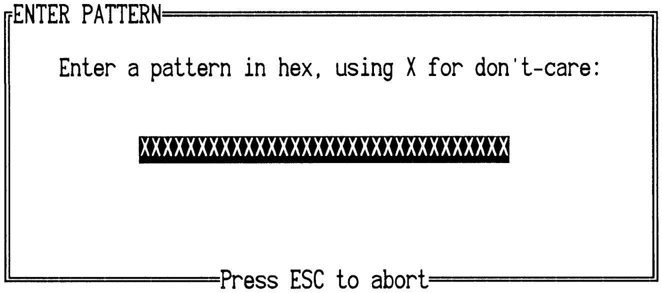
c. Determine whether the offset of one of the patterns applies to the others. Move to the **Either offset** option and press Spacebar to enable or disable the option.

d. Determine the pattern's format (at the bottom of the panel).

▶ Hexadecimal (default)
Character
Binary

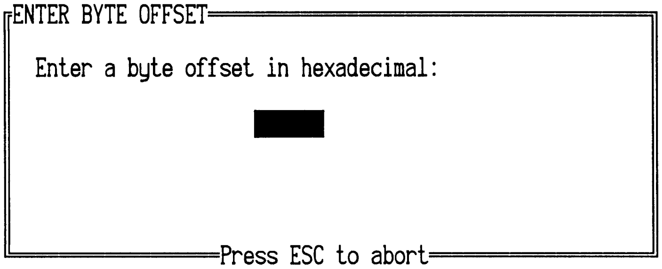
4. Specify the pattern.

a. Move to **Pattern=** and press Enter. In the dialog box that appears, type the pattern and press Enter.



```
ENTER PATTERN

    Enter a pattern in hex, using X for don't-care:

          XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

                    Press ESC to abort
```

b. Move to **Offset=** and press Enter. In the dialog box that appears, type the value of the offset and press Enter. Note that the offset is always in hexadecimal.



```
ENTER BYTE OFFSET

  Enter a byte offset in hexadecimal:

                    Press ESC to abort
```

5. Repeat steps 1 through 4 to define any other matches.

6. Define the relationship between the matches.

a. For each match, press Spacebar to enable (√) or disable (x) that match.

b. Define the logical relationships between Match 1 and Match 2, between Match 3 and Match 4, and between the two pairs of matches. For each, move to the desired option and press Spacebar.

AND
▸ OR

Copying and Pasting a Pattern from the Display Hex Window

If you already captured a frame that contains the desired pattern, you can copy that pattern's characters and its offset, without having to type them again. (This procedure makes use of the Hex and Detail views chosen from the Display menu, as described in more detail in the next chapter.)

To enter a pattern by copying and pasting:

1. Move to **Display\ Detail** and **Display\Hex** and press Spacebar to enable both options. Press F9 (**Pause**) and then F3 (**Data display**) to display the interpreted frames.
2. Find the frame that contains the pattern you want.
3. In the Detail view, move to the desired field. This automatically highlights the corresponding field in the Hex view.
4. While the field is highlighted, press F5 to return to the main menu.
5. Move to **Capture filters\Pattern match** and then to one of the four matches.
6. If necessary, move up to define the **Frame relative** or **Data relative** offset options.
7. Move to **Pattern=** and press Enter to display the associated dialog box.
8. Press the Cursor Up key. In response, the analyzer copies the characters highlighted in the Hex view into the pattern entry dialog box. Press Enter to record the pattern.
9. Move to **Offset=** and press Enter. Press the Cursor Up key to copy the pattern's offset into the offset dialog box. Press Enter to record the offset.

Example of a Capture Filter Pattern Match

The following example is based on the use of Telnet over TCP/IP over Ethernet, using the sample file TCPIP.ENC in the CAPTURE directory. However, the general strategy for setting a pattern match is not specific to the network or protocols of this example.

Suppose you experience a problem while using a terminal emulation package. While connected to a remote host, the network software confuses the actions of the Backspace and Delete keys, which (in this application) are supposed to do different things. Who is mixing them up? The emulator at the PC? The application at the host? The network software between them?

As a first step, you might examine what the emulator transmits to the host when you press Backspace and when you press Delete, as well as what the host echoes back for each character. (Telnet often supports a terminal by transmitting one character at a time to the host. Usually, the host echoes each displayable character back to the terminal one at a time.)

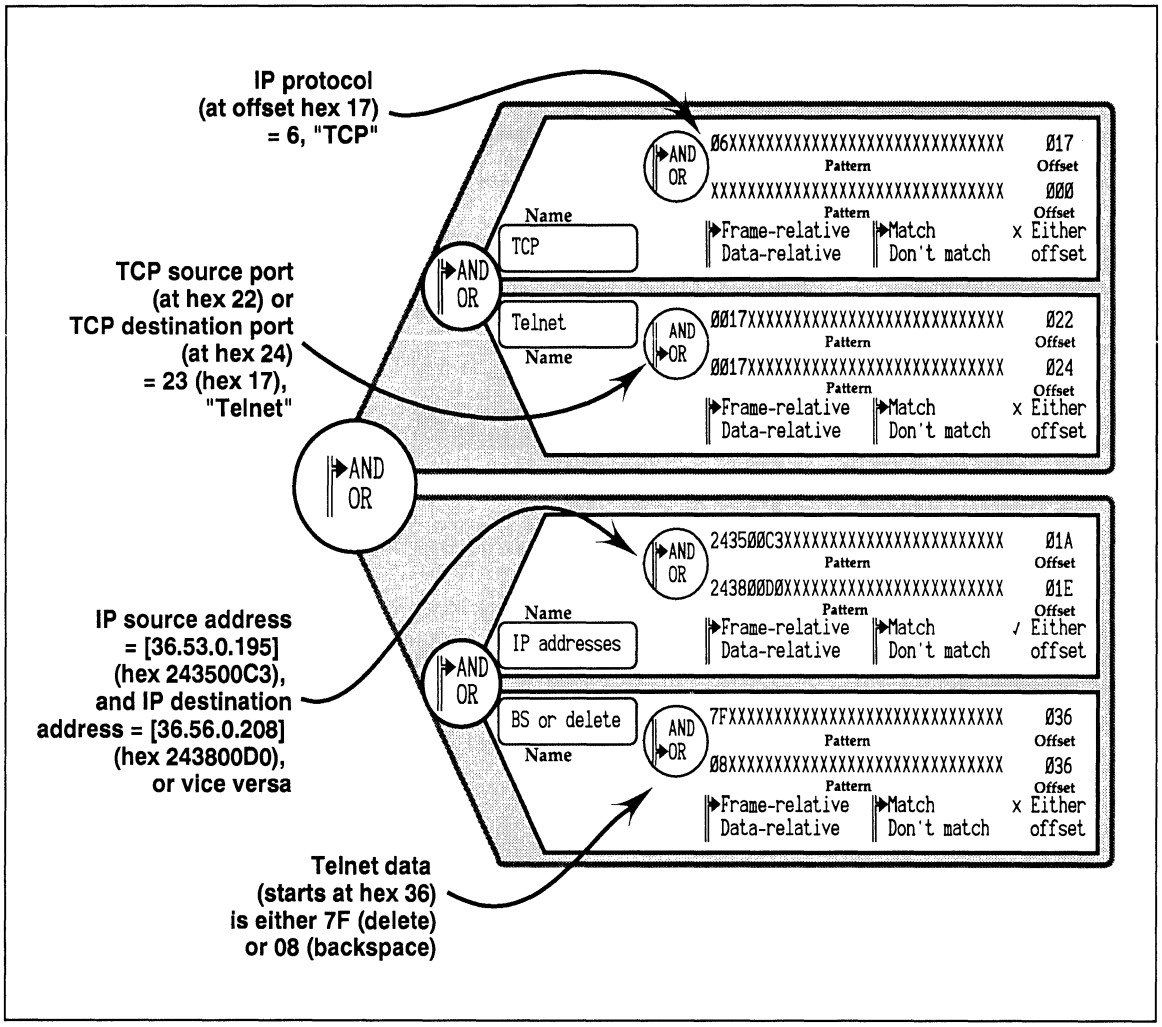
To study what happens, you need a filter that accepts only those frames that include either Backspace or Delete embedded in a Telnet frame passing between the host and the terminal emulation program. Although you can't set a capture filter for the Telnet protocol explicitly (since you can't filter on high-level protocols during capture), you can achieve the same result with pattern matching. Here's how you discover a pattern that identifies not just a Telnet frame, but one whose content involves the characters in question.

First, set an address filter to select all frames sent from the terminal emulator. Then (from the terminal emulator) execute a command that uses Backspace and then a command that uses Delete. By browsing through the frames thus captured, you can readily find Telnet frames addressed to the host. By examining the captured frames, you can see that each consists of:

- A DLC frame (with a DLC source, destination, and IP ethertype), and within that
- An IP frame (with an IP source, destination, and TCP protocol), and within that
- A TCP frame (with a TCP source and destination port of "Telnet"), and within that
- A Telnet frame that contains the record of a keystroke sent from the terminal emulator to the host.

To study how the program treats Backspace and Delete, you can use the "copy and paste" facility to set a capture filter to accept a frame that matches the following pattern:

- It contains the IP protocol number for "TCP" (hex "06" at offset 17).
- It contains the TCP code for Telnet data (indicated by a TCP source or destination port number of hexadecimal 17).
- Its IP source is the address of the PC running the terminal emulator, and its IP destination is the address of the host, or vice versa (by checking either offset).
- The Telnet data is either the code for delete (7F) or the code for backspace (08).



Name: TCP

AND

06XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX Pattern — 017 Offset

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX Pattern — 000 Offset

Frame-relative / Data-relative; Match / Don't match; x Either offset

Name: Telnet

OR

0017XXXXXXXXXXXXXXXXXXXXXXXXXXXX Pattern — 022 Offset

0017XXXXXXXXXXXXXXXXXXXXXXXXXXXX Pattern — 024 Offset

Frame-relative / Data-relative; Match / Don't match; x Either offset

Name: IP addresses

AND

243500C3XXXXXXXXXXXXXXXXXXXXXXXX Pattern — 01A Offset

243800D0XXXXXXXXXXXXXXXXXXXXXXXX Pattern — 01E Offset

Frame-relative / Data-relative; Match / Don't match; √ Either offset

Name: BS or delete

OR

7FXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX Pattern — 036 Offset

08XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX Pattern — 036 Offset

Frame-relative / Data-relative; Match / Don't match; x Either offset

Figure 3–38. Example of a pattern match in the capture filter.

Figure 3–38 is based on the sample file TCPIP.ENC in the CAPTURE directory. It shows how pairs of individual patterns are combined to create matches, and how the resulting matches are combined to create the filter. The shading shows how various components are grouped. The fields show the data for the example. (Of course, in a real situation, the IP addresses would be different, but the values for "Telnet" and "TCP" are appropriate.)

Void/Claim Frames Filter

On FDDI networks, this filter checks for the presence of void or claim frames. When enabled, the Sniffer analyzer captures void and claim frames. When disabled, the analyzer ignores these frames. Note that this is a hardware filter and only works on live capture. This filter is not applicable to trace file replay.

Claim frames are used in the "claim process" as part of the ring initialization process. The claim process begins when a station's MAC entity transmits claim frames (containing the station's address and bid for the target token rotation time). Other stations in the ring compare the claim frames with their own. When a station receives its own claim frame, it wins the right to initialize the ring.

Void frames are frames that contain no data, though they contain starting and ending bits.

The default is x **Void/Claim frames** disabled.

To change the Void/Claim frames filter:

1. Move to **Capture filters\Protocol\Void/Claim frames.**
2. Press the Spacebar to enable (√) or disable (x) the filter.

Filters for Defective Frames

On a WAN/Synchronous link and on Ethernet, StarLAN, and PC Network topologies, the Sniffer analyzer can filter frames for either the presence or absence of certain defects. Note that this ability is available only if the adapter card retains defective frames and passes them to the Sniffer's CPU. The adapter card for token ring simply discards defective frames, so you cannot filter for defective frames.

The breakdown for Ethernet frames includes:

- **Good frames** that contain none of the other defects.
- **Bad CRC frames,** which include frames found to be defective by the cyclic redundancy check (CRC).
- **Short frames,** which include frames shorter than 60 bytes.
- **Collision frames** (Ethernet-II only), which indicate the results of a collision.

How the Defective Frames Filters Work (Ethernet)

Figure 3–39 shows the normal collision window and late collisions that occur after byte 64. Within the normal collision window, there is the preamble area and the frame area. Whether collisions in each of these areas are counted and whether—and how—the associated frames are flagged depends on whether your Sniffer analyzer has an Ethernet or Ethernet-II adapter card.

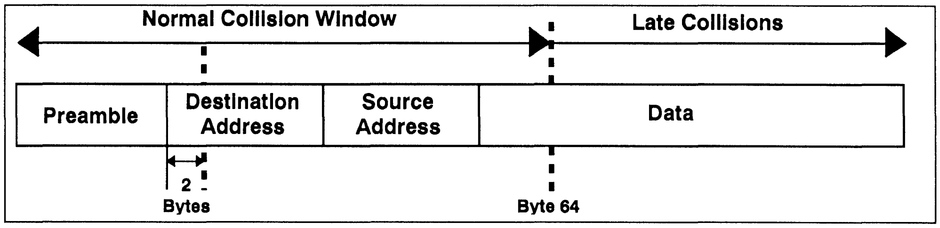


Figure 3–39. Collision detection.

For analyzers with an Ethernet adapter card, collisions in the preamble are neither counted nor flagged. Collisions after the first two bytes of the frame area are counted as short frames and flagged "R" (runt). Collisions after byte 64 are counted as CRC errors and flagged "C" (CRC).

For analyzers with an Ethernet-II adapter card, collisions in the preamble are counted, but the frames are *not* stored in the capture buffer. Collisions in the frame area are counted as collision frames and flagged "X" (Collision). Collisions after byte 64 are also counted and flagged "X."

Figure 3–40 provides an overview of how collision frames are treated by the two networks.

	Ethernet		Ethernet-II	
Collision detected in...	**counted**	**flagged**	**counted**	**flagged**
Preamble	no	no	yes	not stored
Frame area	yes	R (Runt)	yes	X (Collision)
Late collision	yes	C (CRC)	yes	X (Collision)

Figure 3–40. Overview of how collision frames are treated.

Note: Because collisions that occurred in the preamble area (or the first two bytes of the frame area) are not followed by frame data, you won't be able to see the collision frames even though they are counted. Since many collisions occur in the preamble area of the frame, this is a common occurrence.

To set filters for frame defects:

1. Move to **Capture filters** and then to the defect category for which you want to filter.
2. Press Spacebar to enable (√) or disable (x) the desired options.
   √ Good frames
   √ Bad CRC frames
   √ Short frames
   √ Collision frames (Ethernet-II)

Defective Frames on an FDDI Network

The capture filters for an FDDI network do not provide separate choices for the various kinds of defective frames. They are simply referred to as error frames. When you enable **Error frames** from the **Capture filters** menu, the capture will include these types of error frames:

- E-flag set: Another station has marked this frame as an error frame by setting the frame's E-flag.
- Bad CRC: The analyzer detected the bad CRC. In accordance with the FDDI standard, the analyzer will set the frame's E-flag.
- Fragment frame: The analyzer detected the fragment frame and will decode the frame as having invalid frame status.

Sniffer Internetwork Analyzer Capture Filters

When capturing traffic on a WAN/Synchronous link, the following capture filters are available:

- Pattern match
- From DTE
- From DCE
- RR frames
- RNR frames
- Info frames
- Good frames
- Bad CRC frames

The **Pattern match, Good frames**, and **Bad CRC frames** filters are the same as those for LANs. For additional information, see "Pattern Match Filter" on page 3–39 and "Filters for Defective Frames" on page 3–50.

From DTE/From DCE Capture Filters

The **From DTE** (Data Terminal Equipment) and **From DCE** (Data Communication Equipment) filters allow you to filter on direction. Although the WAN/Synchronous link is bidirectional (**From DTE** or **From DCE**), you can choose to accept frames in just one, the other, or both directions. You can also set both **From DTE** and **From DCE** to off (x). However, if you do this, no data will be captured.

RR Frames/RNR Frames Capture Filters

You can also filter for **RR** (Receiver Ready) and **RNR** (Receiver not Ready) frames. These frames are exchanged by the DTE and DCE devices in the process of setting up communications between the endpoints of a WAN/Synchronous link. Once the link is established, these frames control the flow of frames. Therefore, if you are investigating problems in handshaking or flow control, these filters may be relevant. When you are interested primarily in the higher-level messages, the RR and RNR frames are usually irrelevant.

Info Frames Capture Filter

The **Info frames** capture filter allows you to filter on SDLC/HDLC Info frames (commonly called "I-frames"). Info frames carry the actual data to be transmitted for the user. Additionally, SDLC/HDLC Info frames can carry flow and error control data, and as such, may be useful for troubleshooting problems on the WAN link.

To set the Sniffer Internetwork Analyzer capture filters:

1. Move to **Capture filters** and then to the desired filter.

2. Press Spacebar to enable (√) or disable (x) the desired filter, as appropriate. For example:

   √ From DTE
   √ From DCE

Stopping Capture

You can always stop a capture in progress by pressing F10 (**Stop capture**). However, instead of randomly stopping capture and risking losing frames when the buffer fills, you can also stop capture automatically in one of two ways:

- When the buffer is full
- When the Sniffer analyzer detects a trigger event

You can either enable or disable the automatic **Stop capture** feature. If you choose to stop capture automatically, you can further define whether to stop when the buffer is full or when the trigger event is detected. You can also save all or a portion of the capture buffer that contains the trigger event to the hard disk.

To determine how to stop the capture:

1. Move to **Trigger\Stop capture** and then to the desired option.

   ▶ Stop at trigger
   Stop when full

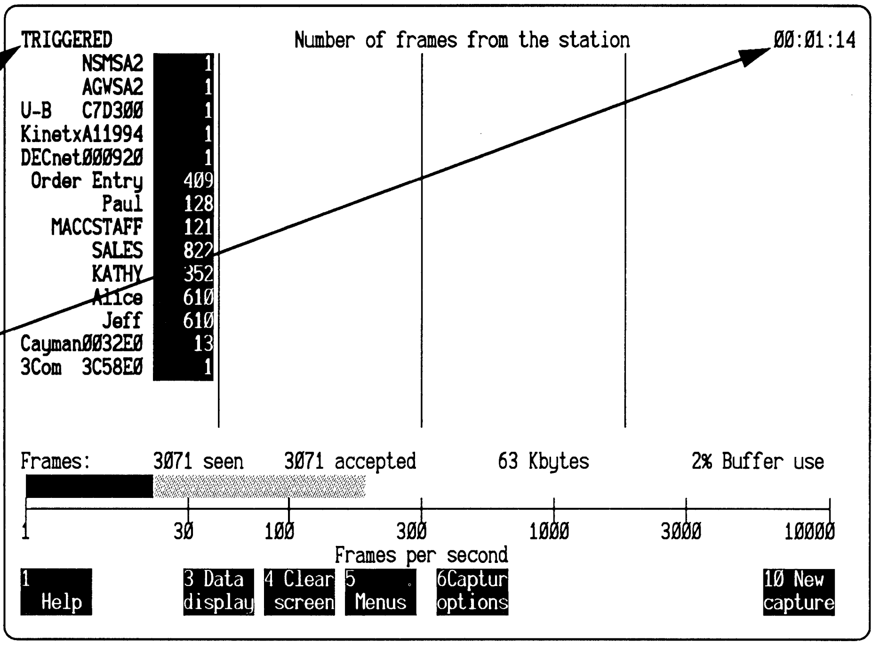
2. Press Spacebar to enable (√) that option.

Defining a Trigger to Stop Capture

If you enabled the **Stop at trigger** option, the Sniffer analyzer automatically stops capture when it detects a *trigger event*, which can be either an internal or external trigger.

An internal trigger can be a specified defective frame (on WAN/Synchronous links and on Ethernet, StarLAN, and PC Network topologies) or a frame that contains a pattern you specify. An external trigger occurs when the analyzer detects a signal at its serial port. Such a signal is typically sent by another computer, which is linked to the analyzer with a serial port to serial port connection, or by a sensor connected to the port. In addition, the analyzer can send a signal to the port when the trigger event occurs. This signal could notify another computer or device connected to the serial port.

When the trigger event occurs, the capture either stops immediately or after a specified delay. As a result, the capture buffer contains the *trigger frame*, the frame that preceded the trigger frame, and (optionally) the frames that followed it. The word "TRIGGERED" replaces the word "CAPTURING" in the top left of the capture screen. You can see this in Figure 3–41.



```
TRIGGERED                 Number of frames from the station            00:01:14
        NSMSA2      1
        AGWSA2      1
U-B    C7D300       1
KinetxA11994        1
DECnet000920        1
  Order Entry     409
         Paul     128
    MACCSTAFF     121
        SALES     822
        KATHY     352
        Alice     610
         Jeff     610
Cayman0032E0       13
3Com   3C58E0       1

Frames:    3071 seen    3071 accepted      63 Kbytes       2% Buffer use

1          30      100      300      1000      3000      10000
                      Frames per second
1 Help   3 Data display   4 Clear screen   5 Menus   6Captur options   10 New capture
```

"TRIGGERED" indicates that the trigger event has occurred.

Shows the time the trigger was detected

Figure 3–41. Indication that capture is stopped by trigger event.

When you display the contents of the capture buffer, the trigger frame is marked with the letter "T" when later displayed in the Summary view (see "Flags Display Option" on page 4–27). You can use this flag to search for the trigger frame and to display the time relative to its arrival (see "Searching for Frames" on page 4–41).

Note that the capture buffer never contains more than one frame marked T. Even if a second frame with the trigger pattern arrives during the delay before capture is stopped, only the first frame is reported and flagged as the trigger.

Setting a trigger consists of three tasks:

- Defining the trigger event
- Determining whether to save the portion of the capture buffer that contains the trigger frame to disk (disk snapshot)
- Defining the delay after the trigger event at which capture stops

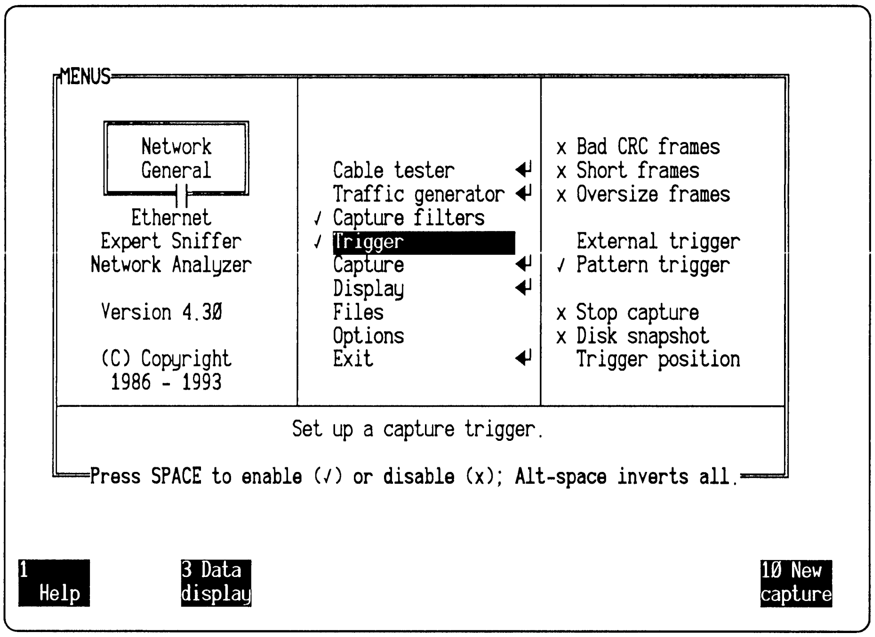
As with the capture filters, you can temporarily prevent a trigger pattern from stopping capture by disabling the **Trigger** option.

Defining the Trigger Event

Defining a trigger event that consists of defective frames (on most LANs or on WAN/Synchronous links) or of an external trigger is relatively straightforward. Defining a trigger that consists of a pattern match requires more planning and perhaps some experimentation. For detailed information about defining pattern matches, refer to "Defining Complex Pattern Matches" on page 3–40.

The FDDI analyzer allows you to use Error frames as the trigger event.

Figure 3–42 shows the options associated with defining the trigger for an Ethernet-II Sniffer analyzer.



```
MENUS
   Network                                      x Bad CRC frames
   General           Cable tester          ↵    x Short frames
                     Traffic generator     ↵    x Oversize frames
  Ethernet         √ Capture filters
Expert Sniffer     √ Trigger                      External trigger
Network Analyzer     Capture               ↵    √ Pattern trigger
                     Display               ↵
Version 4.30         Files                      x Stop capture
                     Options                    x Disk snapshot
(C) Copyright        Exit                  ↵      Trigger position
 1986 - 1993
                     Set up a capture trigger.
Press SPACE to enable (√) or disable (x); Alt-space inverts all.

1 Help        3 Data display                             10 New capture
```

Figure 3–42. Trigger menu for an Ethernet-II analyzer.

To define the trigger event on a LAN:

1. Move to **Trigger\Stop capture\Stop at trigger** and press Spacebar to choose the desired option.

   ▸ Stop at trigger
   Stop when full

2. To define an external trigger, move to **Trigger\External trigger** and press Spacebar to enable (√) the desired options.

   x From COM1 CTS/DSR (send trigger signal)
   x To COM RTS/DTR (receive trigger signal)

3. To define defective frames as the trigger event on Ethernet, StarLAN, or PC Network, press Spacebar to enable (√) the desired options.

   √ Bad CRC frames
   x Short frames
   x Oversize frames (Ethernet only)
   x Error frames (FDDI only)

4. To define a pattern as the trigger event, define up to four matches. For each match, press Spacebar to set up the desired pattern.

   √ Match 1
   AND
   ▸ OR
   √ Match 2
   AND
   ▸ OR

√ Match 3
 AND
▸ OR
√ Match 4

Examples of Pattern Match Triggers: LAN

Figure 3–43 shows two examples of how to use pattern matches as a trigger to stop capture.

Token Ring/IBM	Ethernet/XNS (3Com + network)
To trigger on a frame reporting an SMB error, first set the capture filter to pass only NetBIOS frames. Then set the trigger to stop the capture when it finds that the primary SMB return code is not equal to 00 (zero means "Classic"). In an IBM SMB frame, the primary return code is a single byte located at data relative offset 27 (hex).	To trigger on a frame reporting an SMB error, first set the capture filter to pass only XNS frames. Then set the trigger to stop the capture when it finds that the primary SMB return code is not equal to 00 (zero means "Classic"). In an XNS SMB frame, the primary return code is a single byte located at data relative offset 3D (hex).

Figure 3–43. Sample trigger pattern matches on token ring and Ethernet networks.

To define the trigger event on a WAN/Synchronous link:

1. Move to **Trigger\Stop capture\Stop at trigger** and press Spacebar to enable (√) the option.
2. To define **Bad CRC frames** as the trigger, move to that option and press Spacebar to enable (√) it.
3. To define an external trigger, move to the desired options and press Spacebar to enable or disable the options.

   √ From COM1 CTS/DSR
   √ To COM RTS/DTR

4. To define a pattern as the trigger event, define up to four matches. For each match, press Spacebar to set up the desired pattern.

   √ Match 1
    AND
   ▸ OR
   √ Match 2
    AND
   ▸ OR
   √ Match 3
    AND
   ▸ OR
   √ Match 4

Saving the Trigger Frame to Disk

The **Disk snapshot** option, when enabled, lets you save the portion of capture buffer that contains the trigger frame as a file, to examine its contents later. As each snapshot file is saved, the system assigns it the name "Snap", a number from 1 through the maximum number you defined (the default is 10), and an extension that identifies your network. For example, the fourth snapshot on an Ethernet network would be named "SNAP4.ENC". These files are stored in the CAPTURE directory.

The options associated with the **Disk snapshot** option include:

- Whether to save when the snapshot file is full or when the trigger event is detected. If you choose the **Save when full** option, the buffer is saved continuously (whether the trigger event is detected or not) until you reach the maximum number of snapshot files, unless the **Overwrite files** option is enabled.
- The size of the snapshot file.
- The maximum number of snapshot files to be created.
- Whether to overwrite existing snapshot files when you exceed the maximum specified by the **Files =** option.
- Whether to save the snapshot files in compressed format. This process is transparent to the analyzer. That is, when you play back files saved in compressed format, they will be autmatically decompressed by the analyzer. Note, however, that compressed files cannot be decompressed by earlier (pre-4.30) versions of the analyzer software.

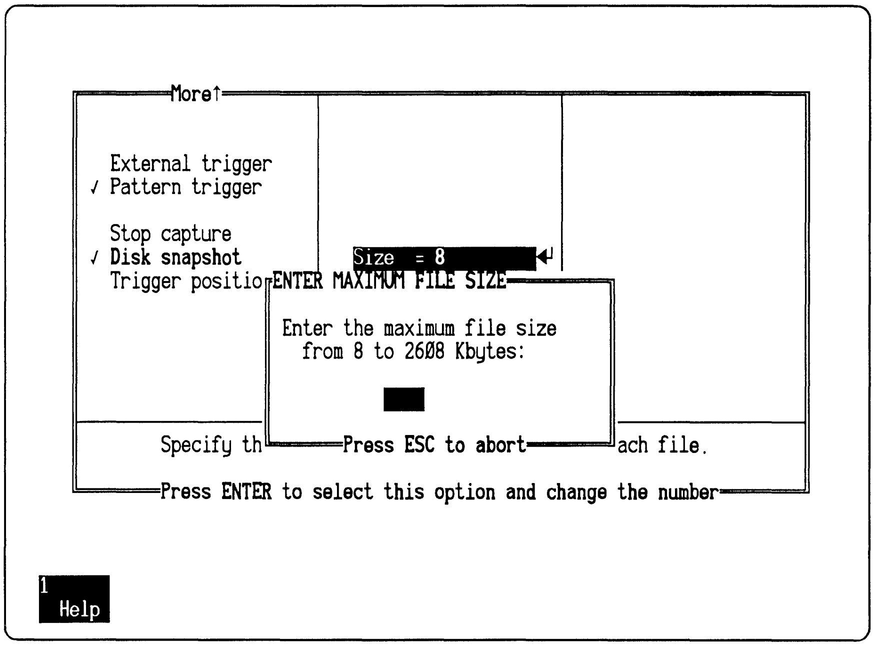
How much information is saved in the snapshot files also depends on the **Trigger position** you specify, which determines the delay after the trigger event before the capture stops. This determines how many of the frames that surround the trigger frame are captured. This option is explained in more detail in the next section. The relationship between the two options is shown in Figure 3–46.

To save snapshot files to disk:

1. Move to **Trigger\Disk snapshot.** Press Spacebar, if necessary, to enable (√) the option.
2. Determine when to take the snapshot. If you choose **Save when full,** how much is saved depends on the size you specify for the snapshot file.

   ▶ Save at trigger
   Save when full

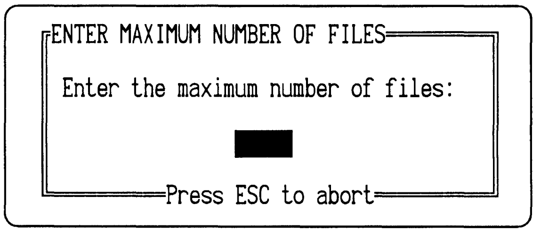
3. To change the size of the snapshot files, move to **Size**= and press Enter. In the dialog box that appears, type the desired file size and press Enter. Figure 3–44 shows this dialog box.



```
More↑

  External trigger
√ Pattern trigger

  Stop capture
√ Disk snapshot          Size  = 8 ↵
  Trigger positio ENTER MAXIMUM FILE SIZE

                  Enter the maximum file size
                    from 8 to 2608 Kbytes:

Specify th           Press ESC to abort          ach file.
Press ENTER to select this option and change the number

1
Help
```

Figure 3–44. Defining the size of snapshot files.

4. To change the maximum number of snapshot files created, move to **Files=** and press Enter. In the dialog box that appears, type the desired maximum number of files and press Enter.



```
ENTER MAXIMUM NUMBER OF FILES

 Enter the maximum number of files:

          Press ESC to abort
```

5. To determine how to handle files that exceed this maximum, move to **Overwrite files.** Press Spacebar to enable (√) or disable (x) the option.

6. To determine whether the files are saved compressed or uncompressed, move to **Compress files**. Press Spacebar to enable (√) or disable (x) the option.

Defining the Trigger Delay

The **Trigger position** option determines whether capture stops immediately when the trigger event is detected or after some delay. By setting a delay, you can retain the frames that precede or follow the trigger event.

The effects of the various stopping options are summarized in Figure 3–45.

Option	Effect
Stop when full	Even if the trigger event has not occurred, capture stops when there is no more space in the capture buffer.
Continuous capture	The frames that arrived earlier are discarded to make room in the capture buffer for the newer arrivals. When the trigger event occurs, the analyzer (as usual) posts the word "TRIGGERED" on the screen, but does not stop capturing. If nothing else happens to stop capture, sooner or later —depending on the size of the frames and the space in the buffer— arriving frames will displace those already captured and the trigger frame will be among those discarded.
0% pretrigger	Capture continues until the trigger frame is the oldest remaining in the capture buffer (frame 1), and all other frames follow it.
25% pretrigger	Capture continues until 25% of the space in the capture buffer is devoted to frames that arrived before the trigger frame.
50% pretrigger	As above, but 50% of the space in the capture buffer is devoted to frames that arrived before the trigger frame.
75% pretrigger	As above, but 75% of the space in the capture buffer is devoted to frames that arrived before the trigger frame.
100% pretrigger	Capture stops at once, so that the trigger frame is the last to arrive in the capture buffer and all other frames preceded it.

Figure 3–45. Effect of "stop capture" options in the trigger menu.

The **Trigger position** option also determines what is included in the disk snapshot files, if that option is enabled (see previous section). The relationship between the two options is shown in Figure 3–46.

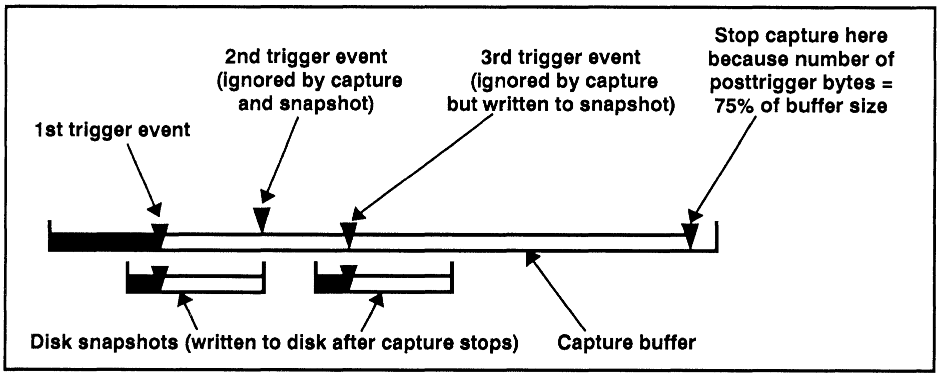

2nd trigger event (ignored by capture and snapshot)
3rd trigger event (ignored by capture but written to snapshot)
Stop capture here because number of posttrigger bytes = 75% of buffer size
1st trigger event
Disk snapshots (written to disk after capture stops)
Capture buffer

*Figure 3–46. Relationship between the **Disk snapshot** and **Trigger position** options.*

To define the trigger delay:

1. Move to **Trigger\Trigger position**.
2. Determine when to stop the capture. Move to **Stop at capture** and then to the percentage of frames saved before the trigger was detected. To select one, move to the desired option and press Spacebar.

   0% pretrigger
   25% pretrigger
   50% pretrigger
   ▸ 75% pretrigger (default)
   100% pretrigger

Temporarily Disabling the Trigger Option

As with the capture filters, you can temporarily disable the defined trigger without changing the trigger options you defined. In that way, you don't have to undo your work. This is especially useful if you defined a complex match pattern as the trigger event.

To temporarily disable the trigger:

1. Move to **Trigger** and press Spacebar to disable (x) the option.

Starting the Capture

After you set the capture mode, various capture options, the capture filters, and the trigger, you are ready to start the capture.

To start capture:

1. Make sure all options are defined correctly.
2. Press F10 (**New Capture**). Or, in the main menu, move to **Capture** and press Enter.

   The Sniffer analyzer starts to capture frames. The screen shows the progress of the capture in the screen format you specified (individual counts, pair counts, or skylines).

Pausing or Stopping Capture

Once started, capture continues until one of the following happens:

- You press F10 (**Stop capture**) to stop capture.
- The specified trigger event occurs (if you enabled **Stop capture\Stop at trigger**).
- The capture buffer is full (if you enabled **Stop capture\Stop when full**).
- You press F9 (**Pause capture**) to pause capture. This permits you to adjust the screen format or the capture filters and then resume the capture.

What You Can Do While Capture is Paused

If you press F9 (**Pause**), the Sniffer analyzer pauses the capture. Frames are no longer captured, but the frames already captured remain in the capture buffer. At this point, you can use the function keys as follows:

F1 **Help** — To access the analyzer's help facility (which is not accessible while actively capturing).

F2 **Display active** — To toggle the display between showing either all connections/sessions or only active connections/sessions. Applicable only in Sniffer Internetwork Analyzer (SDLC/SNA, HDLC/X.25, or Frame Relay) views.

F3 **Data display** — To stop the capture and use the Display function. If you press F3, you *cannot* resume the earlier capture (but you can start a new capture, which first clears the capture buffer).

F4 **Clear screen** — To clear the current display on the screen. Frames in the capture buffer are not affected.

F5 **Menus** — To return to the main menu.

F6 **Capture options** — To change the capture options. Frames already in the capture buffer are not affected.

If you make any changes to the options or filters, the analyzer clears the screen before resuming capture if you press F6 (**Return**) or F9 (**Resume**).

F9 **Resume** — To continue the capture. The next frame to be captured is appended to the capture buffer after the last frame captured before you pressed F9. There is no indication to show that a pause occurred.

F10 **New capture** — To start a new capture.

What You Can Do When Capture Has Stopped

Once capture has stopped, you can either display, save, or discard the frames in the capture buffer.

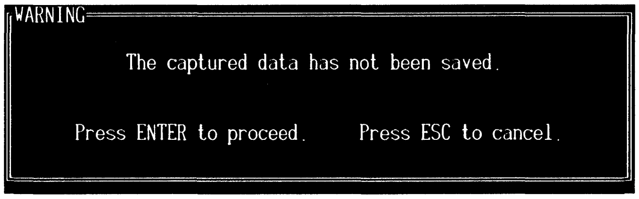
Display — Press F3 (**Data display**) to interpret and display the frames in the capture buffer. For details, see Chapter 4.

Save — You can save the frames in the capture filter and use the resulting data files as a source for capturing frames.

For more information, see "Defining the Capture Source: Live Network or Data File" on page 3–10.

Discard

When you start a new capture or exit from the application without saving the contents of the capture buffer, the Sniffer analyzer displays a warning dialog box (Figure 3–47). If you press Enter, the frames in the capture buffer are discarded.



```
WARNING
            The captured data has not been saved.

     Press ENTER to proceed.      Press ESC to cancel.
```

Figure 3–47. Discarding captured frames.

CHAPTER FOUR: DISPLAYING INTERPRETED FRAMES 4

Displaying Interpreted Frames

Overview

This chapter describes one of the Sniffer analyzer's central functions: displaying information about the various layers of protocols embedded in the captured frames. Topics related to displaying interpreted frames include:

- Setting filters to limit which frames are displayed.
- Displaying frames at three levels of detail, in either the normal or the two-viewport format.
- Searching for frames in the displays.
- Editing frames in the Hexadecimal display.
- Printing and importing data.
- Background information about protocol interpretation.

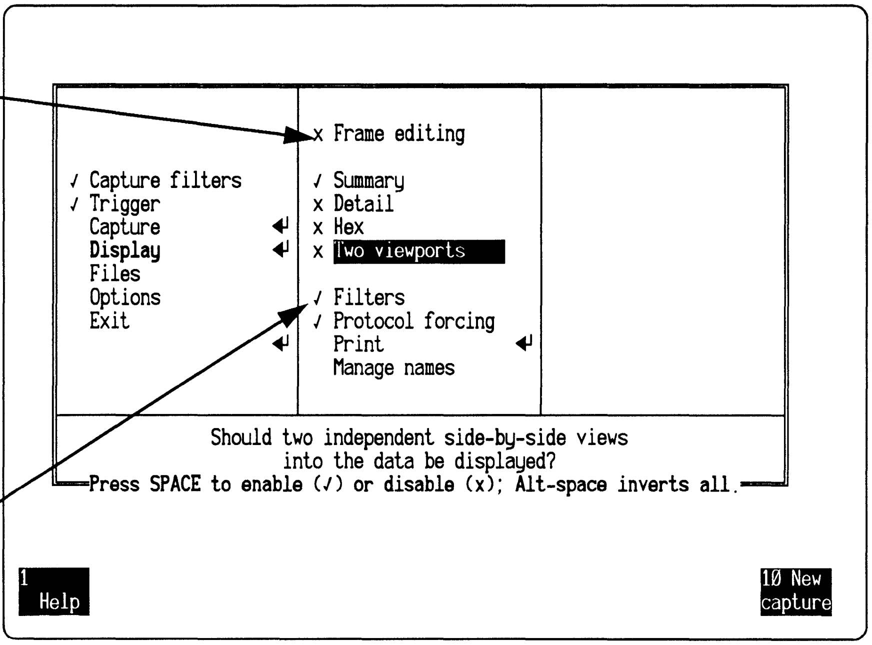
The "Protocol Forcing" display option is described in Chapter 6, "Using Protocol Forcing." Protocol forcing is an advanced Sniffer analyzer function that lets you invoke a specific protocol interpreter (PI) for a frame or set of frames.

Display Menu Overview

Figure 4–1 provides an overview of the basic menu items associated with the Display menu. Many of these items, in turn, have associated options. Beneath the menu is a brief explanation of the highlighted option (**Two viewports** in the example). Note that, although the figure shows the menu as it appears for an Ethernet Sniffer analyzer, the basic Display menu items are the same for all networks.

As with other Sniffer analyzer menu options, you press the Cursor keys to move the highlight to the desired option and then to define that option.

- For options marked with the √ and x symbols, you can press Spacebar to enable (√) or disable (x) the option.
- For options connected with a vertical bar (radio control), you can choose one of those options by moving to it and pressing Spacebar.
- For options where you must define a specific value, such as the range of frames to print, you can either choose that value from a list or enter the desired value into a dialog box.



```
                           x Frame editing

 ✓ Capture filters         ✓ Summary
 ✓ Trigger                 x Detail
   Capture            ↵    x Hex
   Display            ↵    x Two viewports
   Files
   Options                 ✓ Filters
   Exit                    ✓ Protocol forcing
                      ↵      Print            ↵
                             Manage names

             Should two independent side-by-side views
                    into the data be displayed?
 Press SPACE to enable (✓) or disable (x); Alt-space inverts all.

1                                                        10 New
  Help                                                   capture
```

"x" means the option is disabled

"√" means the option is enabled

Figure 4–1. Overview of the Display menu options.

Role of the Capture Buffer in Displaying Frames

Once the capture buffer contains captured frames, you can interpret those frames and display the results. For an overview of how the analyzer processes frames, see Figure 1–2 on page 1–7.

Frames may be in the capture buffer either as the result of a capture or because they were loaded from a file that was saved during a previous capture session. Whenever you start a new capture session or when you load a file, the frames currently in the buffer are lost. If you try to do so, the Sniffer analyzer displays a warning dialog box that lets you save the frames in the capture buffer as a file.

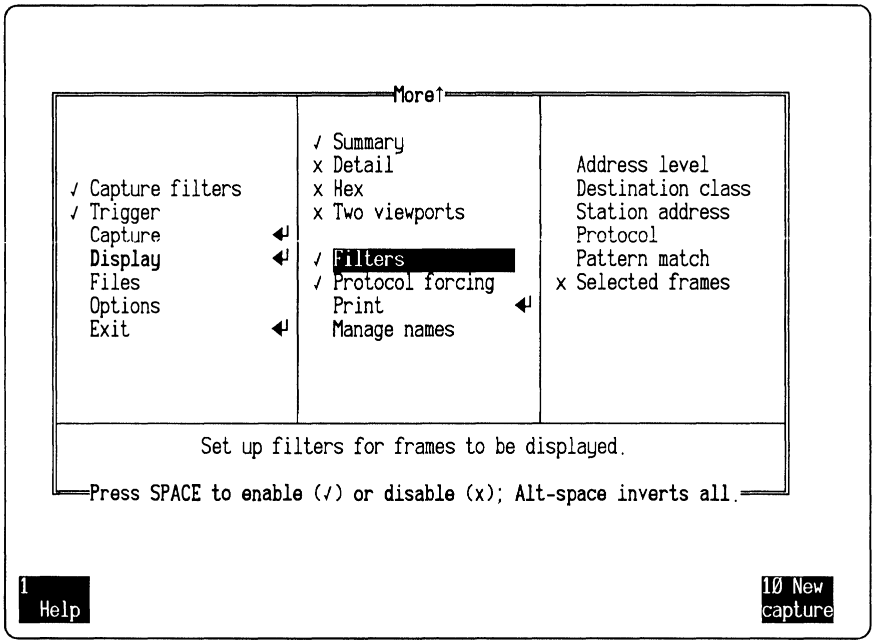
Setting the Display Filters

As with the capture filters, which limit the frames that are captured, the display filters let you eliminate from display those frames that don't interest you. You can set the display filters either before you display captured frames or while you are displaying them.

Filtering does not remove frames from the capture buffer, it simply excludes them from the display. When frames are excluded, those that are displayed have the same frame numbers as before. For example, you might see frame 30 followed by frame 35 because a display filter excluded frames 31 - 34. When you save the contents of the capture buffer to a file, you can choose to either save all frames or only those that pass the display filters.

Overview of Available Filters

Figure 4–2 shows the available display filters.



```
Set up filters for frames to be displayed.
Press SPACE to enable (✓) or disable (x); Alt-space inverts all.
```

Figure 4–2. The display filters.

The following display filters are available for all LANs:

Address level For frames that contain an address in one of the enabled protocols.

Destination class For frames that contain a DLC address in the indicated class (broadcast or specific).

Station address For frames that contain any of up to four specific addresses at any of the levels selected by the **Address level** filter.

Protocol For frames that contain one or more of the enabled protocols.

Pattern match For frames that contain the logical combination of patterns you specify.

Selected frames For frames you flagged with the "S" flag.

If a frame meets the criteria for one filter, the Sniffer analyzer continues to test for the other filters. As a result, a frame may match several of the display filters.

In addition, the following display filters are available for Ethernet, StarLAN, and PC Network:

Good frames For frames that do not contain detected frame defects.

Bad CRC frames For frames with a bad CRC check.

Short frames For frames of less than 60 bytes (runts).

Collision frames (Ethernet-II Sniffer analyzers only) For frames that resulted from collisions.

If a frame meets the criteria for one frame defect the analyzer does not test for any of the others.

The following display filters are available for WAN/Synchronous links:

Address level For frames that contain an address in one of the enabled protocols.

Destination class For frames that contain a DLC address in the indicated class (broadcast or specific).

Station address For frames that contain any of up to four specific addresses at any of the levels selected by the **Address level** filter.

Protocol For frames that contain one or more of the enabled protocols.

Pattern match For frames that contain the logical combination of patterns you specify.

Selected frames For frames you flagged with the "S" flag.

Bad CRC frames For frames with a bad CRC check.

Additionally, the following display filters are available for those token ring and Ethernet analyzers that include Expert functionality:

Network object For those frames associated with a specified network object. For more information, see the *Expert Sniffer Network Analyzer Operations* manual.

Symptom frames For those frames associated with symptoms. For more information, see the *Expert Sniffer Network Analyzer Operations* manual.

Each of these filters is explained in more detail after the procedure that follows. The Expert mode-specific filters, however, are explained in the *Expert Sniffer Network Analyzer Operations* manual.

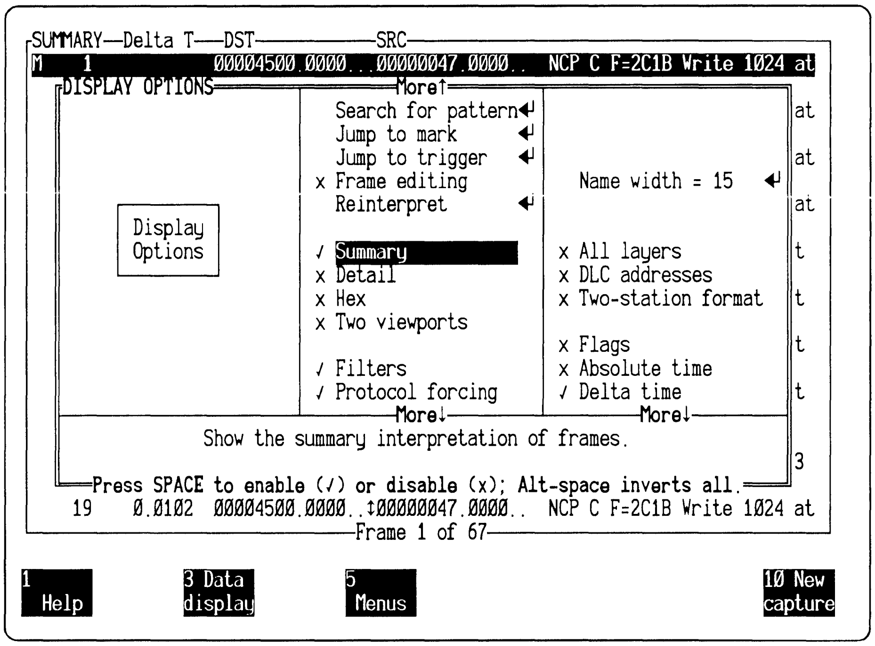
Procedure: Specifying the Display Filters

To set display filters before you start the display:

1. Move to **Display\Filters**. If necessary, press Spacebar to enable (√) the option.
2. Move to the desired filter and press Spacebar to enable (√) or disable (x) that filter.
3. For filters with associated options, define those options.

To change filters (or display options) during the display:

1. Press F6 (**Display options**). In response, the Sniffer analyzer superimposes the Display Options menu (shown in Figure 4–3) over the display window.



```
SUMMARY—Delta T——DST——————SRC———————————————————————————————
M    1        00004500.0000...00000047.0000..   NCP C F=2C1B Write 1024 at
 DISPLAY OPTIONS══════════════More↑═══════════════════════════
                    │   Search for pattern↵ │                        │at
                    │   Jump to mark      ↵ │                        │
                    │   Jump to trigger   ↵ │                        │at
                    │ x Frame editing       │  Name width = 15    ↵  │
                    │   Reinterpret       ↵ │                        │at
    Display         │                       │                        │
    Options         │ ✓ Summary             │ x All layers           │t
                    │ x Detail              │ x DLC addresses        │
                    │ x Hex                 │ x Two-station format   │t
                    │ x Two viewports       │                        │
                    │                       │ x Flags                │t
                    │ ✓ Filters             │ x Absolute time        │
                    │ ✓ Protocol forcing    │ ✓ Delta time           │t
 ───────────────────────────More↓──────────────────More↓─────
              Show the summary interpretation of frames.
                                                                 3
 ══Press SPACE to enable (✓) or disable (x); Alt-space inverts all.══
   19    0.0102  00004500.0000..↕00000047.0000..  NCP C F=2C1B Write 1024 at
 ─────────────────────────Frame 1 of 67──────────────────────────

1           3 Data       5                                   10 New
  Help      display        Menus                             capture
```

Figure 4–3. The Display Options menu.

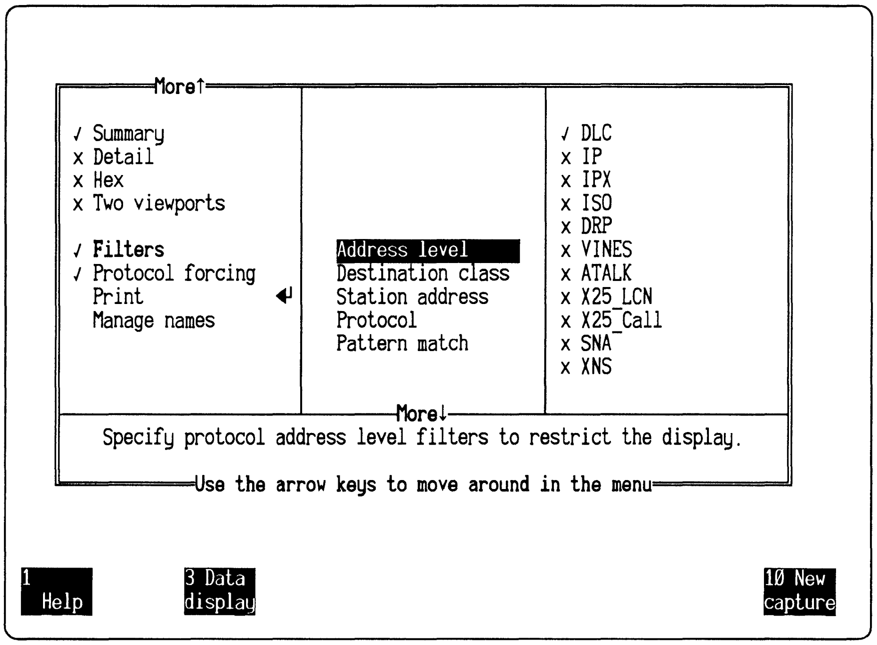
2. Move to **Filters** and make the desired changes in the filters.
3. Press F3 (**Data display**) to return to the display, which will be modified according to the changes you made.

Address Level Filter

When you set an **Address level** filter, you can enable one or more protocols associated with the **Address level** filter. As a result, the filter accepts only those frames that are addressed in one of the protocols you enabled. Therefore, to be included in the display, a frame must contain both:

- An address level from the enabled set of protocols
- An address in that protocol

Figure 4–4 shows the protocol layers associated with the **Address level** filter. The default is only the lowest protocol layer (DLC) enabled (√). Since every frame has a low-level address, the default accepts all frames.



```
More↑
√ Summary                                        √ DLC
x Detail                                         x IP
x Hex                                            x IPX
x Two viewports                                  x ISO
                                                 x DRP
√ Filters              Address level             x VINES
√ Protocol forcing     Destination class         x ATALK
  Print            ↵   Station address           x X25_LCN
  Manage names         Protocol                  x X25_Call
                       Pattern match             x SNA
                                                 x XNS
More↓
   Specify protocol address level filters to restrict the display.

Use the arrow keys to move around in the menu

1          3 Data                                          10 New
 Help      display                                         capture
```

Figure 4–4. Specifying the Address level display filters.

Every frame contains both the address of the station from which it just came and the address of the station that is its immediate destination. These addresses are in the frame's lowest level, usually DLC. However, a frame frequently contains other addresses as well. For example, it may contain the address of the original source and the address of the ultimate destination. This means that the data field of a lower-level frame may include a message written in a higher-level protocol, with its own source and destination, written according to that protocol's rules.

This is usually the case for all frames on a WAN/Synchronous communications link. It is also very likely when frames are relayed through a gateway between LANs. At the DLC level, a frame's source and destination may be the stations responsible for the current leg of its journey. Within the DLC frame, there may be addresses in embedded protocols such as XNS, IP, X.400, and so on.

Although many protocols require that the frame include an address, that requirement is not universal. If the protocol permits both addressed and unaddressed messages, an **Address level** filter accepts a frame only when it actually contains an address.

To set an Address level display filter:

1. Move to **Display\Filters\Address level.**
2. Move to the protocols you want to enable (√) or disable (x) and press Spacebar accordingly.

Effect on Displayed Frames

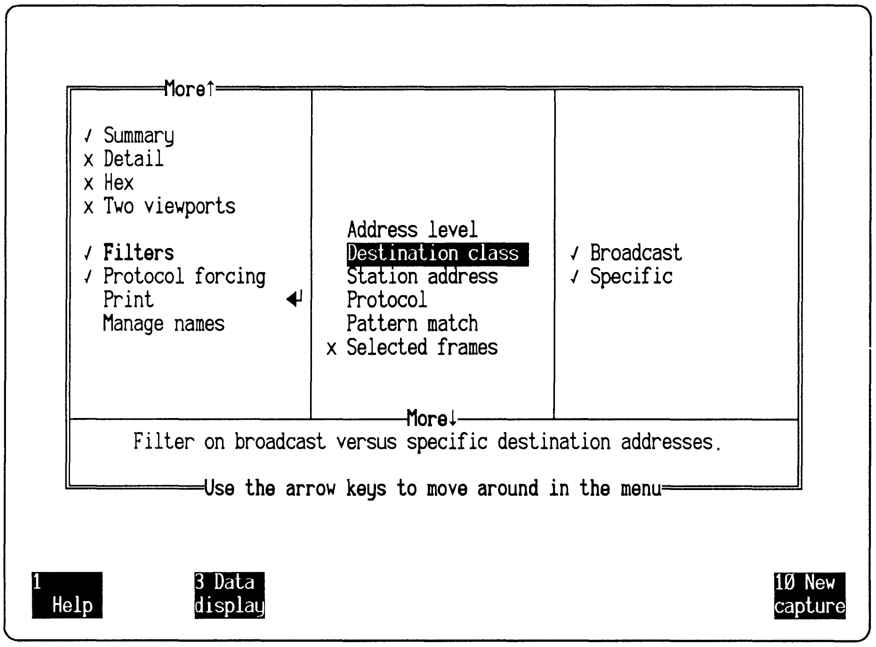
The effect on the displayed frames depends on the display options you choose when defining the Summary view. If you enable the **All layers** option, any enabled protocols are shown, with the highest level on top. Unless you also enable the **DLC addresses** option, the address associated with the highest level protocol is shown. For more information, see "The Summary View Display Options" on page 4–22.

Destination Class Filter

During display, the **Destination class** filter lets you include or exclude messages addressed (at any level) to a broadcast destination[1] or to frames with specific addresses. Of course, if you exclude both options, there is nothing left to look at.

For each destination class you include (broadcast or specific), you can also specify the address level (or levels) to be included, as shown in Figure 4–4. The default is all address levels enabled, so that the **Destination class** filter accepts all frames. Note that the Sniffer analyzer accepts a frame if it includes the desired type of address at *any* of the levels that are enabled.

Figure 4–5 shows the two options associated with the **Destination class** display filter. The default is both options enabled (√).



Filter on broadcast versus specific destination addresses.

Figure 4–5. Specifying the Destination class display filter.

To set a destination class display filter:

1. Move to **Display\Filters\Destination class.**

[1] During capture, however, the Sniffer analyzer can filter for broadcast addresses only at the DLC level.

2. Move to **Broadcast** or **Specific**. Press Spacebar to enable (√) or disable (x) those options.
3. If you enabled the **Broadcast** option, press Enter and make sure the desired address levels for the **Broadcast** option are enabled or disabled. To enable or disable an address level, move to the desired levels and press Spacebar.
4. Similarly, if you enabled the **Specific** option, make sure the desired address levels for the **Specific** option are enabled or disabled. Note that, although the two lists contain the same address levels, your selections of **Broadcast** addresses are independent of those for **Specific** addresses.

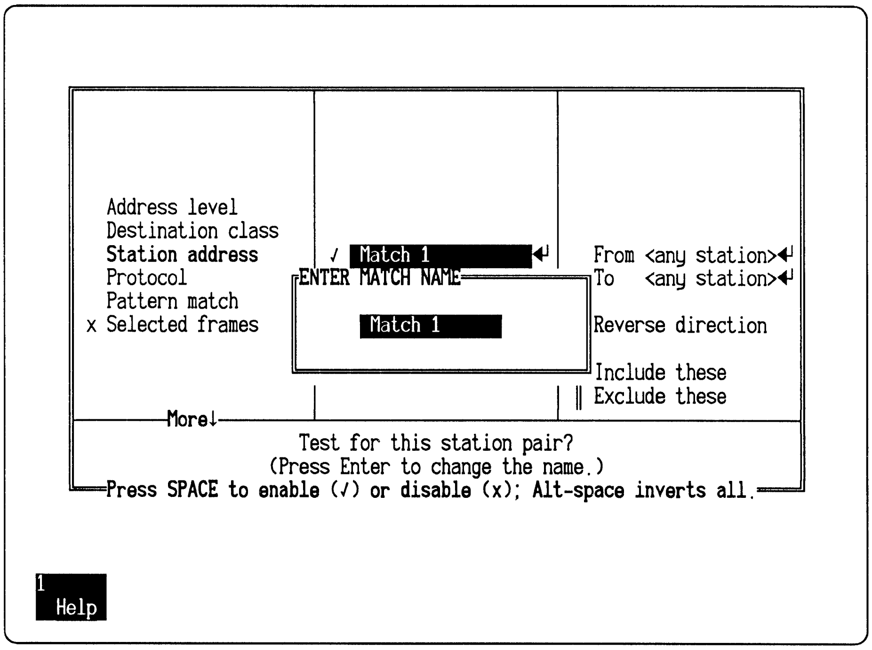
Station Address Display Filter

A **Station address filter** consists of some logical combination of up to four matches, which consist of four pairs of addresses. Address filters for display work just like address filters for capture, but with one important difference. During display, the addresses you specify can be at any level recognized by the protocol interpreters. By contrast, a capture filter can only filter for low-level addresses.

The procedure for setting an address filter for display is similar to the procedure for setting an address filter for capture, as described in "Defining the Station Address Filters" on page 3–35.

To set a station address filter for display:

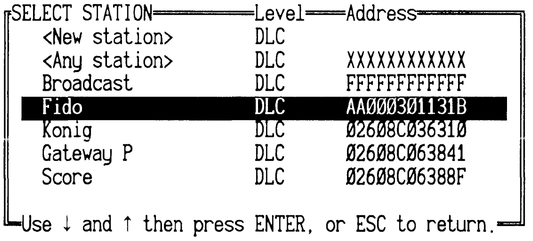
1. Move to **Capture filters\Station address\Match 1.**
2. If you want to name this match, press Enter. In the dialog box that appears (shown in Figure 4–6), type a name and press Enter.



```
  Address level
  Destination class
  Station address      ✓ Match 1         ↵   From <any station>↵
  Protocol            ENTER MATCH NAME         To   <any station>↵
  Pattern match
x Selected frames         Match 1              Reverse direction

                                               Include these
                                             ‖ Exclude these
            More↓
                    Test for this station pair?
                   (Press Enter to change the name.)
     Press SPACE to enable (✓) or disable (x); Alt-space inverts all.

1
 Help
```

Figure 4–6. Naming a station address filter match.

3. To specify a source address, move to **From** and press Enter. In the table that appears (shown in Figure 4–7), move to the desired station and press Enter. (If you enabled the **DLC addresses** option in the **Display\Summary** menu, the DLC address is automatically highlighted. If that option is disabled (the default) the highest level address is highlighted.)

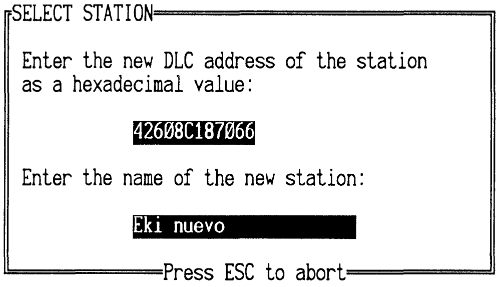


```
SELECT STATION              Level   Address
  <New station>             DLC
  <Any station>             DLC     XXXXXXXXXXXX
  Broadcast                 DLC     FFFFFFFFFFFF
  Fido                      DLC     AAØØØ3Ø1131B
  Konig                     DLC     Ø26Ø8CØ3631Ø
  Gateway P                 DLC     Ø26Ø8CØ63841
  Score                     DLC     Ø26Ø8CØ6388F

Use ↓ and ↑ then press ENTER, or ESC to return.
```

Figure 4–7. Selecting a station as a station address filter.

Note that the address—either its name, if it has one, or the numeric address—replaces **<any station>** in the **From** menu item.

4. If the address you want isn't in the table, move to the top of the screen, to the **<New station>** item that matches the desired address level and press Enter. In the dialog box that appears, type a new address and a corresponding name and press Enter. Figure 4–8 shows the dialog box for entering a new station.



```
SELECT STATION

Enter the new DLC address of the station
as a hexadecimal value:

          426Ø8C187Ø66

Enter the name of the new station:

          Eki nuevo

              Press ESC to abort
```

Figure 4–8. Defining a new station as a station address filter.

5. To specify a destination address, move to **To** and press Enter. Repeat the instructions in step 3 for selecting an address. The DLC address is automatically highlighted if you enabled the **DLC addresses** option in the **Display\Summary** menu. Otherwise, the highest level address is highlighted.

6. To specify whether this match also applies to traffic in the reverse direction, move to **Reverse direction** and press Spacebar to enable (√) the option.

7. To specify whether to include or exclude frames identified by this match, move to either **Include these** or **Exclude these** and press Spacebar to select the option you want.

   ▸Include these
   Exclude these

8. Repeat steps 1 through 7 for up to four matches.

9. To specify what to do with frames not covered by the matches, move to **Others** and either to **Include** or **Exclude**. Press Spacebar to specify the desired option.

Considerations when Setting Address Filters

When capturing, address filters are limited to matching DLC addresses. When displaying, address filters allow for higher level addresses as well. However, several considerations apply to both modes:

- Using fewer than four address matches
- Disabling defined address matches
- Taking advantage of the address match order

For additional information about these topics, see "Defining Station Address Matches: Some Considerations" on page 3–34.

Adding Addresses to the Name Table

If the address you want is not in the name table, you must add it to the table before you can select it as an address filter.

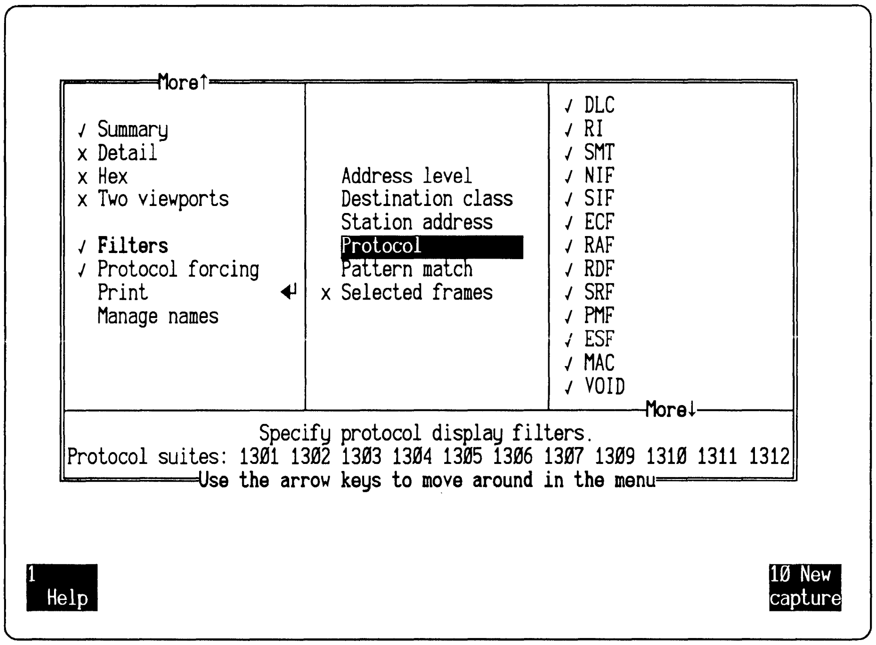
To facilitate this process, you can capture traffic that includes the addresses for which you want to filter and then display the results. In response, the Sniffer analyzer adds detected addresses to the top of the name table. You can then name them manually, if you want, to save them permanently. For more information about using the name table, see "Assigning Names to Addresses" on page 5–6.

Protocol Display Filter

In contrast to the **Protocol** capture filter, which filters on the particular SAP or at the DLC level, the **Protocol** display filter can filter for any of the protocols recognized by the protocol interpreters. The default is to accept every protocol.

When you move to the **Protocol** option, the panel to the right displays a list of protocols, shown in Figure 4–9. Note that, because this list includes higher-level protocols, it is much longer than the list associated with the capture filters. Beside each name, a √ indicates that the display filter will display that protocol, an x that it won't. The filter accepts a frame in the display when it contains *any* of the protocols you enable.

Note: The SNMP display filter is not effective when the SNMP contains ASN.1.



```
═══════════More↑══════════════════════════════════════════════════
                                                 √ DLC
 √ Summary                                       √ RI
 x Detail                                        √ SMT
 x Hex                   Address level           √ NIF
 x Two viewports         Destination class       √ SIF
                         Station address         √ ECF
 √ Filters               Protocol                √ RAF
 √ Protocol forcing      Pattern match           √ RDF
   Print            ↵  x Selected frames         √ SRF
   Manage names                                  √ PMF
                                                 √ ESF
                                                 √ MAC
                                                 √ VOID
                                              ──────More↓──────
              Specify protocol display filters.
Protocol suites: 1301 1302 1303 1304 1305 1306 1307 1309 1310 1311 1312
═══════════Use the arrow keys to move around in the menu═══════════

1                                                              10 New
 Help                                                          capture
```

Figure 4–9. Specifying the Protocol display filters.

To define the Protocol display filters:

1. Move to **Display\Filters\Protocol**.
2. In the associated list, move to any protocols you want to disable and press Spacebar (x).

To enable only one protocol filter:

By default, all protocols are enabled. You can use the following shortcut to enable just one—or a few— protocols.

1. Press Alt-Spacebar to disable all protocols (x).
2. Move to the protocol you want to enable and press Spacebar (√).

Pattern Match Display Filter

A pattern is a particular sequence of bits within a frame (specified in hex or binary code, or as ASCII text). In a simple pattern, the bits occur at just one location. In a complex pattern, a set of up to eight simple component patterns is linked with AND/OR logic.

The considerations related to defining a pattern match as a display filter are the same as for defining such a pattern as a capture filter. For complete information on pattern matching, see "Four Contexts for Pattern Matching" on page 3–39.

To set up a pattern match filter for display:

1. Move to **Display\Filters\Pattern match\Match 1.**
2. Follow the procedure "To define a pattern match for a capture filter:" on page 3–45, starting with step 2.

Selected Frames Display Filter

This filter works in conjunction with the "S" flag, which is applied to the highlighted frame during display if you press F9 (**Select frame**). By enabling the **Selected frames** display filter and disabling all other filters, you can create a file that contains just the frames you flagged and then save those frames as a file.

To filter only for selected frames:

1. In the **Summary** view, move to the frames you want to select and press F9 (**Select frame**).
2. Move to **Display\Filters\Selected frames** and press Spacebar to enable (√) the option.
3. Disable all other **Display\Filters** options.
4. Press F3 (**Data display**) to display the frames.

To save selected frames to disk:

1. Move to **Files\Save\Data** and press Spacebar to enable (√) the **Filtered only** option.
2. Press Enter. In the dialog box that appears, name the file that contains the selected frames.

Filters for Defective Frames

On Ethernet, StarLAN, and PC Network Sniffer analyzers, you can filter frames for either the presence or absence of certain defects. This ability is available only if the adapter card retains defective frames and passes them to the Sniffer analyzer's CPU. On token ring, FDDI, and WAN/Synchronous networks, the adapter card does not pass defective frames to the Sniffer analyzer.

The breakdown for good and defective frames includes:

- Good frames that contain none of the detected defects.
- Bad CRC frames, which include frames found to be defective by the CRC.
- Short frames, which include frames shorter than 60 byte (runts).
- Collision frames (Ethernet-II only), which indicate collisions.

For more information about how defective frames are counted and flagged, see "How the Defective Frames Filters Work (Ethernet)" on page 3–50.

To set filters for good frames or for frame defects:

1. Move to **Display\Filters** and then to the defect category for which you want to filter.
2. Press Spacebar to enable or disable the desired options.

√ Good frames
√ Bad CRC frames
√ Short frames
√ Collision frames (Ethernet-II only)

Disabling the Display Filters

If you find that the frames that interest you are not displayed, you might suspect that a display filter is eliminating those frames. By temporarily disabling the display filters, you can determine whether or not the display filters are removing the frames that interest you from the display.

There are two ways to disable the display filters you selected:

- Disabling the **Display\Filters** option
- Using the **Use defaults** option

By disabling the **Display filters** option, you *temporarily* disable all display filters. This allows you to display all the frames in the capture buffer to make sure the frames of interest were captured, without having to disable individual filters you may have spent considerable time setting up. After examining the display without the filters, you can fine-tune your display filters.

To temporarily disable all selected display filters:

1. Move to **Display\Filters** and press Spacebar to disable (x) the option.

If you choose the **Use defaults** option, all selected display filters *and* all other options are reset to the factory default settings. Because you may have spent considerable time defining various options, *do not* use the **Use defaults** option unless you want to start over again, using the factory defaults.

Note: You can also use the **Files\Save\Setups** option to save the current configuration of options (including the display filters) to a file and then apply those options to other captures.

Displaying Interpreted Frames

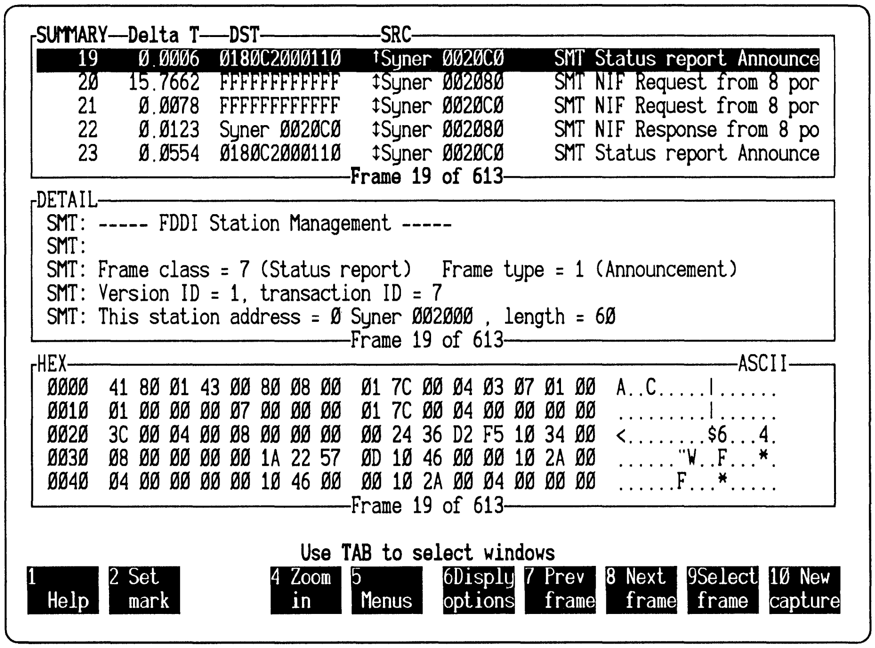
After frames are captured and stored in the capture buffer, you can use the **Display** command to start the interpretation. Those frames that pass the display filters are processed by the protocol interpreters, which decode the various protocol layers embedded in each frame. Although the lowest level protocols are interpreted automatically depending on your network, separate protocol interpreter suites interpret higher-level protocols by first dissecting each frame into its component layers and then decoding each layer according to its protocol.

The Display Options: An Overview

Depending on which display options you enable, you can show the results of the interpretation in one or more of the following views:

- **Expert** view, which shows network objects, symptoms, and diagnoses indentified by the Expert analyzer. See the *Expert Sniffer Network Analyzer Operations* manual for details.
- **Summary** view, which shows either a one-line summary of each frame or several lines, with one for each enabled protocol level within a frame.
- **Detail** view, which shows the contents of the interpreted protocols within the frame, including the fields and parameters within each protocol. Since a low-level frame may contain higher-level frames, a single frame may require several levels of interpretation.
- **Hexadecimal** view, which shows all bytes within the frame to provide a record of the received data. Depending on the network, you can choose either an ASCII or EBCDIC interpretation, or let the Sniffer analyzer adjust the interpretation automatically as needed.

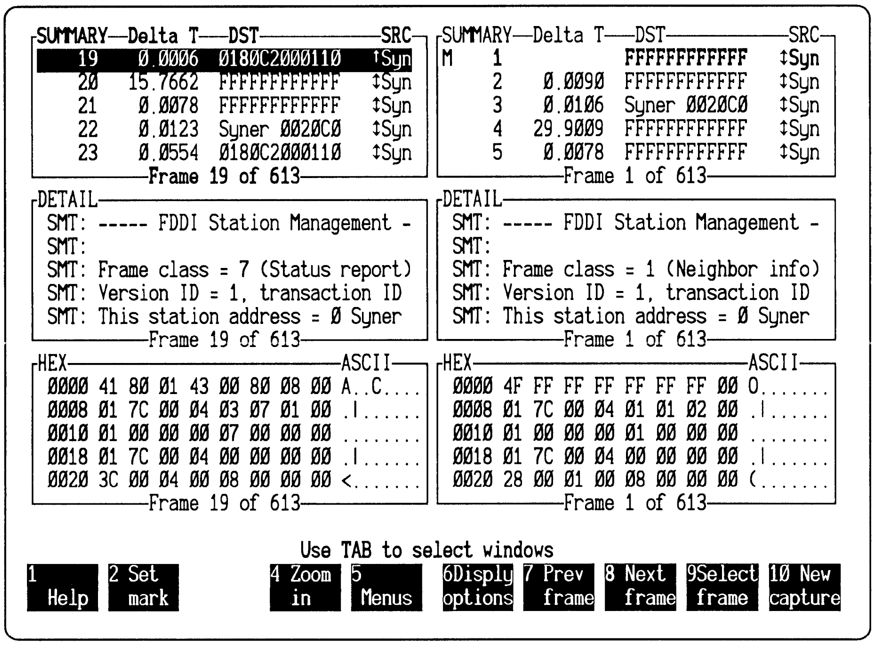
You can view the results of the interpretation of frames in the Summary, Detail, and Hexadecimal views, either individually or simultaneously. When you display more than one view, the Summary view is on top, the Detail view is in the middle, and the Hex view is at the bottom, as shown in Figure 4–10.



```
┌SUMMARY─Delta T──DST──────────SRC───────────────────────────────────
   19    Ø.ØØØ6  Ø18ØC2ØØØ11Ø  ↑Syner ØØ2ØCØ    SMT Status report Announce
   2Ø   15.7662  FFFFFFFFFFFF  ↕Syner ØØ2Ø8Ø    SMT NIF Request from 8 por
   21    Ø.ØØ78  FFFFFFFFFFFF  ↕Syner ØØ2ØCØ    SMT NIF Request from 8 por
   22    Ø.Ø123  Syner ØØ2ØCØ  ↕Syner ØØ2Ø8Ø    SMT NIF Response from 8 po
   23    Ø.Ø554  Ø18ØC2ØØØ11Ø  ↕Syner ØØ2ØCØ    SMT Status report Announce
───────────────────────────────Frame 19 of 613──────────────────────
┌DETAIL──────────────────────────────────────────────────────────────
 SMT: ----- FDDI Station Management -----
 SMT:
 SMT: Frame class = 7 (Status report)   Frame type = 1 (Announcement)
 SMT: Version ID = 1, transaction ID = 7
 SMT: This station address = Ø Syner ØØ2ØØØ , length = 6Ø
───────────────────────────────Frame 19 of 613──────────────────────
┌HEX──────────────────────────────────────────────────────ASCII─────
 ØØØØ  41 8Ø Ø1 43 ØØ 8Ø Ø8 ØØ  Ø1 7C ØØ Ø4 Ø3 Ø7 Ø1 ØØ  A..C.....|......
 ØØ1Ø  Ø1 ØØ ØØ ØØ Ø7 ØØ ØØ ØØ  Ø1 7C ØØ Ø4 ØØ ØØ ØØ ØØ  .........|......
 ØØ2Ø  3C ØØ Ø4 ØØ Ø8 ØØ ØØ ØØ  ØØ 24 36 D2 F5 1Ø 34 ØØ  <........$6...4.
 ØØ3Ø  Ø8 ØØ ØØ ØØ ØØ 1A 22 57  ØD 1Ø 46 ØØ ØØ 1Ø 2A ØØ  ......"W..F...*.
 ØØ4Ø  Ø4 ØØ ØØ ØØ ØØ 1Ø 46 ØØ  ØØ 1Ø 2A ØØ Ø4 ØØ ØØ ØØ  ......F...*.....
───────────────────────────────Frame 19 of 613──────────────────────

                          Use TAB to select windows
```

Figure 4–10. Displaying interpreted frames in all three views.

In general, all displayed views focus on a single frame. However, by using the **Two viewports** option, you can also look at two different frames simultaneously, in up to six different views (Figure 4–11).



```
SUMMARY—Delta T——DST——————————SRC—   SUMMARY—Delta T——DST——————————SRC—
   19    Ø.ØØØ6  Ø18ØC2ØØØ11Ø  ↑Syn   M    1           FFFFFFFFFFFF  ↕Syn
   2Ø   15.7662  FFFFFFFFFFFF  ↕Syn        2   Ø.ØØ9Ø  FFFFFFFFFFFF  ↕Syn
   21    Ø.ØØ78  FFFFFFFFFFFF  ↕Syn        3   Ø.Ø1Ø6  Syner ØØ2ØCØ  ↕Syn
   22    Ø.Ø123  Syner ØØ2ØCØ  ↕Syn        4  29.9ØØ9  FFFFFFFFFFFF  ↕Syn
   23    Ø.Ø554  Ø18ØC2ØØØ11Ø  ↕Syn        5   Ø.ØØ78  FFFFFFFFFFFF  ↕Syn
———————————Frame 19 of 613—————————   ————————————Frame 1 of 613——————————
DETAIL—————————————————————————————   DETAIL——————————————————————————————
 SMT: ----- FDDI Station Management -  SMT: ----- FDDI Station Management -
 SMT:                                  SMT:
 SMT: Frame class = 7 (Status report)  SMT: Frame class = 1 (Neighbor info)
 SMT: Version ID = 1, transaction ID   SMT: Version ID = 1, transaction ID
 SMT: This station address = Ø Syner   SMT: This station address = Ø Syner
———————————Frame 19 of 613—————————   ————————————Frame 1 of 613——————————
HEX————————————————————————ASCII———   HEX————————————————————————ASCII————
 ØØØØ 41 8Ø Ø1 43 ØØ 8Ø Ø8 ØØ A..C....  ØØØØ 4F FF FF FF FF FF FF ØØ O.......
 ØØØ8 Ø1 7C ØØ Ø4 Ø3 Ø7 Ø1 ØØ .|......  ØØØ8 Ø1 7C ØØ Ø4 Ø1 Ø1 Ø2 ØØ .|......
 ØØ1Ø Ø1 ØØ ØØ ØØ Ø7 ØØ ØØ ØØ ........  ØØ1Ø Ø1 ØØ ØØ ØØ Ø1 ØØ ØØ ØØ ........
 ØØ18 Ø1 7C ØØ Ø4 ØØ ØØ ØØ ØØ .|......  ØØ18 Ø1 7C ØØ Ø4 ØØ ØØ ØØ ØØ .|......
 ØØ2Ø 3C ØØ Ø4 ØØ Ø8 ØØ ØØ ØØ <.......  ØØ2Ø 28 ØØ Ø1 ØØ Ø8 ØØ ØØ ØØ (.......
———————————Frame 19 of 613—————————   ————————————Frame 1 of 613——————————

                          Use TAB to select windows
```

Figure 4–11. Displaying interpreted frames with the Two viewports option.

What is displayed in the Summary and Hex views depends on the display options you select for those views, described later in "The Summary View Display Options" on page 4–22 and "The Hexadecimal View Display Options" on page 4–37. The Detail view always shows all known information for the current frame.

About the Use of Color

If you have a color monitor, each protocol layer is shown in a different color. Where possible, each layer is identified with one of the seven layers of the OSI model. However, because many protocols predate the OSI model, they may not neatly fit into this scheme.

Normal color displays use a blue background. Highlighted areas are identified by a light-blue background in the Summary and Detail views and a white background in the Hex view.

The colors associated with various network layers are shown in Figure 4–12.

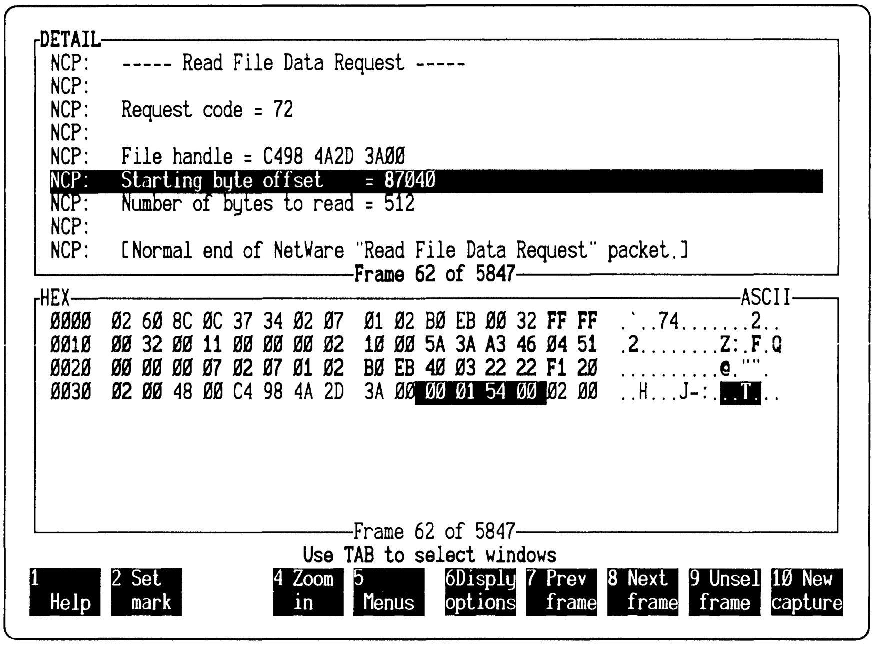
Protocol	Layer	Color
Physical level protocols	1	Magenta
Fragmentation protocols	1+	Red
Link level protocols	2	Brown
Network level protocols	3	Green
Transport level protocols	4	Yellow
Session level protocols	5	Light green
Presentation level protocols	6	Light cyan
Application level protocols	7-	Light red
Application level protocols II	7	Light magenta
Name protocols and network management layers		Cyan (blue-green)
Various protocol glue layers		Black
Other (SMT)		Light blue

Figure 4–12. Colors associated with protocol layers of the OSI model.

Scrolling within the Display Views

Information that is not visible on the screen can be reached by scrolling. For faster techniques, see "Searching for Frames" on page 4–41.

If you scroll to a frame within one view, all other displayed views also scroll to that frame automatically (see Figure 4–13). For example, if you scroll to highlight a particular frame in the Summary view, the first line pertaining to that frame is highlighted in the Detail view and the corresponding bytes are highlighted in the Hex view. In this way, it is easy to match a sequence of bytes with its interpretation.



```
DETAIL
 NCP:    ----- Read File Data Request -----
 NCP:
 NCP:    Request code = 72
 NCP:
 NCP:    File handle = C498 4A2D 3AØØ
 NCP:    Starting byte offset    = 87Ø4Ø
 NCP:    Number of bytes to read = 512
 NCP:
 NCP:    [Normal end of NetWare "Read File Data Request" packet.]
                               Frame 62 of 5847
HEX                                                              ASCII
 ØØØØ  Ø2 6Ø 8C ØC 37 34 Ø2 Ø7  Ø1 Ø2 BØ EB ØØ 32 FF FF  .`..74.......2..
 ØØ1Ø  ØØ 32 ØØ 11 ØØ ØØ ØØ Ø2  1Ø ØØ 5A 3A A3 46 Ø4 51  .2........Z:.F.Q
 ØØ2Ø  ØØ ØØ ØØ Ø7 Ø2 Ø7 Ø1 Ø2  BØ EB 4Ø Ø3 22 22 F1 2Ø  ..........@.""..
 ØØ3Ø  Ø2 ØØ 48 ØØ C4 98 4A 2D  3A ØØ ØØ Ø1 54 ØØ Ø2 ØØ  ..H...J-:...T...
                               Frame 62 of 5847
                            Use TAB to select windows
```

Figure 4–13. Synchronized scrolling in the display views.

If you enabled the **Two viewports** display option, which splits the screen into two independent viewports, you can scroll independently in each of the two viewports. Within each viewport, however, scrolling in one view automatically scrolls to the corresponding information in the other views.

Note: On an FDDI Sniffer Network Analyzer, performance delays may occur when scrolling through a large (up to 32 Mbyte) capture buffer with a display filter set. For example, you display an 18 Mbyte trace file in Summary, Detail, and Hex windows. You then set a protocol filter to look at SMT frames. If you are at the end of the buffer and press F7 (**Prev Frame**), a delay may occur while the analyzer filters through the large trace file for an SMT frame.

Moving between the Display Views

The view that contains the cursor is said to be *active*. This view is identified by a highlighted border (on a color monitor) or a contrasting color (on a monochrome monitor).

When all three views are open, the Summary view is active when you first press F3 (**Data display**). To make another view active, press Tab. To move in the reverse direction, press Shift Tab.

Enlarging a Display View

To enlarge the active view and obscure the others, press F4 (**Zoom in**). To return to the display of all views at the normal size, press F4 (**Zoom out**) again.

Compensation for Bit-Reversal in PC Network Addresses

The Sniffer analyzer for PC Network includes a capture option called **Flip DLC address**. This option changes the way in which bits within each byte of a DLC address are interpreted as characters, which, in turn, changes the address that is visible during display.

During transmission, PC Network follows the low-order-bit-first convention (like Ethernet). However, PC Network often runs software developed for token ring networks. In the computer, IBM software keeps a single representation of station addresses and uses it for both token ring and PC Network operations. This permits the software to keep just one table of DLC addresses, rather than one version for token ring and a separate version for PC Network. To permit a single address table to work despite different conventions for transmission, IBM software for PC Network reverses the bits within each of the 12 bytes that contain the DLC source and destination addresses. In this way, the transmission on the PC Network wire continues to match the IEEE assignment, and the computers linked by PC Network can use the same address tables as those linked by token ring.

To allow PC Network DLC addresses to match those of token ring, enabling the **Flip DLC address** option reverses the order of bits in the frame's source and destination address during capture, before the frame reaches the capture buffer. Thus, the value displayed depends on whether this option was enabled or disabled during capture. Note that the apparent difference in the DLC addresses affects the Summary, Detail, and Hex views.

Once you set the Sniffer analyzer to match a particular network, you do not need to change it further.

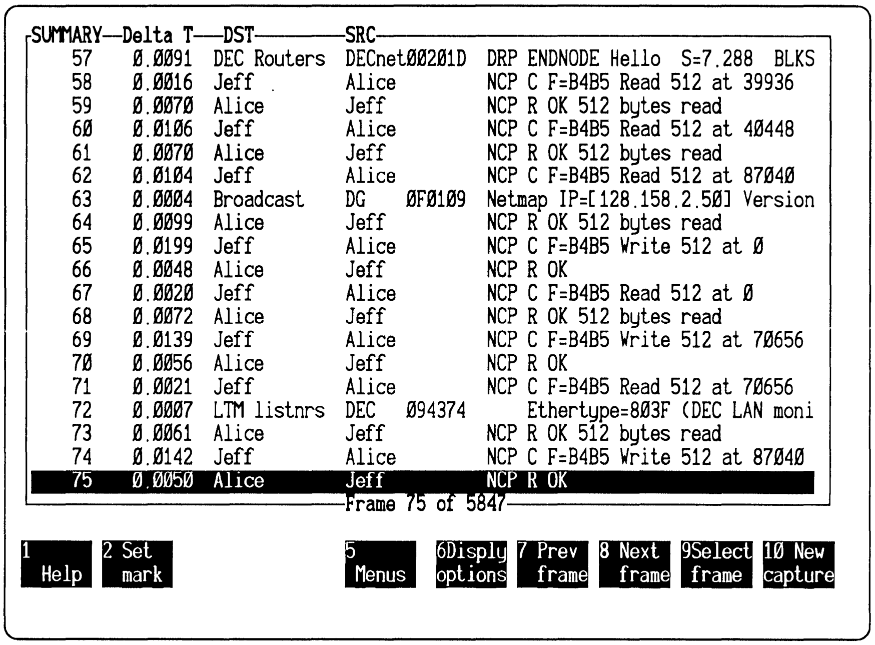
Compensation for Bit-Reversal in FDDI Networks

The Sniffer analyzer for FDDI networks includes **Show SMT addresses** and **Show LLC addresses** display options. These options change the way DLC addresses are displayed. in both the Summary and Detail views.

Activating the **Show SMT addresses** option displays all frame addresses in the canonical format rather than using the most significant bit (MSB) form to represent the 48-bit addresses. Using the **Show LLC addresses** displays all frame addresses in the MSB form.

The Summary View

The Summary view provides a condensed view of the captured frames (Figure 4–14). It is the only view that can show several frames at once. Each frame is reduced to a single line or a few lines (depending on whether the **Summary\All layers** is enabled). Although each frame is abbreviated and condensed, you can see the sequence and context of the frames at a glance. You can then examine individual frames in greater detail or skip over them.



```
SUMMARY—Delta T——DST————————SRC—————————————————————————————————————
   57    0.0091  DEC Routers  DECnet00201D  DRP ENDNODE Hello  S=7.288  BLKS
   58    0.0016  Jeff         Alice         NCP C F=B4B5 Read 512 at 39936
   59    0.0070  Alice        Jeff          NCP R OK 512 bytes read
   60    0.0106  Jeff         Alice         NCP C F=B4B5 Read 512 at 40448
   61    0.0070  Alice        Jeff          NCP R OK 512 bytes read
   62    0.0104  Jeff         Alice         NCP C F=B4B5 Read 512 at 87040
   63    0.0004  Broadcast    DG    0F0109  Netmap IP=[128.158.2.50] Version
   64    0.0099  Alice        Jeff          NCP R OK 512 bytes read
   65    0.0199  Jeff         Alice         NCP C F=B4B5 Write 512 at 0
   66    0.0048  Alice        Jeff          NCP R OK
   67    0.0020  Jeff         Alice         NCP C F=B4B5 Read 512 at 0
   68    0.0072  Alice        Jeff          NCP R OK 512 bytes read
   69    0.0139  Jeff         Alice         NCP C F=B4B5 Write 512 at 70656
   70    0.0056  Alice        Jeff          NCP R OK
   71    0.0021  Jeff         Alice         NCP C F=B4B5 Read 512 at 70656
   72    0.0007  LTM listnrs  DEC   094374     Ethertype=803F (DEC LAN moni
   73    0.0061  Alice        Jeff          NCP R OK 512 bytes read
   74    0.0142  Jeff         Alice         NCP C F=B4B5 Write 512 at 87040
   75    0.0050  Alice        Jeff          NCP R OK
————————————————————————————Frame 75 of 5847————————————————————————
```

Figure 4–14. Sample Summary view.

How information is displayed, and *how much* information is shown in the Summary view depends on which of the display options are enabled, as described in "The Summary View Display Options" on page 4–22.

Regardless of the display options, the Summary view always shows frame numbers and either station names (if the names correspond to addresses in the name table) or numeric addresses (if they do not). For information about maintaining the name table, see "Managing Names" on page 5–3.

Numeric Addresses in the Summary View

If a numeric address is shown, it appears in the conventional format for its type. For example, a DLC address is shown in hexadecimal, an IP address is shown as [n.n.n.n], and so on. On Ethernet or token ring, each station's DLC address contains six bytes, which are written as 12 hexadecimal digits. The default is to display the highest level protocol address.

To display other protocol addresses, you must enable the desired protocol levels in the **Address level** filter, as described in "Address Level Filter" on page 4–7. To display DLC addresses, you must enable the **DLC addresses** option.

On ARCNET, the first two bytes contain the source and destination. The next two bytes are shown as an integer representing the frame's total length. This is actually a simplification of what is actually transmitted on the network. ARCNET uses two different formats; one for short frames and another for long frames. A short frame has a 1-byte length. A particular value in the first byte means that a second byte is present. (As a side effect of this implementation, certain frame lengths are illegal.) The Sniffer analyzer evaluates the length according to the ARCNET convention. However, it records all frames in the same format, using a 2-byte length field.

The analyzer replaces the one or two bytes that were actually transmitted with a standard 2-byte representation. In this respect, what the analyzer records is not an exact replica of the transmission. However, it greatly simplifies the task of pattern matching, since the data field starts at the same offset in all recorded ARCNET frames.

Display of Manufacturer IDs

Where a 6-byte DLC address is shown, the analyzer attempts to interpret the first three bytes as the name of the manufacturer of the adapter card. If the manufacturer's code is in the manufacturer's table, that code replaces the first six characters of the station address with an ASCII abbreviation of the manufacturer's name.

Note: The file that contains the names for manufacturer IDs is named STARTUP.*xx*D (where *xx* is a two-letter network abbreviation, such as TR or EN). For an overview of this table, see Figure 9–8 on page 9–14.

Name Width Display Option

You can define the width of the name field in the summary view, from 6 characters up to 31 characters (the default is 15 characters). For example, if you use long names, you may want to make the name field wider to accommodate the names. This option also affects the Expert view. See the *Expert Sniffer Network Analyzer Operations* manual for details.

On ARCNET or LocalTalk, a DLC address consists of a single byte. On Ethernet, StarLAN, PC Network, or token ring, each station's address contains six bytes, which can be written as 12 hexadecimal digits.

If the display includes a name longer than the specified name width, the Sniffer analyzer truncates that name and replaces its last two visible characters with dots (to show that the name has been truncated). For example, if the **Name width** option specifies an 8-character field and you enter the 10-character name "**FileServer**," the Summary view would show "**FileSe..**"

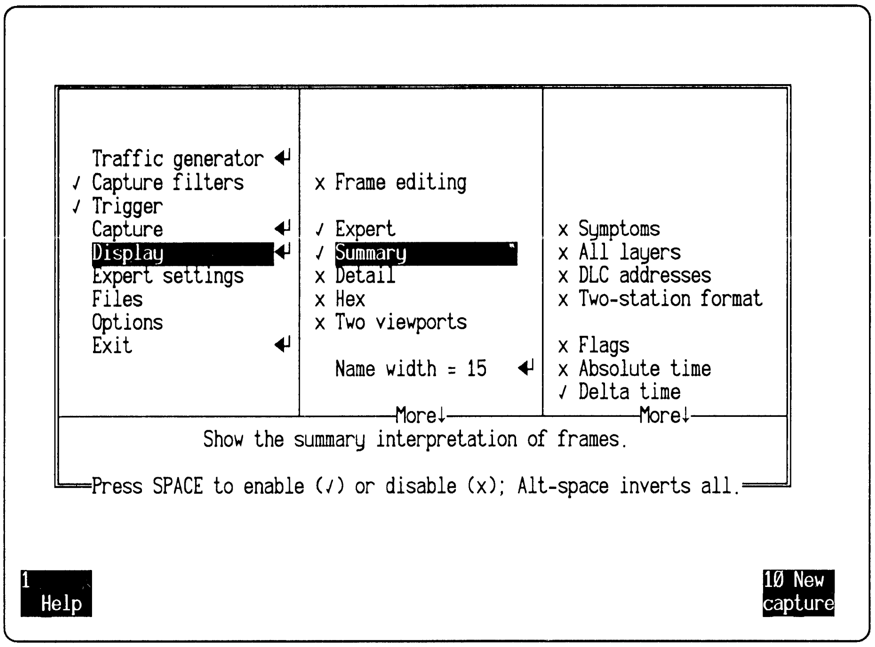
To define the Name width option:

1. Move to **Display\Name width=** and press Enter.
2. In the dialog box that appears, enter the desired name width.

The Summary View Display Options

Figure 4–15 provides an overview of the default Summary view display options. As you can see, all options are disabled except the **Delta time** option. These options would result in a display similar to Figure 4–14. Note that, if you enabled all the options, you would have to scroll horizontally to see all of the resulting display. If you use a larger, external screen, you may be able to display more rows or columns.

Note: For ARCNET, you can also choose between displaying addresses as Hex or Octal values.



```
  Traffic generator ↵
✓ Capture filters      x Frame editing
✓ Trigger
  Capture         ↵    ✓ Expert                x Symptoms
  Display         ↵    ✓ Summary               x All layers
  Expert settings      x Detail                x DLC addresses
  Files                x Hex                   x Two-station format
  Options              x Two viewports
  Exit            ↵                            x Flags
                         Name width = 15   ↵   x Absolute time
                                               ✓ Delta time
                       ————————More↓———————————————More↓———
              Show the summary interpretation of frames.

══Press SPACE to enable (✓) or disable (x); Alt-space inverts all.══

1                                                            10 New
  Help                                                       capture
```

Figure 4–15. The Summary view display options.

The first four display options determine *how* information is displayed. The sections that follow describe each option in more detail.

Symptoms If enabled, the summary view shows the last symptom found (if any) for each frame. See the *Expert Sniffer Network Analyzer Operations* manual for details on symptoms.

All layers If enabled, the Summary view shows one line for each protocol level contained in a frame. If disabled, only one line—for the highest enabled protocol level—is shown. The default is **All layers** disabled (x).

DLC addresses If enabled, the Summary view shows the DLC address for each displayed frame, even if several protocol levels are shown (**All layers** enabled). If disabled, the address associated with the highest level protocol is shown. The default is **DLC addresses** disabled (x).

Two-station format If enabled, displays only traffic between two stations.

The rest of the display options determine *whethe*r each of the following is displayed. The default is all options disabled, except for **Delta time**.

Flags Shows flags associated with a frame.

Absolute time Shows when the frame was received.

Delta time Shows the interval between the current frame and the previous frame.

Relative time Shows the interval between the current frame and the marked frame.

Bytes Shows the frame's length.

Cumulative bytes Shows the length of all frames, starting with the marked frame and including the current frame.

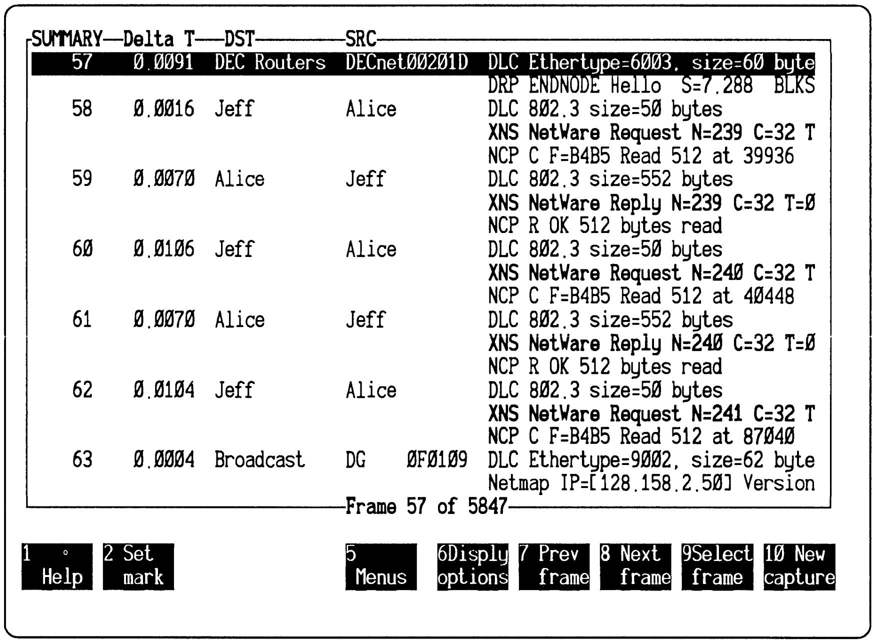
NW utilization Shows an estimate of the percentage of the network's bandwidth devoted to transmitting the displayed frame.

All Layers Display Option

This option determines whether the Summary view shows a single line that identifies only the frame's highest protocol level or whether it shows a separate line for each interpreted protocol level[1]. If you disable the **All layers** option, the lowest level appears on top of the others. How addresses appear also depends on the **DLC addresses** option. If that option is disabled, the address associated with the highest level is automatically shown. On a color monitor, each level is color coded (see "About the Use of Color" on page 4–17).

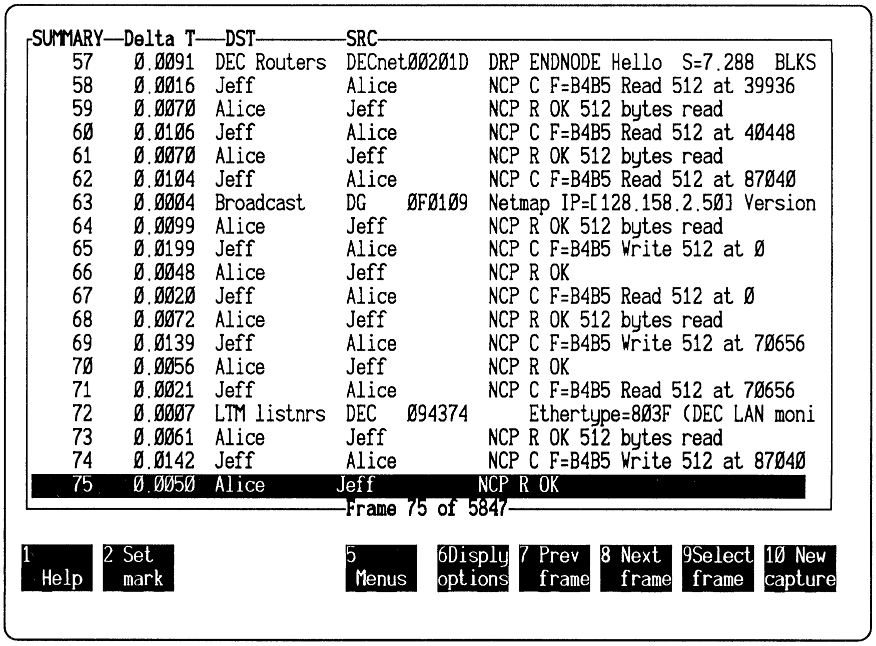
Figure 4–16 shows a Summary view that resulted from enabling both the **All layers** and the **DLC addresses** options. Figure 4–17 shows a view with the **All layers** and **DLC addresses** options disabled.

[1] In X Windows, there is a separate line for each protocol of each message within the frame.



```
SUMMARY—Delta T——DST————————SRC——————————————————————————————————————
    57    0.0091  DEC Routers  DECnet00201D  DLC Ethertype=6003, size=60 byte
                                             DRP ENDNODE Hello  S=7.288  BLKS
    58    0.0016  Jeff         Alice         DLC 802.3 size=50 bytes
                                             XNS NetWare Request N=239 C=32 T
                                             NCP C F=B4B5 Read 512 at 39936
    59    0.0070  Alice        Jeff          DLC 802.3 size=552 bytes
                                             XNS NetWare Reply N=239 C=32 T=0
                                             NCP R OK 512 bytes read
    60    0.0106  Jeff         Alice         DLC 802.3 size=50 bytes
                                             XNS NetWare Request N=240 C=32 T
                                             NCP C F=B4B5 Read 512 at 40448
    61    0.0070  Alice        Jeff          DLC 802.3 size=552 bytes
                                             XNS NetWare Reply N=240 C=32 T=0
                                             NCP R OK 512 bytes read
    62    0.0104  Jeff         Alice         DLC 802.3 size=50 bytes
                                             XNS NetWare Request N=241 C=32 T
                                             NCP C F=B4B5 Read 512 at 87040
    63    0.0004  Broadcast    DG    0F0109  DLC Ethertype=9002, size=62 byte
                                             Netmap IP=[128.158.2.50] Version
————————————————————————————————————Frame 57 of 5847—————————————————
```

Figure 4–16. Summary view, All layers and DLC addresses enabled.



```
SUMMARY—Delta T——DST————————SRC——————————————————————————————————————
    57    0.0091  DEC Routers  DECnet00201D  DRP ENDNODE Hello  S=7.288  BLKS
    58    0.0016  Jeff         Alice         NCP C F=B4B5 Read 512 at 39936
    59    0.0070  Alice        Jeff          NCP R OK 512 bytes read
    60    0.0106  Jeff         Alice         NCP C F=B4B5 Read 512 at 40448
    61    0.0070  Alice        Jeff          NCP R OK 512 bytes read
    62    0.0104  Jeff         Alice         NCP C F=B4B5 Read 512 at 87040
    63    0.0004  Broadcast    DG    0F0109  Netmap IP=[128.158.2.50] Version
    64    0.0099  Alice        Jeff          NCP R OK 512 bytes read
    65    0.0199  Jeff         Alice         NCP C F=B4B5 Write 512 at 0
    66    0.0048  Alice        Jeff          NCP R OK
    67    0.0020  Jeff         Alice         NCP C F=B4B5 Read 512 at 0
    68    0.0072  Alice        Jeff          NCP R OK 512 bytes read
    69    0.0139  Jeff         Alice         NCP C F=B4B5 Write 512 at 70656
    70    0.0056  Alice        Jeff          NCP R OK
    71    0.0021  Jeff         Alice         NCP C F=B4B5 Read 512 at 70656
    72    0.0007  LTM listnrs  DEC   094374     Ethertype=803F (DEC LAN moni
    73    0.0061  Alice        Jeff          NCP R OK 512 bytes read
    74    0.0142  Jeff         Alice         NCP C F=B4B5 Write 512 at 87040
    75    0.0050  Alice        Jeff          NCP R OK
————————————————————————————————————Frame 75 of 5847—————————————————
```

Figure 4–17. Summary view, All layers and DLC addresses disabled.

To define the displayed protocol levels in Summary view:

1. Move to **Display\Summary\All layers**. Press Spacebar to enable (√) or disable (x) the option.

DLC Addresses Display Option

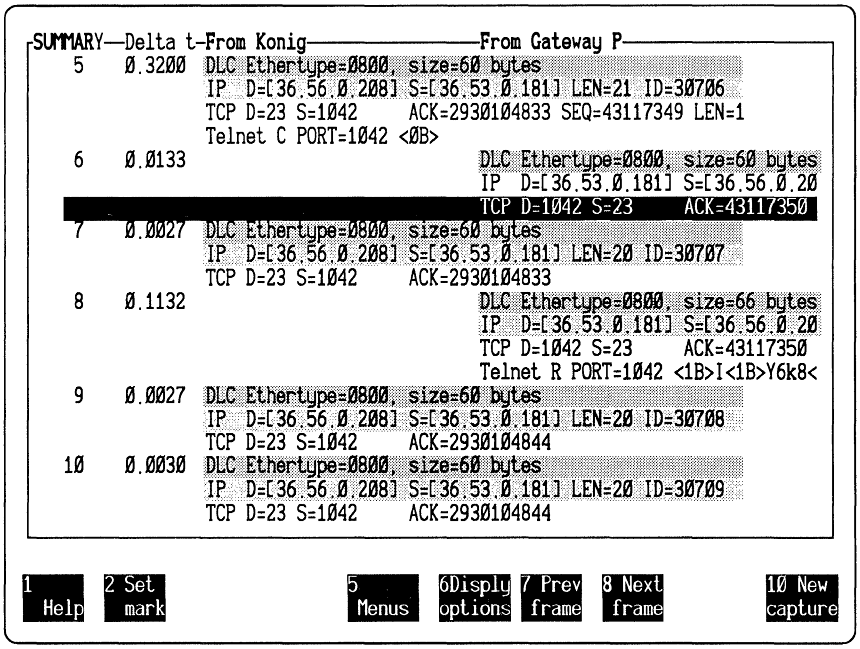
This option determines whether the DLC address or the address associated with the highest level protocol is shown in the Summary view. If the option is disabled, the highest level address is shown. If it is enabled, the DLC address is shown even if you display all protocol layers. Figure 4–17, for example, shows the highest layer—the result of disabling the **DLC addresses** option.

Two-Station Format Display Option

When you examine network activity, you often want to focus on traffic between a pair of stations. To do this, you can set up filters that define the two stations (see "Station Address Display Filter" on page 4–10) and enable the **Two-station format** option.

Note: If you do not set these filters, the Sniffer analyzer accepts other frames as well and displays those frames in the usual format. Since this is inconsistent with the two-station format, it makes the feature less useful.

The two-station format shows transmissions from one station (the station that was detected first) on the left side of the screen and transmissions from the other station on the right, as shown in Figure 4–18. Note that the source and destination fields are omitted. Instead, there are two columns, headed **From** *xxx* and **From** *yyy*. A frame from the station on the left is assumed be addressed to the station on the right, and vice versa.



```
SUMMARY—Delta t-From Konig—————————————————From Gateway P——————————————
    5    Ø.32ØØ  DLC Ethertype=Ø8ØØ, size=6Ø bytes
                 IP  D=[36.56.Ø.2Ø8] S=[36.53.Ø.181] LEN=21 ID=3Ø7Ø6
                 TCP D=23 S=1Ø42     ACK=293Ø1Ø4833 SEQ=43117349 LEN=1
                 Telnet C PORT=1Ø42 <ØB>
    6    Ø.Ø133                             DLC Ethertype=Ø8ØØ, size=6Ø bytes
                                            IP  D=[36.53.Ø.181] S=[36.56.Ø.2Ø
                                            TCP D=1Ø42 S=23     ACK=4311735Ø
    7    Ø.ØØ27  DLC Ethertype=Ø8ØØ, size=6Ø bytes
                 IP  D=[36.56.Ø.2Ø8] S=[36.53.Ø.181] LEN=2Ø ID=3Ø7Ø7
                 TCP D=23 S=1Ø42     ACK=293Ø1Ø4833
    8    Ø.1132                             DLC Ethertype=Ø8ØØ, size=66 bytes
                                            IP  D=[36.53.Ø.181] S=[36.56.Ø.2Ø
                                            TCP D=1Ø42 S=23     ACK=4311735Ø
                                            Telnet R PORT=1Ø42 <1B>I<1B>Y6k8<
    9    Ø.ØØ27  DLC Ethertype=Ø8ØØ, size=6Ø bytes
                 IP  D=[36.56.Ø.2Ø8] S=[36.53.Ø.181] LEN=2Ø ID=3Ø7Ø8
                 TCP D=23 S=1Ø42     ACK=293Ø1Ø4844
   1Ø    Ø.ØØ3Ø  DLC Ethertype=Ø8ØØ, size=6Ø bytes
                 IP  D=[36.56.Ø.2Ø8] S=[36.53.Ø.181] LEN=2Ø ID=3Ø7Ø9
                 TCP D=23 S=1Ø42     ACK=293Ø1Ø4844
```

Figure 4–18. Two-station format for the Summary view.

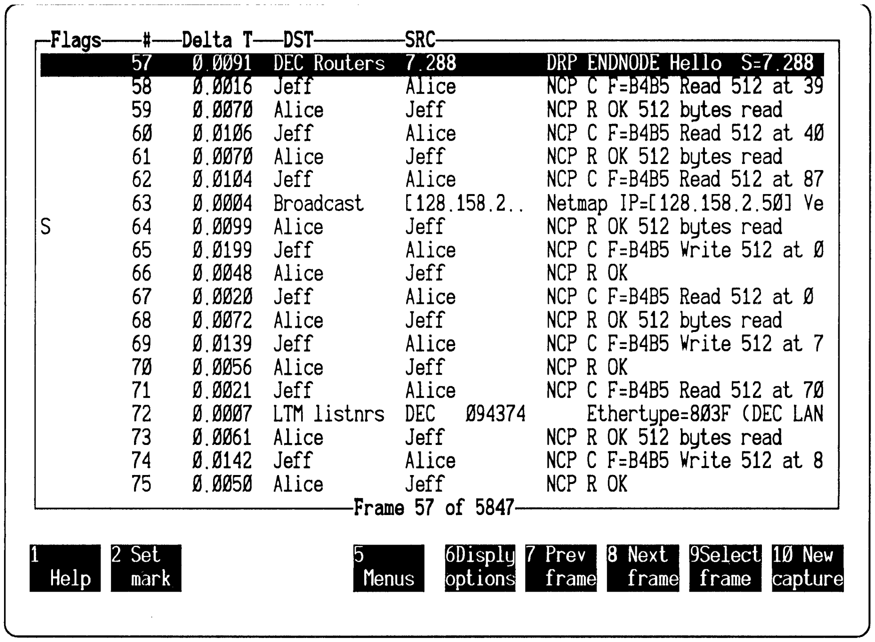
To use the two-station format:

1. Set the **Station address** filters to display only the two stations of interest.
2. Move to **Display\Summary\Two-Station Format** and press Spacebar to enable (√) the option.

3. To adjust the separation between the columns, change the **Name width** option.
4. To adjust the display's horizontal position, use the horizontal Cursor keys to scroll sideways.

Flags Display Option

If you enable the **Flags** option, the Sniffer analyzer displays, in the far left column, up to six of the flags associated with a frame. Figure 4–19, for example, shows the **Selected fram**e flag for frame 64.



```
Flags    #   Delta T   DST           SRC
         57  Ø.ØØ91  DEC Routers   7.288            DRP ENDNODE Hello  S=7.288
         58  Ø.ØØ16  Jeff          Alice            NCP C F=B4B5 Read 512 at 39
         59  Ø.ØØ7Ø  Alice         Jeff             NCP R OK 512 bytes read
         6Ø  Ø.Ø1Ø6  Jeff          Alice            NCP C F=B4B5 Read 512 at 4Ø
         61  Ø.ØØ7Ø  Alice         Jeff             NCP R OK 512 bytes read
         62  Ø.Ø1Ø4  Jeff          Alice            NCP C F=B4B5 Read 512 at 87
         63  Ø.ØØØ4  Broadcast     [128.158.2..     Netmap IP=[128.158.2.5Ø] Ve
S        64  Ø.ØØ99  Alice         Jeff             NCP R OK 512 bytes read
         65  Ø.Ø199  Jeff          Alice            NCP C F=B4B5 Write 512 at Ø
         66  Ø.ØØ48  Alice         Jeff             NCP R OK
         67  Ø.ØØ2Ø  Jeff          Alice            NCP C F=B4B5 Read 512 at Ø
         68  Ø.ØØ72  Alice         Jeff             NCP R OK 512 bytes read
         69  Ø.Ø139  Jeff          Alice            NCP C F=B4B5 Write 512 at 7
         7Ø  Ø.ØØ56  Alice         Jeff             NCP R OK
         71  Ø.ØØ21  Jeff          Alice            NCP C F=B4B5 Read 512 at 7Ø
         72  Ø.ØØØ7  LTM listnrs   DEC    Ø94374        Ethertype=8Ø3F (DEC LAN
         73  Ø.ØØ61  Alice         Jeff             NCP R OK 512 bytes read
         74  Ø.Ø142  Jeff          Alice            NCP C F=B4B5 Write 512 at 8
         75  Ø.ØØ5Ø  Alice         Jeff             NCP R OK
                                  Frame 57 of 5847
```

Figure 4–19. Displaying flags in the Summary view.

Note: Three of the flags listed below (M, E, and S) are displayed whether or not **Flags** is enabled. The remaining flags are displayed only if you enable the **Flags** option.

Flags include:

M Mark—the reference frame for relative time or cumulative bytes. To set the mark on the current frame, press F2 **(Set mark)**.

T Trigger—the frame defined as the trigger event, which contains the specified pattern that stops the capture.

↓ Protocol forced—the rules associated with the protocol forcing feature apply to this frame (see "Specifying a Protocol Forcing Rule" on page 6–3). If there are multiple arrows, each indicates one force (up to six recursions).

E Edited—this frame was edited.

S Selected frame—this frame was selected by the user. You can apply this flag to any frame by moving to the frame and then pressing F9 (**Select frames**). By also enabling the **Selected frames** display filter, you can collect all selected frames and save them to a file, as described in greater detail in "Selected Frames Display Filter" on page 4–14.

C CRC (Ethernet)— a frame whose CRC does not agree with the actual bytes received, which suggests that it contains invalid characters.

R Short/Runt (Ethernet)— a frame that is less than 60 bytes, which may indicate a collision.

L Lost frame (Ethernet)— the frames that preceded this frame reached the network interface card but were lost before they reached the capture buffer.

O Overrun (Ethernet)—the frame that preceded this frame was discarded because of an error during transfer from the network to the capture buffer. This may happen during high-volume traffic with small frames.

X Collision (Ethernet-II only)—the frame that preceded this frame is the result of a collision. This flag is applied only if the collision occurred after the frame's preamble.

A Abort— (WAN/Synchronous) the frames that immediately preceded this frame were aborted by the sender.

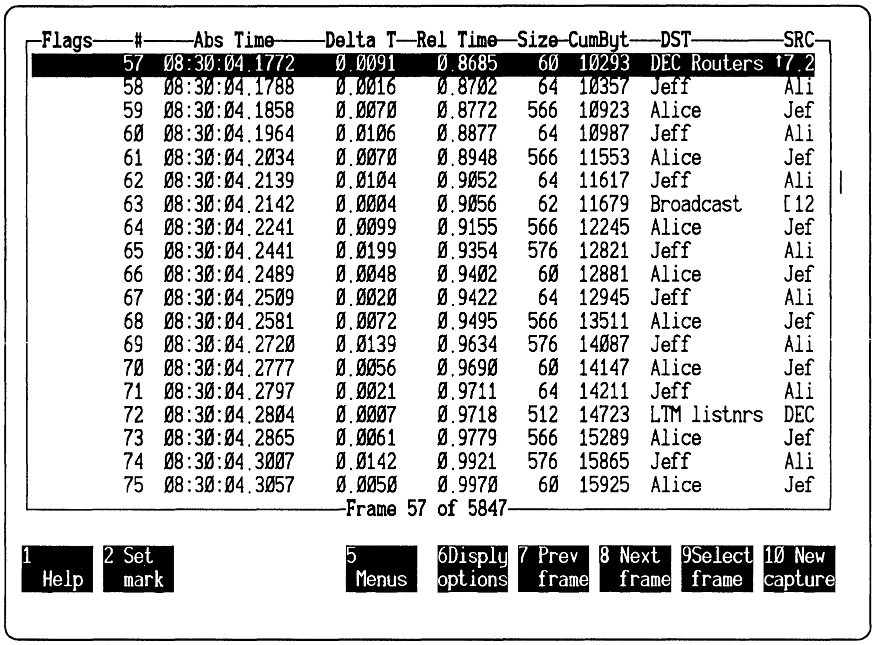
"Time" and "Volume" Display Options

To examine a network's throughput, you need to know about the volume and timing of transmissions. For every frame, you can include or omit various indicators of the time or the flow of data, including:

- Absolute time
- Delta time
- Relative time
- Bytes
- Cumulative bytes
- Network utilization

Figure 4–20 shows a Summary view with all options enabled.

Note: If you enable all the options, the display may be wider than the screen. If that happens, use the Cursor keys to scroll sideways to see the entire display.



```
Flags    #    Abs Time      Delta T  Rel Time Size CumByt  DST           SRC
        57  Ø8:3Ø:Ø4.1772   Ø.ØØ91   Ø.8685    6Ø  1Ø293  DEC Routers  ↑7.2
        58  Ø8:3Ø:Ø4.1788   Ø.ØØ16   Ø.87Ø2    64  1Ø357  Jeff          Ali
        59  Ø8:3Ø:Ø4.1858   Ø.ØØ7Ø   Ø.8772   566  1Ø923  Alice         Jef
        6Ø  Ø8:3Ø:Ø4.1964   Ø.Ø1Ø6   Ø.8877    64  1Ø987  Jeff          Ali
        61  Ø8:3Ø:Ø4.2Ø34   Ø.ØØ7Ø   Ø.8948   566  11553  Alice         Jef
        62  Ø8:3Ø:Ø4.2139   Ø.Ø1Ø4   Ø.9Ø52    64  11617  Jeff          Ali
        63  Ø8:3Ø:Ø4.2142   Ø.ØØØ4   Ø.9Ø56    62  11679  Broadcast     [12
        64  Ø8:3Ø:Ø4.2241   Ø.ØØ99   Ø.9155   566  12245  Alice         Jef
        65  Ø8:3Ø:Ø4.2441   Ø.Ø199   Ø.9354   576  12821  Jeff          Ali
        66  Ø8:3Ø:Ø4.2489   Ø.ØØ48   Ø.94Ø2    6Ø  12881  Alice         Jef
        67  Ø8:3Ø:Ø4.25Ø9   Ø.ØØ2Ø   Ø.9422    64  12945  Jeff          Ali
        68  Ø8:3Ø:Ø4.2581   Ø.ØØ72   Ø.9495   566  13511  Alice         Jef
        69  Ø8:3Ø:Ø4.272Ø   Ø.Ø139   Ø.9634   576  14Ø87  Jeff          Ali
        7Ø  Ø8:3Ø:Ø4.2777   Ø.ØØ56   Ø.969Ø    6Ø  14147  Alice         Jef
        71  Ø8:3Ø:Ø4.2797   Ø.ØØ21   Ø.9711    64  14211  Jeff          Ali
        72  Ø8:3Ø:Ø4.28Ø4   Ø.ØØØ7   Ø.9718   512  14723  LTM listnrs   DEC
        73  Ø8:3Ø:Ø4.2865   Ø.ØØ61   Ø.9779   566  15289  Alice         Jef
        74  Ø8:3Ø:Ø4.3ØØ7   Ø.Ø142   Ø.9921   576  15865  Jeff          Ali
        75  Ø8:3Ø:Ø4.3Ø57   Ø.ØØ5Ø   Ø.997Ø    6Ø  15925  Alice         Jef
                             Frame 57 of 5847
```

Figure 4–20. Displaying time and traffic volume information.

Absolute time

Absolute time shows when the last byte of a frame was received. At that time, the Sniffer analyzer attaches the timestamp based on its internal clock. All other time displays are based on this value. On networks other than token ring, **Absolute time** is displayed to the nearest tenth of a millisecond. On token ring, it is displayed to the nearest millisecond.

Absolute time also appears in the Detail view.

Delta time

Delta time shows the interval between the current frame's timestamp and that of the preceding frame. Because Delta time shows the interval to the preceding displayed frame, frames that are not displayed do not affect Delta time.

Note: You can use the **Frame editing** feature to change this value.

Relative time

Relative time shows the difference between the current frame's timestamp and the timestamp of the reference frame, which is marked with the "M" flag (see "Flags Display Option" on page 4–27). When you first display the buffer, the first frame is the marked frame.

You can set this flag by pressing F2 (**Set mark**) while the desired frame is highlighted. This removes the flag from the currently marked frame. Once you mark a reference frame, you can find it quickly (see "Jumping to the Marked Frame" on page 4–45).

Bytes

Bytes shows the total number of bytes in the frame, not including the CRC frame.

Cumulative bytes

Cumulative bytes shows the sum of the lengths of the displayed frames, from the reference frame (flagged "M") through the current frame (including both). If you did not redefine the reference frame, the Sniffer analyzer counts from the first displayed frame.

Note: You can choose to display *either* the **Cumulative bytes** *or* the **Network utilization** option. The Sniffer analyzer will not allow you to enable both options. Enabling one disables the other.

Network utilization

Network utilization shows an estimate of the percentage of the network's bandwidth devoted to transmitting the displayed frame (and perhaps those preceding and following it). The measurement is:

$$\frac{\textit{100} \times \textit{bytes in all frames accepted during the interval}}{\textit{Theoretical maximum that could be transmitted during the interval}}$$

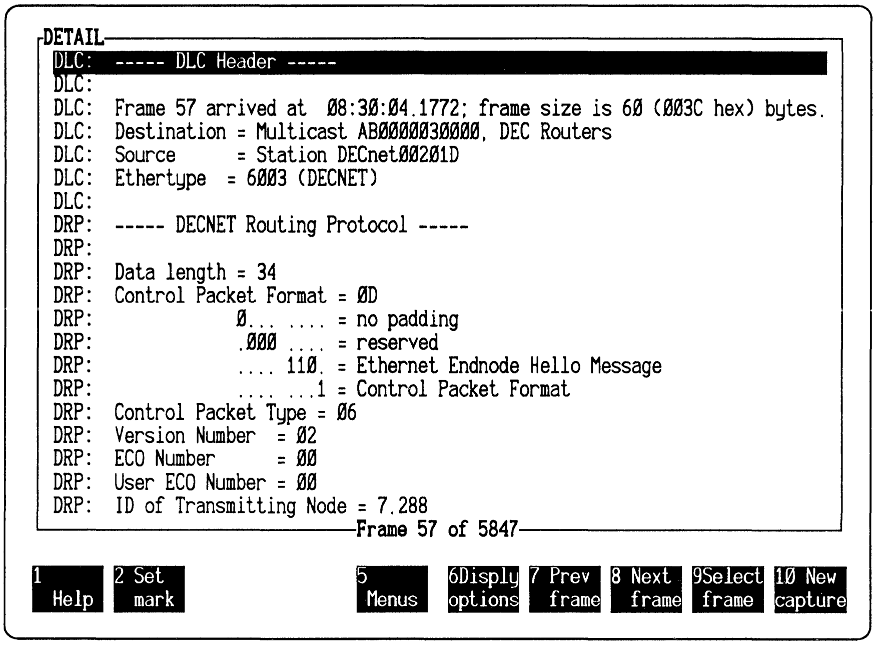
The interval is a time window centered around the frame. You can set the size of the interval to 1, 10, 100, or 1000 milliseconds. For example, if you pick 100 millisecond intervals, the utilization for a frame that arrived at 13:27:06.100 is based on the number of bytes in frames whose arrival times ranged from 13:27:06.050 to 13:27:06.150.

Utilization is a moving average. With a smaller interval, you'll see larger momentary fluctuations. A larger interval, however, smooths them out. Any measure of network utilization must be based on a time window, whether described explicitly or not. Viewed without window averaging, a network is always either 100 percent busy (when a frame is being transmitted) or 0 percent busy (when no frame is being transmitted).

The Detail View

The Detail view presents a complete interpretation of a frame for each field and the associated parameters. It also shows some information not contained within the frame, such as the absolute time, which shows when the frame arrived.

Figure 4–21 shows a sample Detail view.



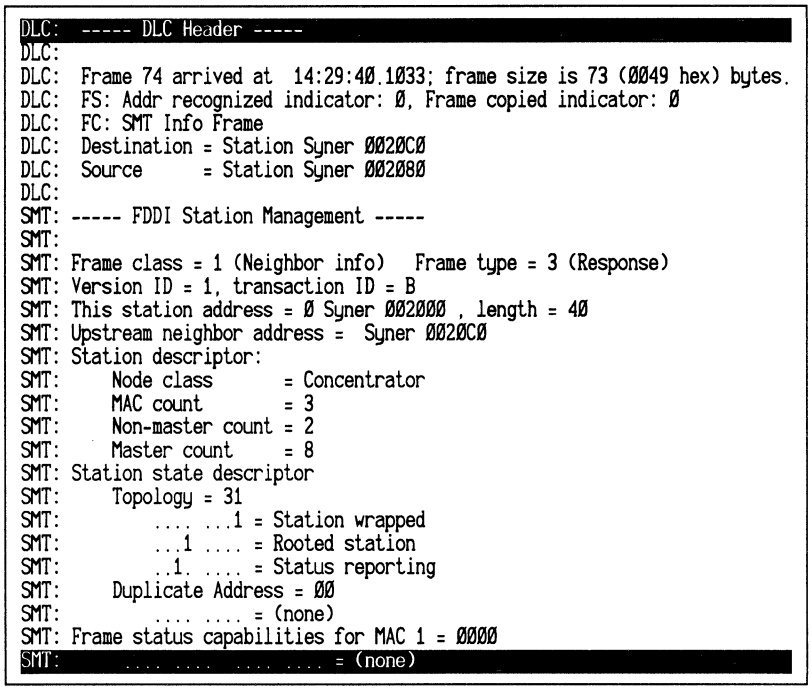
```
DETAIL
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 57 arrived at  08:30:04.1772; frame size is 60 (003C hex) bytes.
DLC:  Destination = Multicast AB0000030000, DEC Routers
DLC:  Source      = Station DECnet00201D
DLC:  Ethertype  = 6003 (DECNET)
DLC:
DRP:  ----- DECNET Routing Protocol -----
DRP:
DRP:  Data length = 34
DRP:  Control Packet Format = 0D
DRP:              0... .... = no padding
DRP:              .000 .... = reserved
DRP:              .... 110. = Ethernet Endnode Hello Message
DRP:              .... ...1 = Control Packet Format
DRP:  Control Packet Type = 06
DRP:  Version Number  = 02
DRP:  ECO Number      = 00
DRP:  User ECO Number = 00
DRP:  ID of Transmitting Node = 7.288
                              Frame 57 of 5847
```

Figure 4–21. Sample Detail view.

Because the Detail view includes so many lines, you can only see a partial view at any one time. The left margin shows which protocol governs that portion of the interpretation. To see another section of the view, you can scroll with the Cursor keys or use the **Search** function (see "Searching for Text" on page 4–42).

When you print the Detail view, the Sniffer analyzer prints the entire text of the open view (or views), regardless of screen boundaries.[1] Figure 4–22 provides an example of the Detail view as it appears when printed. Although this particular example is a TCP/IP frame transmitted over Ethernet, the general format is similar for any network. For information about printing, see "Printing and Importing Data" on page 4–46.

[1] Depending on how you configured your system, you can redirect printer output elsewhere.



```
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 74 arrived at  14:29:4Ø.1Ø33; frame size is 73 (ØØ49 hex) bytes.
DLC:  FS: Addr recognized indicator: Ø, Frame copied indicator: Ø
DLC:  FC: SMT Info Frame
DLC:  Destination = Station Syner ØØ2ØCØ
DLC:  Source      = Station Syner ØØ2Ø8Ø
DLC:
SMT: ----- FDDI Station Management -----
SMT:
SMT: Frame class = 1 (Neighbor info)   Frame type = 3 (Response)
SMT: Version ID = 1, transaction ID = B
SMT: This station address = Ø Syner ØØ2ØØØ , length = 4Ø
SMT: Upstream neighbor address =  Syner ØØ2ØCØ
SMT: Station descriptor:
SMT:     Node class       = Concentrator
SMT:     MAC count        = 3
SMT:     Non-master count = 2
SMT:     Master count     = 8
SMT: Station state descriptor
SMT:     Topology = 31
SMT:         .... ...1 = Station wrapped
SMT:         ...1 .... = Rooted station
SMT:         ..1. .... = Status reporting
SMT:     Duplicate Address = ØØ
SMT:         .... .... = (none)
SMT: Frame status capabilities for MAC 1 = ØØØØ
SMT:        .... ....  .... .... = (none)
```

Figure 4–22. Sample of complete Detail view information when printed.

Protocol Layers in the Detail View

When a frame contains several protocol layers, the Detail view interprets all the layers. The outermost (lowest) layer appears first, followed by any other layers until the innermost (highest) layer, which appears last.

Scrolling in the Detail View

Because the interpretation in the Detail view is often larger than the screen, you can scroll to see the entire display.

When both the Summary and Detail views are displayed, scrolling depends on the display option chosen for Summary view. If you enabled the **All layers** option for the Summary view, the analyzer automatically scrolls to show the highest level in the Detail view as well. If the option is disabled, the analyzer scrolls to match the level highlighted in the Summary view.

Controlling the Layer Initially Displayed in the Detail View

You can also define the layer to which Detail view scrolls when you move to a new frame. If a frame does not include the layer you selected, the next lower layer is highlighted.

To set the level initially displayed in the Detail view:

1. Move to **Display\Summary\All layers** and press Spacebar to enable (√) the option.

2. In the Summary view, move to the level you want to display in the Detail view.

Formats for Higher-Level Numeric Addresses

In the Detail view, the Sniffer analyzer shows the numeric form of each source or destination address, as well as the name assigned to that address in the name table.

The numeric display format of higher-level addresses is hexadecimal, except when there is an established convention for a different form. For example, a 4-byte IP address is shown as a succession of four decimal numbers separated by dots, with the entire number enclosed in square brackets.

For each displayed address, a format appropriate to the level and protocol for that address is shown. Some common examples are shown in Figure 4–23.

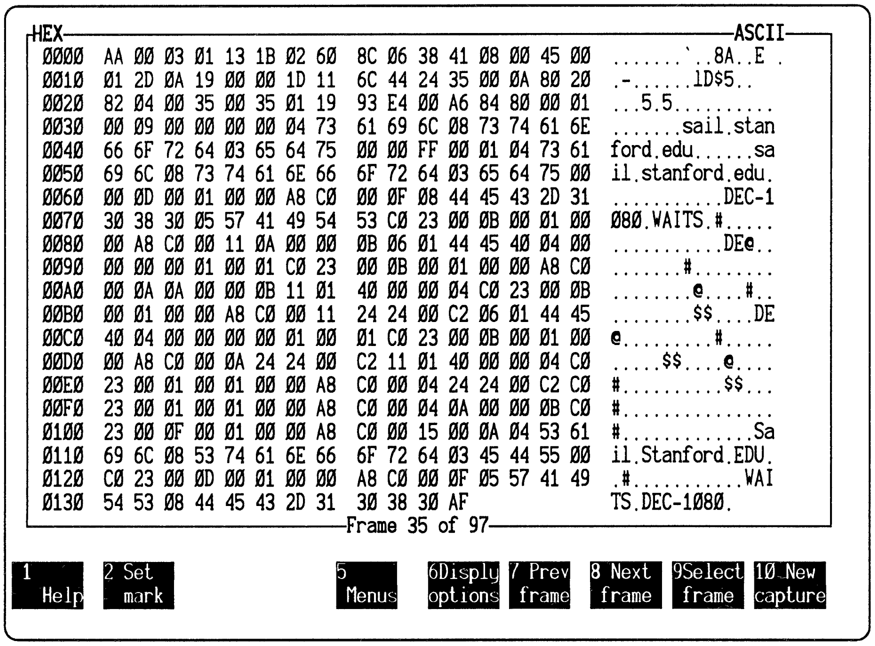
	Ethernet, Token Ring, StarLAN, PC Network, FDDI	**ARCNET, LocalTalk**	**Sniffer Internetwork Analyzer (WAN/Synchronous)**
DLC	Shows all frames as12 hexadecimal digits, corresponding to the 6-byte address. Ex: 020701031EF7	Shows all frames as two hexadecimal digits, corresponding to the 1-byte address. Ex: 3C	Shows each frame as either from DTE or from DCE.
XNS	Format is the same as a 6-byte DLC address. (Although an XNS address may be the same as a DLC address, the analyzer does not attempt to interpret the manufacturer's ID, as in the DLC address.) Ex. 0000404.00001B30F09A		
IP	Address is represented byte by byte. Each byte is shown as a decimal value; a number between 0 and 255. Successive bytes are separated by a dot, and the whole sequence is enclosed in brackets. Ex. [84.12.139.144]		
DRP (DECnet)	Address is represented by two decimal numbers, the *area* and the *node number*, separated by a dot. Each number is computed as the binary value after masking certain bits in the address. Ex. 184.27		
DDP (AppleTalk)	Address is represented by two decimal numbers, the network number (representing a 16-bit network address) and the node ID (representing an 8-bit node number), separated by a dot. Ex. 1080.208		
IPX	Address is represented by two address types, a 4-byte network number and a 6-byte node address, separated by a dot. Ex. 00000007.723259223502		

Figure 4–23. Address formats for selected networks and protocols.

The Hexadecimal View

The Hex view displays each byte as two hex characters, 00 to FF, with a blank between successive bytes. The bytes are arranged 16 to a row in a full-width table (eight to a row in the half-width table for the **Two viewports option**).

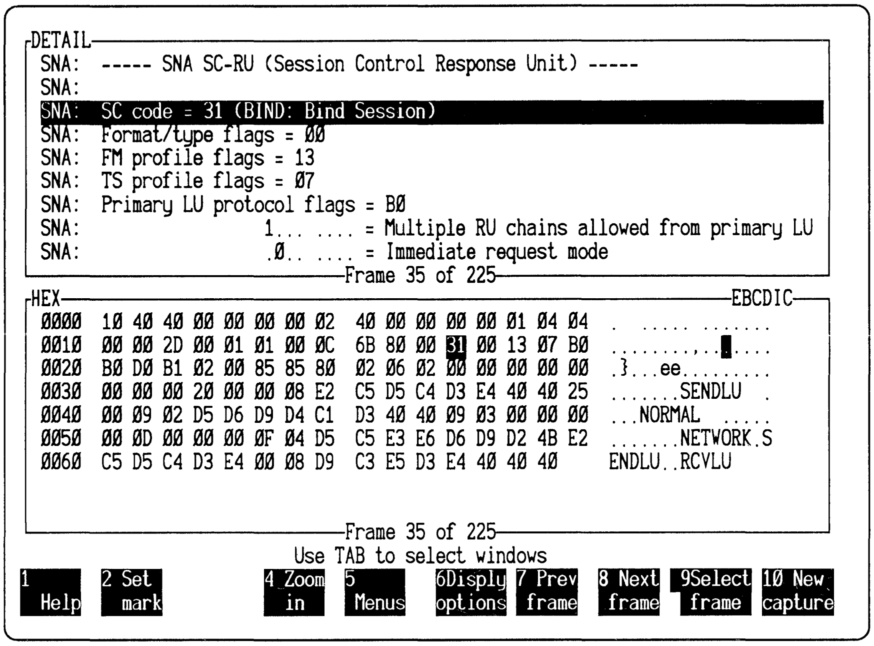
As shown in Figure 4–24, the far left column shows the offset from the beginning of the frame, which allows you to readily calculate each field's address. The hexadecimal offset is required when you describe a pattern to be matched. Note that you can "copy and paste" the offset pattern from a displayed frame, without having to type the hex offset. For more information, see "Copying and Pasting a Pattern from the Display Hex Window" on page 3–47.



```
HEX                                                      ASCII
 ØØØØ  AA ØØ Ø3 Ø1 13 1B Ø2 6Ø  8C Ø6 38 41 Ø8 ØØ 45 ØØ  .......`..8A..E .
 ØØ1Ø  Ø1 2D ØA 19 ØØ ØØ 1D 11  6C 44 24 35 ØØ ØA 8Ø 2Ø  .-......1D$5..
 ØØ2Ø  82 Ø4 ØØ 35 ØØ 35 Ø1 19  93 E4 ØØ A6 84 8Ø ØØ Ø1  ...5.5..........
 ØØ3Ø  ØØ Ø9 ØØ ØØ ØØ ØØ Ø4 73  61 69 6C Ø8 73 74 61 6E  .......sail.stan
 ØØ4Ø  66 6F 72 64 Ø3 65 64 75  ØØ ØØ FF ØØ Ø1 Ø4 73 61  ford.edu......sa
 ØØ5Ø  69 6C Ø8 73 74 61 6E 66  6F 72 64 Ø3 65 64 75 ØØ  il.stanford.edu.
 ØØ6Ø  ØØ ØD ØØ Ø1 ØØ ØØ A8 CØ  ØØ ØF Ø8 44 45 43 2D 31  ..........DEC-1
 ØØ7Ø  3Ø 38 3Ø Ø5 57 41 49 54  53 CØ 23 ØØ ØB ØØ Ø1 ØØ  Ø8Ø.WAITS.#.....
 ØØ8Ø  ØØ A8 CØ ØØ 11 ØA ØØ ØØ  ØB Ø6 Ø1 44 45 4Ø Ø4 ØØ  ...........DE@..
 ØØ9Ø  ØØ ØØ ØØ Ø1 ØØ Ø1 CØ 23  ØØ ØB ØØ Ø1 ØØ ØØ A8 CØ  .......#........
 ØØAØ  ØØ ØA ØA ØØ ØØ ØB 11 Ø1  4Ø ØØ ØØ Ø4 CØ 23 ØØ ØB  ........@....#..
 ØØBØ  ØØ Ø1 ØØ ØØ A8 CØ ØØ 11  24 24 ØØ C2 Ø6 Ø1 44 45  ........$$....DE
 ØØCØ  4Ø Ø4 ØØ ØØ ØØ ØØ Ø1 ØØ  Ø1 CØ 23 ØØ ØB ØØ Ø1 ØØ  @.........#.....
 ØØDØ  ØØ A8 CØ ØØ ØA 24 24 ØØ  C2 11 Ø1 4Ø ØØ ØØ Ø4 CØ  .....$$....@....
 ØØEØ  23 ØØ Ø1 ØØ Ø1 ØØ ØØ A8  CØ ØØ Ø4 24 24 ØØ C2 CØ  #..........$$...
 ØØFØ  23 ØØ Ø1 ØØ Ø1 ØØ ØØ A8  CØ ØØ Ø4 ØA ØØ ØØ ØB CØ  #...............
 Ø1ØØ  23 ØØ ØF ØØ Ø1 ØØ ØØ A8  CØ ØØ 15 ØØ ØA Ø4 53 61  #.............Sa
 Ø11Ø  69 6C Ø8 53 74 61 6E 66  6F 72 64 Ø3 45 44 55 ØØ  il.Stanford.EDU.
 Ø12Ø  CØ 23 ØØ ØD ØØ Ø1 ØØ ØØ  A8 CØ ØØ ØF Ø5 57 41 49  .#...........WAI
 Ø13Ø  54 53 Ø8 44 45 43 2D 31  3Ø 38 3Ø AF               TS.DEC-1Ø8Ø.
                              Frame 35 of 97
```

Figure 4–24. Hexadecimal view of a TCP/IP frame on Ethernet.

If both the Detail and Hex views are displayed, moving the highlight in the Detail view automatically highlights the corresponding bytes in the Hex view, as shown in Figure 4–25. This makes it easy to match a sequence of bytes with the interpretation of those bytes.



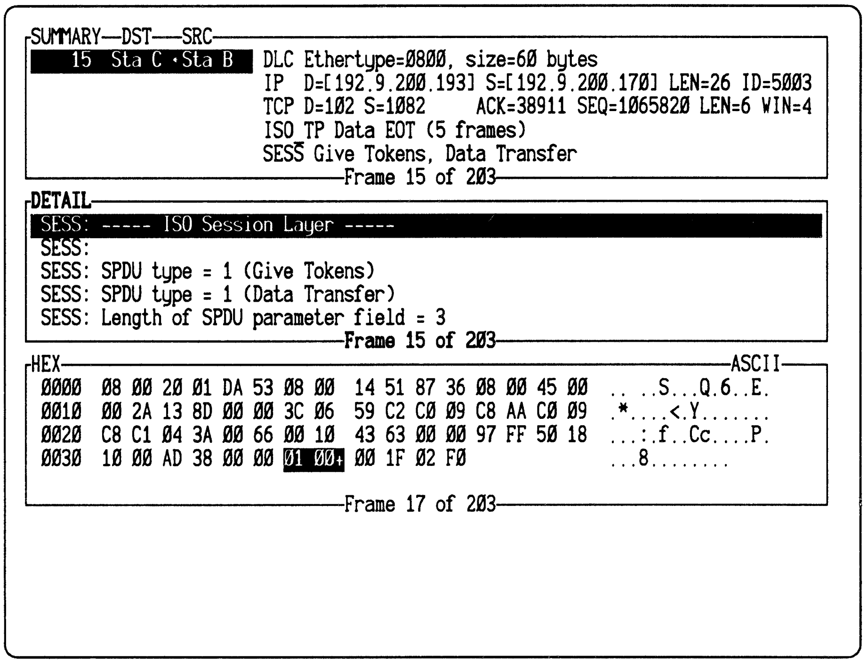
```
DETAIL
 SNA:  ----- SNA SC-RU (Session Control Response Unit) -----
 SNA:
 SNA:  SC code = 31 (BIND: Bind Session)
 SNA:  Format/type flags = ØØ
 SNA:  FM profile flags = 13
 SNA:  TS profile flags = Ø7
 SNA:  Primary LU protocol flags = BØ
 SNA:                  1... .... = Multiple RU chains allowed from primary LU
 SNA:                  .Ø.. .... = Immediate request mode
                              Frame 35 of 225
HEX                                                                    EBCDIC
 ØØØØ  1Ø 4Ø 4Ø ØØ ØØ ØØ ØØ Ø2  4Ø ØØ ØØ ØØ ØØ Ø1 Ø4 Ø4  .  ..... .......
 ØØ1Ø  ØØ ØØ 2D ØØ Ø1 Ø1 ØØ ØC  6B 8Ø ØØ 31 ØØ 13 Ø7 BØ  ..........,.......
 ØØ2Ø  BØ DØ B1 Ø2 ØØ 85 85 8Ø  Ø2 Ø6 Ø2 ØØ ØØ ØØ ØØ ØØ  .}...ee.........
 ØØ3Ø  ØØ ØØ ØØ 2Ø ØØ ØØ Ø8 E2  C5 D5 C4 D3 E4 4Ø 4Ø 25  .......SENDLU  .
 ØØ4Ø  ØØ Ø9 Ø2 D5 D6 D9 D4 C1  D3 4Ø 4Ø Ø9 Ø3 ØØ ØØ ØØ  ...NORMAL  .....
 ØØ5Ø  ØØ ØD ØØ ØØ ØØ ØF Ø4 D5  C5 E3 E6 D6 D9 D2 4B E2  .......NETWORK.S
 ØØ6Ø  C5 D5 C4 D3 E4 ØØ Ø8 D9  C3 E5 D3 E4 4Ø 4Ø 4Ø     ENDLU..RCVLU

                              Frame 35 of 225
                          Use TAB to select windows
```

Figure 4–25. Synchronized highlighting in the Detail and Hex views.

Display of Spanned Frames

In some protocols, a message at one of the higher levels may span several DLC frames. During display, the Detail view reassembles the entire high-level message as though the whole message were in the first frame. This allows you to read the message without having to jump among the frames that contain its parts. When you highlight a part of the Detail view, the Hex view continues to highlight the corresponding hex characters.

Figure 4–26 illustrates the treatment of a spanned high-level message.



```
SUMMARY—DST——SRC
  15  Sta C ‹Sta B  DLC Ethertype=Ø8ØØ, size=6Ø bytes
                    IP  D=[192.9.2ØØ.193] S=[192.9.2ØØ.17Ø] LEN=26 ID=5ØØ3
                    TCP D=1Ø2 S=1Ø82     ACK=38911 SEQ=1Ø6582Ø LEN=6 WIN=4
                    ISO_TP Data EOT (5 frames)
                    SESS Give Tokens, Data Transfer
                              Frame 15 of 2Ø3
DETAIL
 SESS: ----- ISO Session Layer -----
 SESS:
 SESS: SPDU type = 1 (Give Tokens)
 SESS: SPDU type = 1 (Data Transfer)
 SESS: Length of SPDU parameter field = 3
                              Frame 15 of 2Ø3
HEX                                                             ASCII
 ØØØØ  Ø8 ØØ 2Ø Ø1 DA 53 Ø8 ØØ  14 51 87 36 Ø8 ØØ 45 ØØ  .. ..S...Q.6..E.
 ØØ1Ø  ØØ 2A 13 8D ØØ ØØ 3C Ø6  59 C2 CØ Ø9 C8 AA CØ Ø9  .*....<.Y.......
 ØØ2Ø  C8 C1 Ø4 3A ØØ 66 ØØ 1Ø  43 63 ØØ ØØ 97 FF 5Ø 18  ...:.f..Cc....P.
 ØØ3Ø  1Ø ØØ AD 38 ØØ ØØ Ø1 ØØ+ ØØ 1F Ø2 FØ              ...8........

                              Frame 17 of 2Ø3
```

Figure 4–26. Detail and Hex view of a spanned ISO frame.

Here are some points to observe:

- In the Summary view, the frame in which the high-level message starts includes a note that informs you how many frames are spanned by that message. In Figure 4–26, for example, the note "ISO_TP Data EOT (5 frames)" indicates where the ISO TP data was split among frames 15, 16, 17, 18, 19, and 20. There is no presumption that spanned frames are consecutive; unrelated frames might have arrived between them and so appear interspersed in the display.
- In the Detail view, the entire high-level message is displayed as though all of it were in the frame in which it starts. When you print the display, the entire high-level message appears without a break, in as many lines as necessary. On the screen, you can see the rest of the message by scrolling within the Detail view.
- The frame number in the Hex view doesn't necessarily match the frame number in the Detail view. In Figure 4–26, the interpretation of ISO Session Layer is part of the Detail view of frame 15, because that is where the ISO TP data starts. However, the corresponding Hex view shows frame 17 because—although the message started in frame 15—its ISO Session Layer continues to frame 17, starting at offset 36.
- When the field highlighted in the Detail view extends over additional frames, the Hex panel scrolls to the start of the corresponding field, but adds a + sign to show that there is additional information in a different frame.

The Hexadecimal View Display Options

As with the Summary view display options, the Hex view display options determine how data is displayed. This includes:

- Type of interpretation
- Whether to ignore the high bit as a parity bit

Defining the Type of Interpretation

To the right of the hexadecimal codes, the Hex view shows the corresponding ASCII or EBCDIC characters. A standard character is shown by its text equivalent; anything else is represented by a dot.

The interpretation of characters follows either ASCII or EBCDIC conventions. For Ethernet and token ring networks, you can also choose **Dynamic mode**, which automatically adjusts interpretation for each frame as either EBCDIC (for all MAC frames and for any LLC frames whose SAP indicates that it contains SNA) or ASCII (for all other frames).

The option you choose applies to all levels of all frames. The default is to show ASCII characters.

To select the type of interpretation:

1. Move to **Display\Hex**.
2. In the radio control to the right, move to the desired option and press Spacebar.

   ▶ ASCII characters
   EBCDIC characters (MAC, SNA)
   Dynamic mode

Selecting ASCII Parity

You can also enable the **ASCII parity** option, which strips the 8th (high) bit from each byte. Since most protocols do not interpret the high bit, the default is **ASCII parity** disabled (x).

Function Keys Available During Display

While displaying the results of an interpretation in one—or all three—display views, the following function keys are available to manipulate the views.

F1 **Help**. Provides access to the Help system.

F2 **Set mark.** Marks the highlighted frame with the flag "M." The Sniffer analyzer uses this frame as the reference frame from which it calculates relative time and cumulative bytes. (See "Flags Display Option" on page 4–27.)

F3 **Data display/Edit options**. Displays the data that passed the display filters in the formats you defined. After defining the display options (or at any other time when display was interrupted) press F3 (**Data display**) again to resume the display.

If the **Frame editing** option is enabled, this key toggles to **Edit options**, which allows you to edit frame content in the Hex view. (See "Using Hexadecimal View to Edit Frames" on page 4–38.)

F4 **Zoom in/Zoom out.** Temporarily expands the active view to fill the entire window, which allows you to see more detail. To move to an enlarged version of any other open views, press the Tab key. To move to the previous view, press Shift-Tab.

Pressing F4 (**Zoom out**) a second time restores the arrangement of the open views.

F5 **Menus.** Displays the main menu.

F6 **Display options.** Displays the same set of display options as the main menu, as well as several additional options that allow you to search for frames, as described in "Searching for Frames" on page 4–41.

F7 **Previous frame**. Pressing F7 (or the Cursor Up key) moves to the previous frame accepted by the filters, in all open views.

In the Summary view, the highlight moves to the preceding line (either the preceding frame or the preceding level of the current frame). In the Detail view and the Hex view, the current display is replaced by the display for the preceding frame.

F8 **Next frame.** Pressing F8 (or the Cursor Down key) moves to the next line or the next frame, similar to the way F7 moves to the previous frame.

F9 **Select frame/Unselect frame**. Attaches the "S" flag to the highlighted frame. You can use this to select as many frames as you want and then save those frames to a file, as described in "Selected Frames Display Filter" on page 4–14.

Pressing F9 (**Unselect frame**) removes the flag from the highlighted frame.

F10 **New Capture/Stop capture.** Starts the capture process.

When capture is in progress, pressing F10 (**Stop capture**) again stops the capture. To ensure that the captured frames include the frame that interests you, set a trigger, as described in"Defining a Trigger to Stop Capture" on page 3–53.

Using Hexadecimal View to Edit Frames

The **Frame editing** option lets you edit the contents of a frame to change its size, content, or timing. This option is useful for development tasks such as writing protocol interpreters, where it allows you to simulate conditions for testing. It is also useful for inserting or deleting bytes in misaligned frames so that the DLC content may be decoded. By using the **Buffer mode** option in the **Traffic generator** function, you can transmit buffers you create with frame editing.

Warning: If display filters are enabled and the frame being edited is changed so that it fails the filtering criteria, making either the Summary or Detail views active causes the frame to be filtered out. As long as the Hex view is active, the frame being edited is protected from any filters.

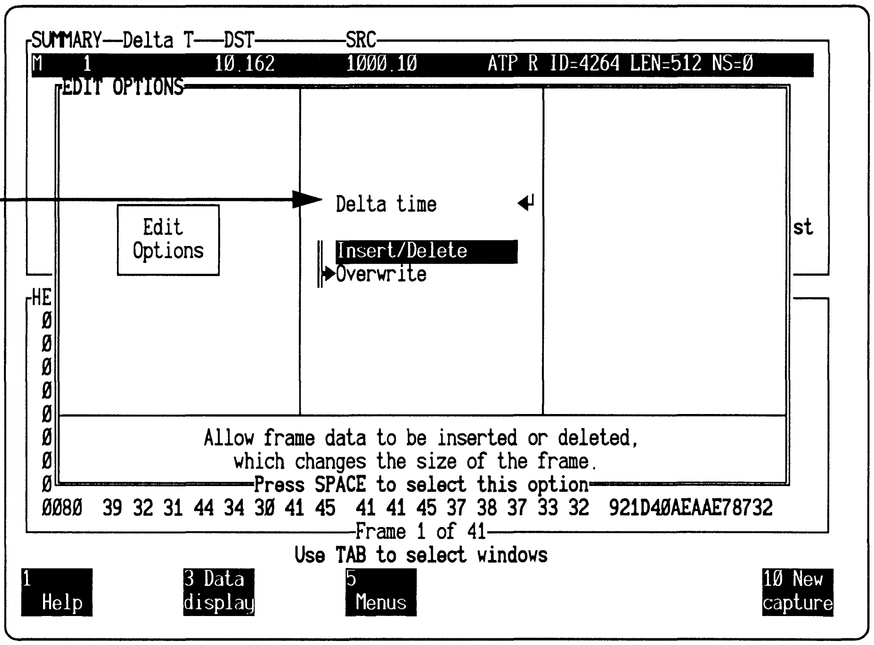
As you edit a frame, the Sniffer analyzer attempts to change the associated descriptions in the Summary and Detail views to match the edited content. Sometimes, however, it may not be able to do so, such as when the value of the edited frame depends on those of the previous frame, as in a session or connection-related PI interpretation.

When you complete editing the frame, you can reinterpret the entire capture buffer so that any options or filters are applied to the edited frame. After reinterpretation, all views will contain the correct descriptions.

When editing frames, consider the following:

- In the Summary view, edited frames are identified with an "E" flag, whether or not the **Flags** option is enabled. In the Detail view, the first line reads "This frame has been edited."
- As long as the Hex view is active, edited frames are not affected by any enabled display filters. This ensures that an edited frame is not eliminated from the display by a filter. When you reinterpret edited frames, however, or when you make the Summary or Detail views active, all filters and other settings are applied.
- If you delete a frame, its frame number remains.
- You can use the Edit option **Delta time** (time between frames) to speed up or delay a transmission, which allows you to affect loads.
- You can choose the Edit option **Insert/Delete** to change the frame size. However, be careful not to exceed or go below the legal frame sizes for your particular network.
- You can use the Edit option **Overwrite** to change only existing frame data.
- On analyzers with an Ethernet-II adapter card, you can use the **Frame editing** option to create bad CRC frames.

Figure 4–27 shows the Edit options associated with Frame editing.



Sets interval between frames

```
SUMMARY—Delta T——DST————SRC
M   1        10.162      1000.10      ATP R ID=4264 LEN=512 NS=0
 EDIT OPTIONS

                Delta time          ↵
  Edit
  Options      Insert/Delete
              ▶Overwrite
HE
0
0
0
0
0
0
0       Allow frame data to be inserted or deleted,
0         which changes the size of the frame.
0          Press SPACE to select this option
0080  39 32 31 44 34 30 41 45  41 41 45 37 38 37 33 32  921D40AEAAE78732
                      Frame 1 of 41
                 Use TAB to select windows
```

Figure 4–27. The Edit options for editing frames.

To edit frames:

1. Move to **Display\Frame editing** and press Spacebar to enable (√) the option.
2. Move to **Display\Hex** and press Spacebar to enable the option.
3. Depending on what other information you want to display, move to and enable the following options:

   √ Summary
   √ Detail
   √ Flags
   √ Delta time

4. Press F3 (**Data display**) and press Tab to make the Hex view active.

   Note that the cursor is blinking on the first byte. If the cursor is a block (the default), whatever you type will overwrite the existing values. If the cursor is an underline, information you type will be inserted and pressing the Delete key will delete existing information.

5. (Optional) Press F3 (**Edit options**) to determine the edit options. This includes **Delta time** and the edit mode.

   a. To change the interval between frames, move to **Delta time** and press Enter. In the dialog box that appears, enter the desired interframe delay in milliseconds.

   b. To change between the overwrite and insert modes, move to the desired edit mode and press Spacebar.

   ‖ Insert/Delete
   ▶ Overwrite

c. To create a bad CRC frame (Ethernet-II only), move to **CRC error** and press Spacebar to enable (√) the option.

6. (Optional) Determine whether to edit the hex codes or the corresponding ASCII (or EBCDIC) characters. To toggle between the two modes, press F2 (**Edit text\Edit hex**).
7. Press the Cursor keys to move to the Hex position you want to edit and type the desired characters. As you type, you can usually see that the corresponding text in the Summary and the Detail views changes.

   In the Summary view, the "E" flag appears in the far left column. This flag is *not* sent if you use the edited frame to generate traffic. In the Detail view, the first line identifies the frame as edited (for the transmitting station only).

To reinterpret edited frames:

1. If necessary, press F6 (**Display options**) to display the Display options menu.
2. Move to **Reinterpret** and press Enter.

   In response, the Sniffer analyzer reinterprets all frames, including those you edited, using any filters and other options that are enabled.

Searching for Frames

You can always find a frame by scrolling though the Summary view. However, there are shortcuts that will locate the desired frame more quickly and conveniently. When searching for frames, you can specify the following criteria:

Frame number — Moves to the frame number you specify.

Text — Searches for text you specify, in either the Summary, Detail, or Hex views.

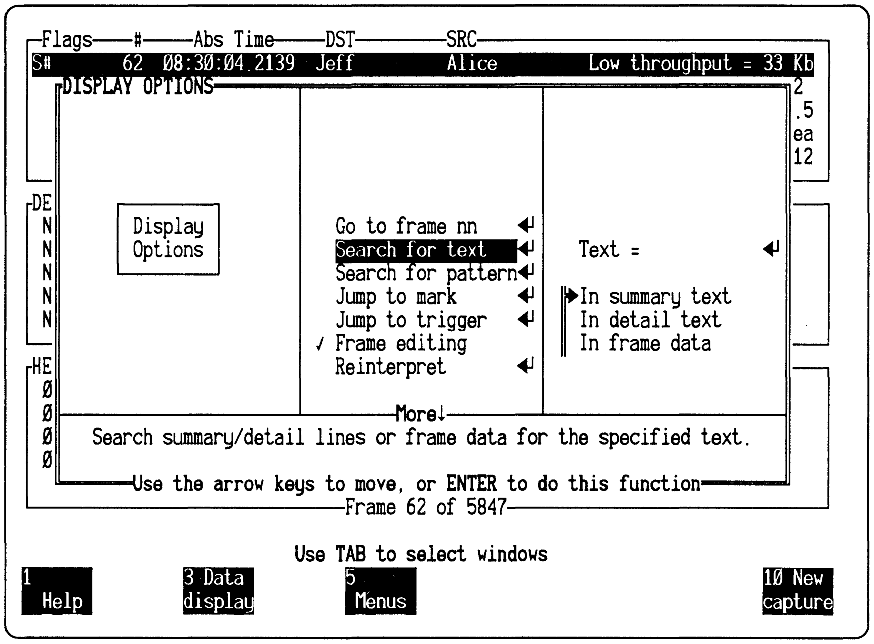
Pattern — Searches for a pattern you specify.

Mark — Moves to the reference frame, which you can specify with the "M" flag.

Trigger — Moves to the trigger frame, which is identified by the system with the "T" flag.

In the Summary view, you can also move to the last frame by pressing the End key. In the Detail view, this key moves to the last line for the current frame.

Figure 4–28 shows the available search options as they appear in the Display Options menu, specifically those associated with the **Search for text** option.



```
Flags  #   Abs Time      DST       SRC
S#    62  08:30:04.2139  Jeff      Alice        Low throughput = 33 Kb
```

Search summary/detail lines or frame data for the specified text.

Use the arrow keys to move, or ENTER to do this function

Frame 62 of 5847

Use TAB to select windows

Figure 4–28. The search options in the Display Options menu.

Searching for a Frame Number

If you know the frame number, you can simply enter that number as the search criterion.

To go to a frame number:

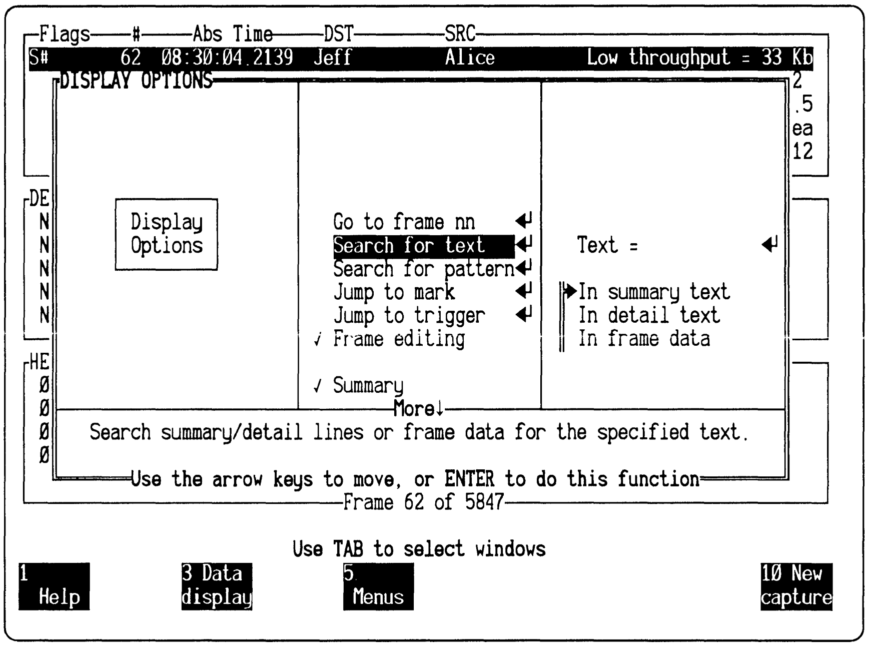
1. During display, press F6 (**Display options**).
2. Move to **Go to frame nn** and press Enter.
3. In the dialog box that appears, enter the desired frame number and press Enter. Note that you cannot specify a number larger than the number of frames in the capture buffer.

Searching for Text

You can also search the capture buffer for a frame that contains a particular text string. This text can either be a part of the data contained within the frames (when searching the frame data in the Hex view) or it can be a part of the Sniffer analyzer's interpretation of the frames (when searching the Summary and Detail views).

The search starts with the frame that follows the highlighted frame and stops at the first match. If a match is not found, searching continues from the first frame in the capture buffer. If no matches are found, the analyzer displays "Match not found" and stops searching.

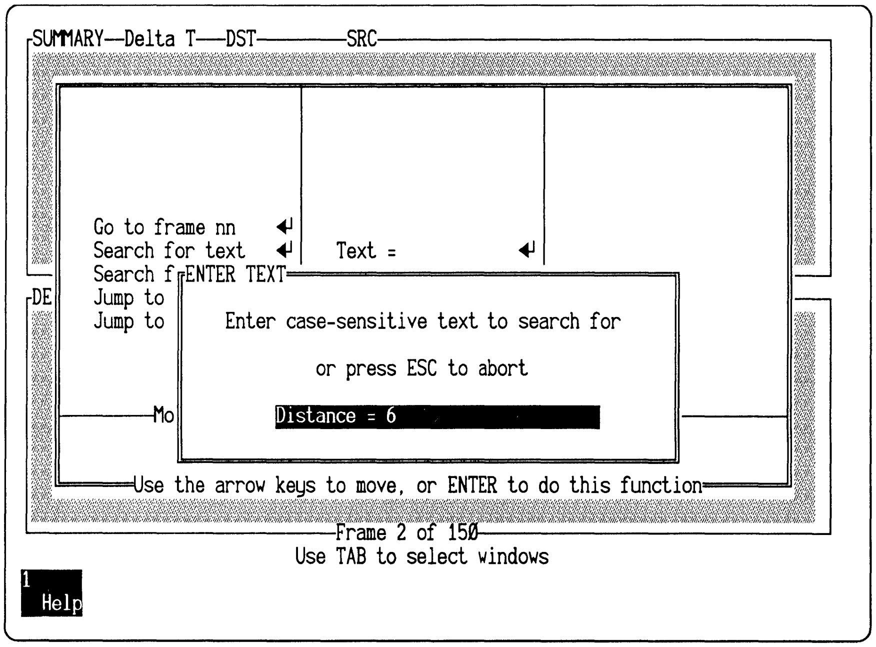
Figure 4–29 shows the options associated with searching for text.



```
Flags──#───Abs Time───DST────────SRC──────────────────────────
S#      62  08:30:04.2139  Jeff        Alice        Low throughput = 33 Kb
 DISPLAY OPTIONS                                                        2
                                                                       .5
                                                                       ea
                                                                       12
DE
 N     Display          Go to frame nn    ↵
 N     Options          Search for text   ↵     Text =              ↵
 N                      Search for pattern↵
 N                      Jump to mark      ↵    ▶In summary text
 N                      Jump to trigger   ↵     In detail text
                      √ Frame editing           In frame data
HE
 0                    √ Summary
 0  ─────────────────────More↓──────────────────────────────
 0  Search summary/detail lines or frame data for the specified text.
 0
    ════Use the arrow keys to move, or ENTER to do this function════
 ───────────────────────Frame 62 of 5847────────────────────────

                     Use TAB to select windows
1            3 Data        5                                 10 New
  Help       display         Menus                           capture
```

Figure 4–29. Searching the capture buffer for text.

Figure 4–30 is an example of how to search captured LocalTalk frames for the phrase "Distance = 6" in the Detail view.



```
SUMMARY─Delta T──DST────────SRC──────────────────────────────



   Go to frame nn    ↵
   Search for text   ↵    Text =              ↵
   Search f ENTER TEXT═══════════════════════════════
DE Jump to
   Jump to     Enter case-sensitive text to search for

                        or press ESC to abort

   ──────Mo            Distance = 6

   ════Use the arrow keys to move, or ENTER to do this function════
 ───────────────────────Frame 2 of 150──────────────────────
                     Use TAB to select windows
1
 Help
```

Figure 4–30. Entering text for which to search.

To search for text:

1. During display, press F6 (**Display options**) to show the **Display options** menu.

2. Specify which view is to be searched. Move to the desired option and press Spacebar.

   ▶ In summary text (default)
   In detail text
   In frame data

   If you chose the **In frame data** option, you can also choose the type of text interpretation.

   ▶ ASCII (default)
   EBCDIC

3. Move to **Search for text** and then to **Text =**. Press Enter.

4. In the dialog box that appears, type up to 31 characters. Because the search is case-sensitive, make sure you enter the letters exactly as they appear in the text.

You can continue searching the capture buffer for other matches that match the specified text.

To repeat a search for text:

1. Press F6 again for the Display Options menu.

2. Move to **Search for text** and press Enter.

   The text dialog box appears, with the string you specified previously in the **Text =** field.

3. To search again for the same text, press Enter. Otherwise, type new text and then press Enter.

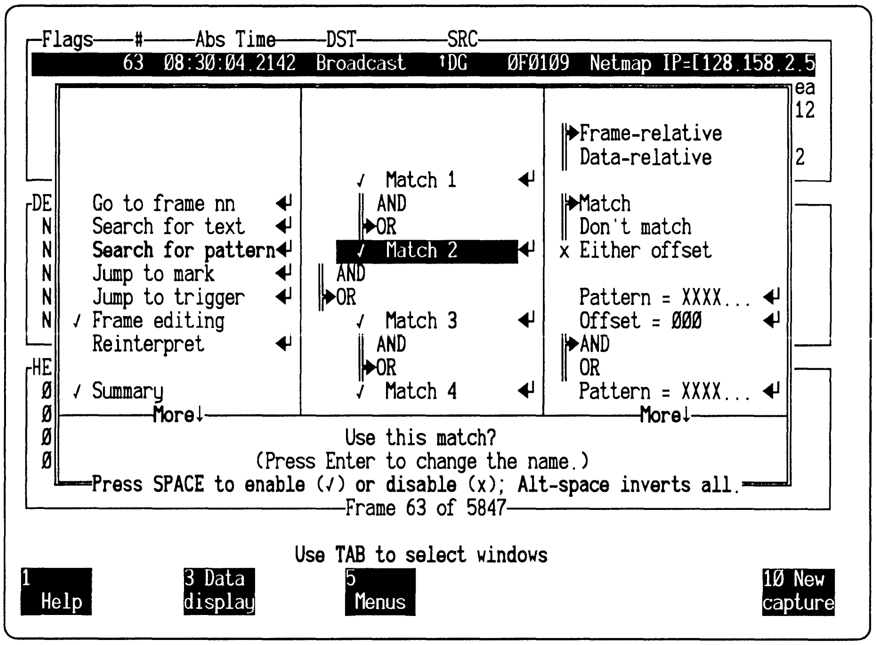
Searching for a Pattern

You can also search for frames that contain particular patterns.

As with a text search, a pattern search starts with the frame that follows the highlighted frame and stops at the first match. If the search reaches the last frame in the capture buffer without finding a match, searching continues from the first frame. If no matches are found, the Sniffer analyzer displays "Match not found" and stops searching.

When the analyzer finds the specified pattern, it displays the message "Found at frame nn." If the Summary view is open, the match frame is highlighted.

Figure 4–31 shows the options associated with searching for a pattern.



```
Flags──#───Abs Time───DST──────SRC─────────────────────────────
      63  08:30:04.2142  Broadcast  ↑DG   0F0109  Netmap IP=[128.158.2.5
                                                                       ea
                                                                       12
                                                  ▶Frame-relative
                                                   Data-relative        2
                               ✓ Match 1      ↵
DE     Go to frame nn     ↵      AND               ▶Match
N      Search for text    ↵     ▶OR                 Don't match
N      Search for pattern↵   ✓ Match 2        ↵   x Either offset
N      Jump to mark       ↵  AND
N      Jump to trigger    ↵ ▶OR                     Pattern = XXXX... ↵
N    ✓ Frame editing           ✓ Match 3      ↵     Offset = 000      ↵
       Reinterpret        ↵      AND               ▶AND
HE                              ▶OR                 OR
0    ✓ Summary                 ✓ Match 4      ↵     Pattern = XXXX... ↵
0    ────────More↓───────────────────────────────────────More↓────────
0                               Use this match?
0                         (Press Enter to change the name.)
   ═══Press SPACE to enable (✓) or disable (x); Alt-space inverts all.═══
   ────────────────────────────Frame 63 of 5847───────────────────────────

                               Use TAB to select windows
1             3 Data        5                                      10 New
  Help        display         Menus                                capture
```

Figure 4–31. Searching the capture buffer for a pattern.

To search the capture buffer for a pattern:

1. Press F6 (**Display options**) to show the **Display options** menu.
2. Move to **Search for Pattern** and then to the right to define up to four matches and the relationships to one another. (For more information about setting up patterns, see "Defining Complex Pattern Matches" on page 3–40.)
3. Return to **Search for Pattern** and press Enter.

To repeat a search for a pattern:

1. Press F6 (**Display options**) again to return to the **Display options** menu.
2. To search for the same pattern, press Enter. To specify a new pattern, follow the previous procedure, starting with step 2.

Jumping to the Marked Frame

You can jump to the reference (marked) frame, which is identified with the "M" flag. This frame is either the first frame in the capture buffer (default) or a frame you specify by pressing F2 (**Set mark**) when that frame is highlighted.

To jump to the marked frame:

1. Press F6 again to display the Display options menu.
2. Move to **Jump to mark** and press Enter.

Jumping to the Trigger Frame

As with the marked frame, you can jump to the trigger frame, which is identified with the "T" flag.

To jump to the trigger frame:

1. Press F6 again to display the **Display options** menu.
2. Move to **Jump to trigger** and press Enter.

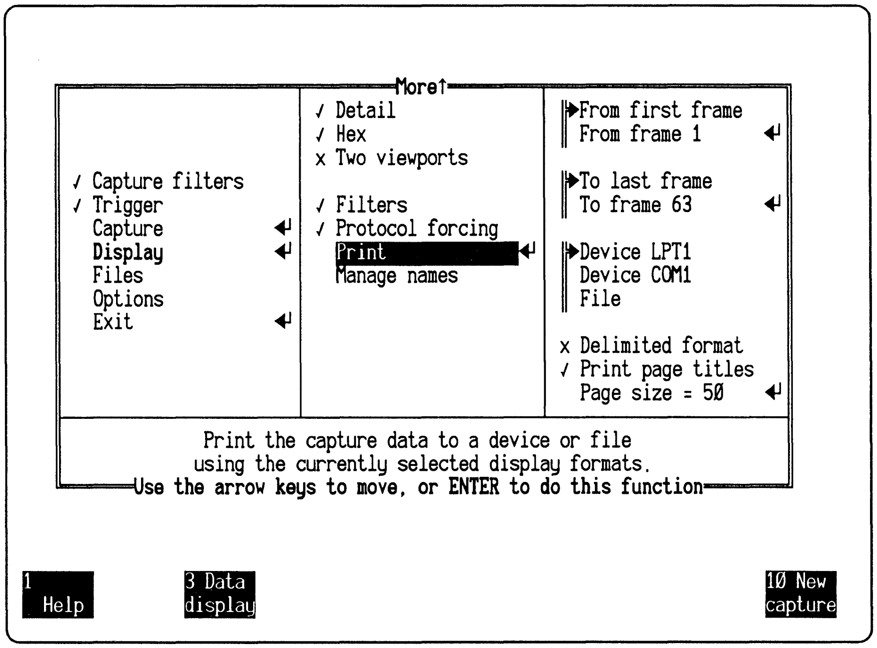
Printing and Importing Data

You can save, print, or import displayed frames, including frames that are visible only by scrolling. In general, printed or imported data are referred to as "reports."

For instructions on how to save data, see "Saving Captured Frames as Data (Trace) Files" on page 5–11. To prepare for printing or importing, you can define the following options:

- Range of included frames
- The destination, either a printer or file
- File format
- Page titles (if any)
- Page size

Figure 4–32 shows the options associated with printing and importing data.



```
                              More↑
                         ✓ Detail                  ▶From first frame
                         ✓ Hex                      From frame 1        ↵
                         x Two viewports
  ✓ Capture filters                                ▶To last frame
  ✓ Trigger              ✓ Filters                  To frame 63         ↵
    Capture          ↵   ✓ Protocol forcing
    Display          ↵     Print             ↵     ▶Device LPT1
    Files                  Manage names             Device COM1
    Options                                         File
    Exit             ↵
                                                  x Delimited format
                                                  ✓ Print page titles
                                                    Page size = 50      ↵

               Print the capture data to a device or file
                  using the currently selected display formats.
        Use the arrow keys to move, or ENTER to do this function

 1            3 Data                                              10 New
   Help       display                                             capture
```

Figure 4–32. Printing and importing data.

In general, printed or imported data shows the information on the screen, but without the restrictions of the small window. If both the Summary and the Detail views are open, the Summary data is printed first followed by the Detail data, with protocols in order from lowest to highest layer. Only those protocols enabled by the **Protocol** filter are included. When data is printed, there are no indications of highlighting or color.

In addition to printing information about frames, you can print information about network objects identified by the Expert analyzer. See the *Expert Sniffer Network Analyzer Operations* manual for details.

The procedure that follows outlines the steps for printing and exporting. For more information about each of the options associated with the **Print** option, see the sections after the procedure.

To create a report:

1. Display the information you want to include.
   a. Set the display filters to exclude frames that do not interest you.
   b. Set the **Address level** filter to determine how source and destination are identified. (This setting affects the way source and destination are described, even if it doesn't alter which frames are displayed.)
   c. Enable (√) or disable (x) the **All layers** and **DLC addresses** options as desired.
   d. Enable or disable the **Two-station format** option as desired.
   e. Set the **Name width** field. If you widen this field, note that the Sniffer analyzer does not fold the output lines, which makes it difficult to predict how long lines will be printed.
   f. Press F3 (**Data display**) to display the chosen views.
2. Define the range of frames in a report:
   a. Press F6 (**Display options**) to show the Display Options menu.
   b. Move to **Print** and then to the desired option. If you do not want to include the first and last frames, move to the **From frame xx** option and press Enter.

      ▶ From first frame
      From frame *xx*

      ▶ To last frame
      From frame *xx*

   c. In the dialog box that appears, enter the desired frame number and press Enter.
3. Define the destination by moving to the desired option and pressing Spacebar.

   ▶ Device LPT1
   Device COM1
   File

4. Define the file format. If you want to import the data, move to **Delimited format** and press Spacebar to enable (√) or disable (x) the option.

Note: If you enable the **Delimited format** option, you should disable the **Print page titles** option because most applications that accept delimited format do not accept page titles.

5. Determine whether to include page titles. Move to **Print page titles** and press Spacebar to enable (√) or disable (x) the option.
6. Determine the page size. Move to the **Page size** option and press Enter. In the dialog box that appears, enter a value between 5 and 99 as the desired page size.
7. Move to **Print** and press Enter. Depending on the report destination you specified, the report is either printed on the chosen printer or saved as a file.

   If you chose the **File** option, a dialog box appears. Enter the filename, using no more than eight characters. Do not include an extension; the Sniffer analyzer automatically attaches the extension .PRN for a file in the normal file format or .CSV (comma-separated values) for a file in the delimited format.

Defining the Range of Frames

Unless you specify otherwise, the analyzer includes frames starting with the reference (marked) frame through the last frame in the buffer. The reference frame is the first frame in the buffer, unless you marked another frame by pressing F2 (**Set mark**).

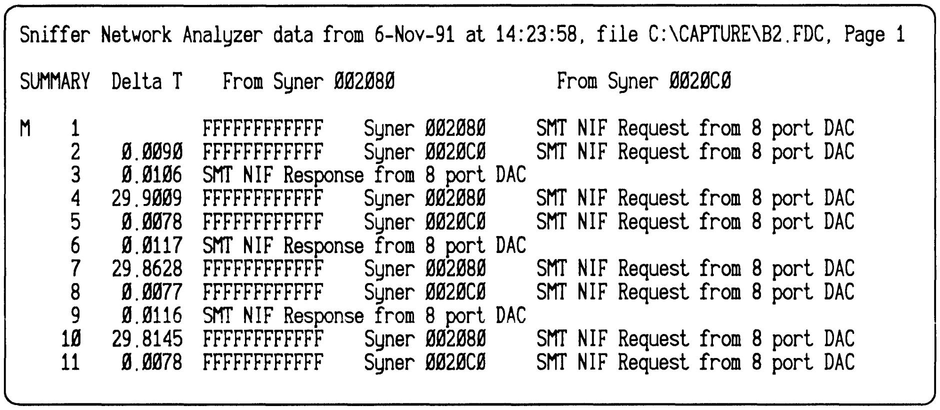
You can also specify the frame numbers of the first and last frames you want to include in the report.

Defining the Destination: Printer or File

You can either print displayed data or save it to disk as a file. Figure 4–33 shows the first page of a report on an Ethernet network, which was taken from the Summary view displayed in the two-station format.

Report destination options include:

LPT1	A parallel printer attached to the LPT1 port.
COM1	A serial printer attached to the COM1 port.
File	A file that is saved to disk (a:\ or c:\).



```
Sniffer Network Analyzer data from 6-Nov-91 at 14:23:58, file C:\CAPTURE\B2.FDC, Page 1

SUMMARY  Delta T    From Syner ØØ2Ø8Ø              From Syner ØØ2ØCØ

M    1              FFFFFFFFFFFF    Syner ØØ2Ø8Ø     SMT NIF Request from 8 port DAC
     2    Ø.ØØ9Ø  FFFFFFFFFFFF    Syner ØØ2ØCØ     SMT NIF Request from 8 port DAC
     3    Ø.Ø1Ø6  SMT NIF Response from 8 port DAC
     4   29.9ØØ9  FFFFFFFFFFFF    Syner ØØ2Ø8Ø     SMT NIF Request from 8 port DAC
     5    Ø.ØØ78  FFFFFFFFFFFF    Syner ØØ2ØCØ     SMT NIF Request from 8 port DAC
     6    Ø.Ø117  SMT NIF Response from 8 port DAC
     7   29.8628  FFFFFFFFFFFF    Syner ØØ2Ø8Ø     SMT NIF Request from 8 port DAC
     8    Ø.ØØ77  FFFFFFFFFFFF    Syner ØØ2ØCØ     SMT NIF Request from 8 port DAC
     9    Ø.Ø116  SMT NIF Response from 8 port DAC
    1Ø   29.8145  FFFFFFFFFFFF    Syner ØØ2Ø8Ø     SMT NIF Request from 8 port DAC
    11    Ø.ØØ78  FFFFFFFFFFFF    Syner ØØ2ØCØ     SMT NIF Request from 8 port DAC
```

Figure 4–33. Portion of printed report, displayed in two-station format, printed in normal print format.

Defining the File Format

You can define the format for data to be printed or exported. For printing, you should generally disable the **Delimited format** option. For importing, you can enable this option to format the data in the CSV format, which is widely used for importing data to spreadsheets.

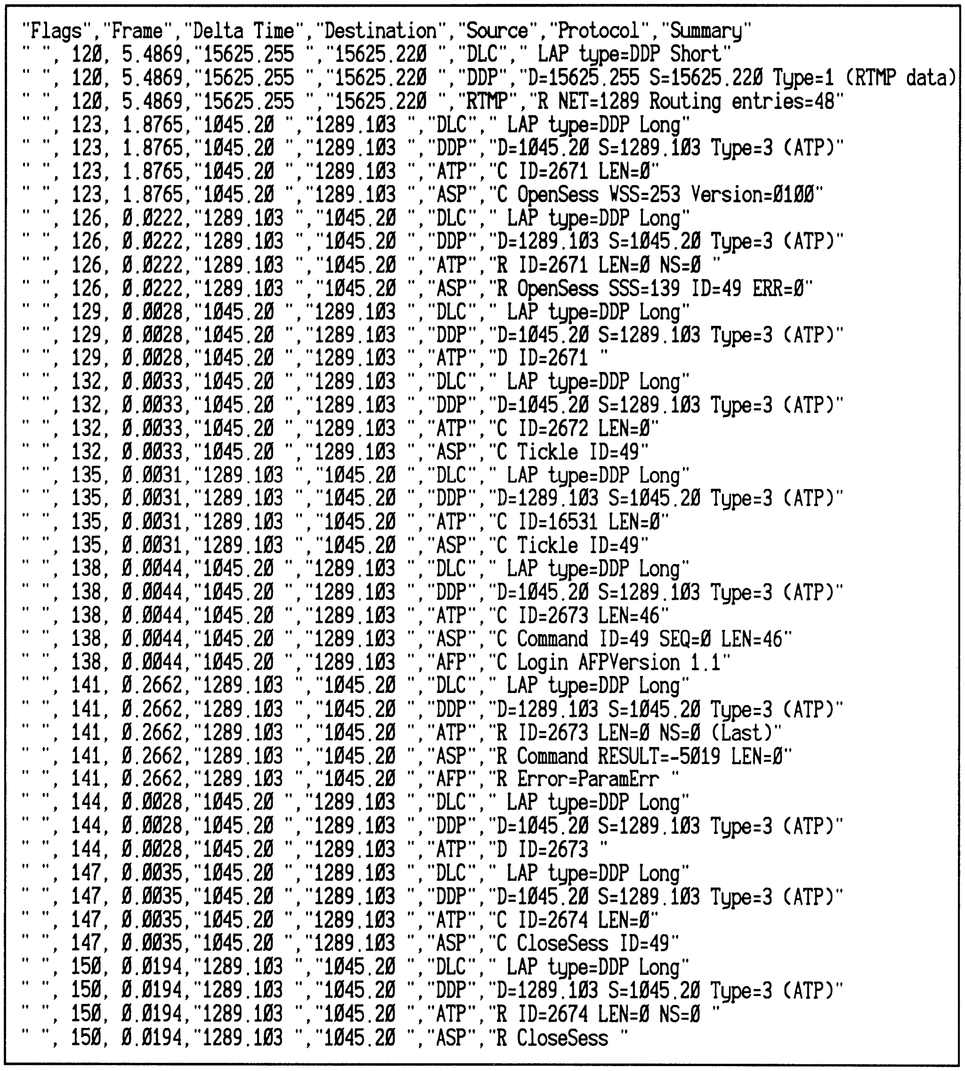
Note: Although you can enable the **Delimited format** option when the Detail or Hex views are open, this format does not apply to the data from those views. Instead, the report will be in the standard printer format.

In delimited format, each character field is surrounded by double quotes and successive fields are separated by commas, as shown in Figure 4–34. The file's first line defines the fields. Each subsequent line is a *record* that contains the values for each field. Each line in the imported file corresponds to a row in the Summary view.

Whether the format shows a single line per frame or one line per protocol level depends on whether the **All layers** display option is enabled (see "All Layers Display Option" on page 4–24). As a result, the file will contain either one line per frame or one line per enabled protocol level.

If the Summary view shows multiple lines, fields that are the same for each line are shown only in the first line. For example, the frame number is shown only with the first of the protocols for that frame. However, in the corresponding delimited file, every line is filled, even when it is part of the same frame.

For examples of the normal and delimited formats, compare Figure 4–33 and Figure 4–34.



```
"Flags","Frame","Delta Time","Destination","Source","Protocol","Summary"
" ", 120, 5.4869,"15625.255 ","15625.220 ","DLC"," LAP type=DDP Short"
" ", 120, 5.4869,"15625.255 ","15625.220 ","DDP","D=15625.255 S=15625.220 Type=1 (RTMP data)
" ", 120, 5.4869,"15625.255 ","15625.220 ","RTMP","R NET=1289 Routing entries=48"
" ", 123, 1.8765,"1045.20 ","1289.103 ","DLC"," LAP type=DDP Long"
" ", 123, 1.8765,"1045.20 ","1289.103 ","DDP","D=1045.20 S=1289.103 Type=3 (ATP)"
" ", 123, 1.8765,"1045.20 ","1289.103 ","ATP","C ID=2671 LEN=0"
" ", 123, 1.8765,"1045.20 ","1289.103 ","ASP","C OpenSess WSS=253 Version=0100"
" ", 126, 0.0222,"1289.103 ","1045.20 ","DLC"," LAP type=DDP Long"
" ", 126, 0.0222,"1289.103 ","1045.20 ","DDP","D=1289.103 S=1045.20 Type=3 (ATP)"
" ", 126, 0.0222,"1289.103 ","1045.20 ","ATP","R ID=2671 LEN=0 NS=0 "
" ", 126, 0.0222,"1289.103 ","1045.20 ","ASP","R OpenSess SSS=139 ID=49 ERR=0"
" ", 129, 0.0028,"1045.20 ","1289.103 ","DLC"," LAP type=DDP Long"
" ", 129, 0.0028,"1045.20 ","1289.103 ","DDP","D=1045.20 S=1289.103 Type=3 (ATP)"
" ", 129, 0.0028,"1045.20 ","1289.103 ","ATP","D ID=2671 "
" ", 132, 0.0033,"1045.20 ","1289.103 ","DLC"," LAP type=DDP Long"
" ", 132, 0.0033,"1045.20 ","1289.103 ","DDP","D=1045.20 S=1289.103 Type=3 (ATP)"
" ", 132, 0.0033,"1045.20 ","1289.103 ","ATP","C ID=2672 LEN=0"
" ", 132, 0.0033,"1045.20 ","1289.103 ","ASP","C Tickle ID=49"
" ", 135, 0.0031,"1289.103 ","1045.20 ","DLC"," LAP type=DDP Long"
" ", 135, 0.0031,"1289.103 ","1045.20 ","DDP","D=1289.103 S=1045.20 Type=3 (ATP)"
" ", 135, 0.0031,"1289.103 ","1045.20 ","ATP","C ID=16531 LEN=0"
" ", 135, 0.0031,"1289.103 ","1045.20 ","ASP","C Tickle ID=49"
" ", 138, 0.0044,"1045.20 ","1289.103 ","DLC"," LAP type=DDP Long"
" ", 138, 0.0044,"1045.20 ","1289.103 ","DDP","D=1045.20 S=1289.103 Type=3 (ATP)"
" ", 138, 0.0044,"1045.20 ","1289.103 ","ATP","C ID=2673 LEN=46"
" ", 138, 0.0044,"1045.20 ","1289.103 ","ASP","C Command ID=49 SEQ=0 LEN=46"
" ", 138, 0.0044,"1045.20 ","1289.103 ","AFP","C Login AFPVersion 1.1"
" ", 141, 0.2662,"1289.103 ","1045.20 ","DLC"," LAP type=DDP Long"
" ", 141, 0.2662,"1289.103 ","1045.20 ","DDP","D=1289.103 S=1045.20 Type=3 (ATP)"
" ", 141, 0.2662,"1289.103 ","1045.20 ","ATP","R ID=2673 LEN=0 NS=0 (Last)"
" ", 141, 0.2662,"1289.103 ","1045.20 ","ASP","R Command RESULT=-5019 LEN=0"
" ", 141, 0.2662,"1289.103 ","1045.20 ","AFP","R Error=ParamErr "
" ", 144, 0.0028,"1045.20 ","1289.103 ","DLC"," LAP type=DDP Long"
" ", 144, 0.0028,"1045.20 ","1289.103 ","DDP","D=1045.20 S=1289.103 Type=3 (ATP)"
" ", 144, 0.0028,"1045.20 ","1289.103 ","ATP","D ID=2673 "
" ", 147, 0.0035,"1045.20 ","1289.103 ","DLC"," LAP type=DDP Long"
" ", 147, 0.0035,"1045.20 ","1289.103 ","DDP","D=1045.20 S=1289.103 Type=3 (ATP)"
" ", 147, 0.0035,"1045.20 ","1289.103 ","ATP","C ID=2674 LEN=0"
" ", 147, 0.0035,"1045.20 ","1289.103 ","ASP","C CloseSess ID=49"
" ", 150, 0.0194,"1289.103 ","1045.20 ","DLC"," LAP type=DDP Long"
" ", 150, 0.0194,"1289.103 ","1045.20 ","DDP","D=1289.103 S=1045.20 Type=3 (ATP)"
" ", 150, 0.0194,"1289.103 ","1045.20 ","ATP","R ID=2674 LEN=0 NS=0 "
" ", 150, 0.0194,"1289.103 ","1045.20 ","ASP","R CloseSess "
```

Figure 4–34. Delimited format (all levels).

Choosing Page Titles

You can choose whether to include page titles for each page. Page titles specify the date and time the data was recorded, the network name (for a "live" capture) or the name of the file (for a capture from a file), and the page number. There are two blank lines between the heading and the start of the data.

If you enable the **Print page titles** option, you also cause explicit page breaks because the Sniffer analyzer includes a form-feed character after the last non-blank line of each page.

Note that this option is automatically disabled if you enable the **Delimited format** option. This is because most applications that accept the delimited format do not accept page titles.

Choosing Page Size

You can also set the page size, which determines the number of lines per page. The default is 50 lines. Depending on whether you enabled the **Print page titles** option, this setting would result in either 50 printed lines or, with a page title, two blank lines and 47 lines of data. Since each page break is indicated by an explicit form feed, there is no separate setting for the physical length of the paper.

Background Information: Protocol Interpretation

This section provides background information useful to understanding the contents of the Sniffer analyzer displays.

Transmission of 6-Byte DLC Addresses

At the DLC level, every station using 6-byte addressing has a unique address. To be more precise, a DLC address uniquely identifies a station's network interface card. The first three bytes of a DLC address identify the adapter card's manufacturer. The IEEE has assigned codes to the various manufacturers. Each manufacturer uses the other three bytes to assign a unique identifier to each of its cards.

Bits on the Wire vs. Bits in Memory

Historically, the various network technologies have had different rules for converting bits "on the wire" to bits in computer memory. Some systems transmit each byte high-order bit first and some transmit low-order bit first. Suppose a byte of computer memory contains the value that in hexadecimal is written 87. In memory, that consists of the following bits:

```
1 Ø Ø Ø  Ø 1 1 1
   8        7
```

If you could see the sequence of bits transmitted along an FDDI or 802.5 ring cable, you would see that each byte is transmitted with the high-order bits first, 1 0 0 0 0 1 1 1. However, if you could make the same observation on Ethernet, you would see that each byte is transmitted with the low-order bit first. For example, you would see hex 87 go by as 1 1 1 0 0 0 0 1.

Ordinarily, these different ways of transmitting are completely invisible to any user or program. The adapter card translates between bits on the wire and bits in computer memory. You see only bytes in memory before they are sent or after they are received, but never while they are in transit. When an Ethernet card receives the sequence 1 1 1 0 0 0 0 1, it turns that sequence into hex 87, and the receiving station has the same value as the sender. Since (at the DLC level) sender and receiver must be on the same network and must use compatible equipment, a byte in the sender's memory results in the same byte in the receiver's memory.

Consequence of the IEEE standard

When the IEEE assigned codes to the various manufacturers, it specified the sequence in which bits are transmitted on the wire. It did not specify what the sender or receiver would see in memory. For example, Network General Corporation was assigned a particular sequence of bits. To transmit that sequence on token ring, a Sniffer analyzer has in its memory the bytes 00 00 A6. But to transmit that same sequence on Ethernet, the Sniffer's memory must contain the bytes 00 00 65 because A6, with the bits of each byte reversed, is 65.

Thus, to comply with the IEEE standard, a given manufacturer ID should translate to one number for Ethernet (or any other network using low-order bit -first), and to a different number for token ring. (At present, token ring is the only network using high-order bit first.) The tables that the analyzer uses to interpret manufacturers' codes make allowances for this. There is one table for token ring and a different table for other networks. Some manufacturers, however, do not follow the IEEE standard and use the same value in memory for both network types.

Protocol Interpretation

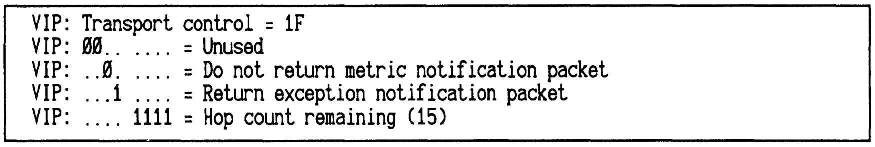
The Sniffer analyzer gets its ability to interpret protocols from several sources. Interpretation for protocols at the lowest level is included in the software that supports the type of network that the analyzer monitors. Interpreters for higher-level protocols are available in suites.

The interpreters from these different sources are linked into the Sniffer analyzer's executable file when it is built. Each protocol interpreter registers its presence and facilities with the analyzer, which permits each interpreter to be represented in the appropriate menus and displays. In the Detail view, in the left column of every line, each interpreter shows the abbreviation of the protocol it is decoding.

While a common registration and display procedure applies to all of the interpreters, the various interpreters are nevertheless essentially independent, just as the protocols themselves are essentially independent. Within each protocol, the fields displayed are those that make sense within the context of the protocol.

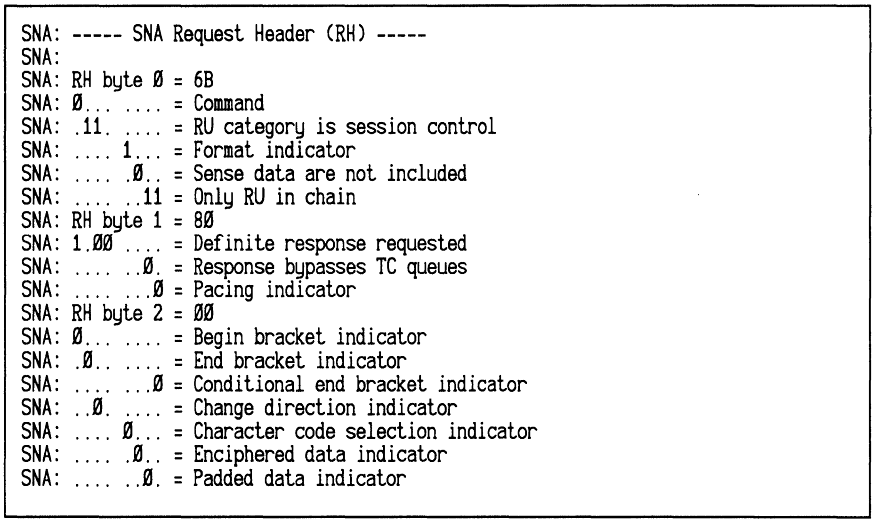
Bit-Level Interpretation

A protocol may record binary attributes as individual bits packed within a single byte. Where that is done, the interpreters often explode each byte to show its eight bits separately. Figure 4–35 illustrates the interpretation of hex 1F at a particular position in the Banyan VINES protocol called VIP. Figure 4–36 shows an interpretation of the sequence 6B 80 00 from an IBM SNA header. This sort of decoding interprets not only the meaning of each bit set at a certain position, but also the meaning of each bit *not* set (that is, each 0). Bit-level interpretation is included in almost all protocols; however, in X Windows it is not universally shown, because the number of possible bit-encodings is extremely large.



```
VIP: Transport control = 1F
VIP: ØØ.. .... = Unused
VIP: ..Ø. .... = Do not return metric notification packet
VIP: ...1 .... = Return exception notification packet
VIP: .... 1111 = Hop count remaining (15)
```

Figure 4–35. Bit-by-bit interpretation of a byte of VINES internet protocol.



```
SNA: ----- SNA Request Header (RH) -----
SNA:
SNA: RH byte Ø = 6B
SNA: Ø... .... = Command
SNA: .11. .... = RU category is session control
SNA: .... 1... = Format indicator
SNA: .... .Ø.. = Sense data are not included
SNA: .... ..11 = Only RU in chain
SNA: RH byte 1 = 8Ø
SNA: 1.ØØ .... = Definite response requested
SNA: .... ..Ø. = Response bypasses TC queues
SNA: .... ...Ø = Pacing indicator
SNA: RH byte 2 = ØØ
SNA: Ø... .... = Begin bracket indicator
SNA: .Ø.. .... = End bracket indicator
SNA: .... ...Ø = Conditional end bracket indicator
SNA: ..Ø. .... = Change direction indicator
SNA: .... Ø... = Character code selection indicator
SNA: .... .Ø.. = Enciphered data indicator
SNA: .... ..Ø. = Padded data indicator
```

Figure 4–36. Bit-by-bit interpretation of three SNA bytes on token ring.

Alternate Displays for ASN.1-Encoded Protocols

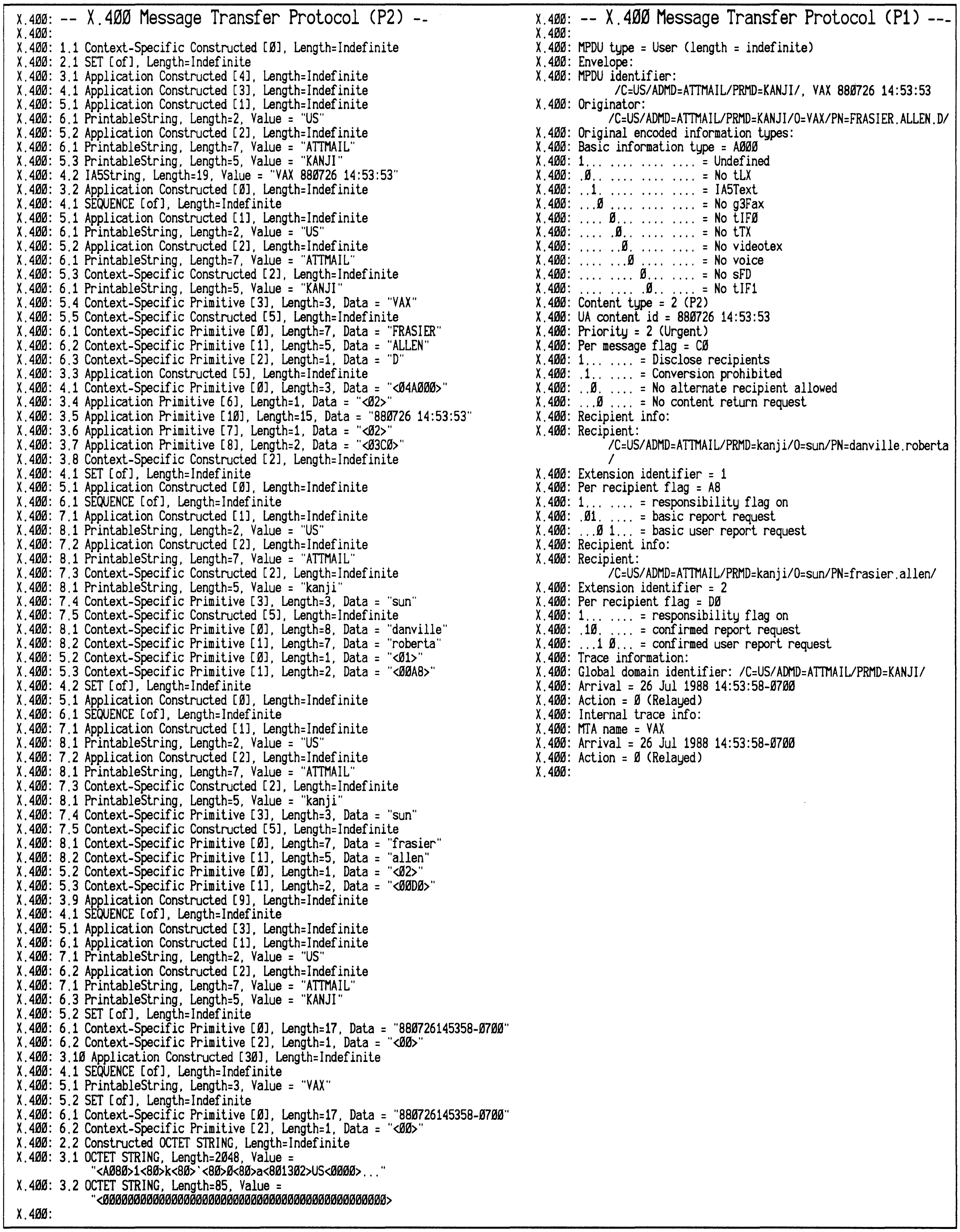
ISO protocols at the presentation and application levels can be interpreted in two modes. Each is written so that it conforms to a general syntax specified in ASN.1 (Abstract Syntax Notation 1, ISO 8825). The individual protocols then assign meanings to the components identified by the ASN.1 syntax. To accommodate this dual level of interpretation, the ISO protocol interpreter suite gives you the option to interpret frames in these layers in either of two ways:

Syntactic — The Sniffer analyzer labels the ASN.1 components within each frame.

Semantic — The analyzer interprets what the various ASN.1 statements mean, according to the rules of the particular protocol in which the ASN.1 statements occur.

When you select interpretation at the X.400 level, you get the semantic interpretation. To see ASN.1 interpretation, disable X.400 in the protocol display filter.

Figure 4–37 shows the same fragment of an X.400 frame interpreted first for ASN.1 syntax and then for its content as part of a P1 message envelope.



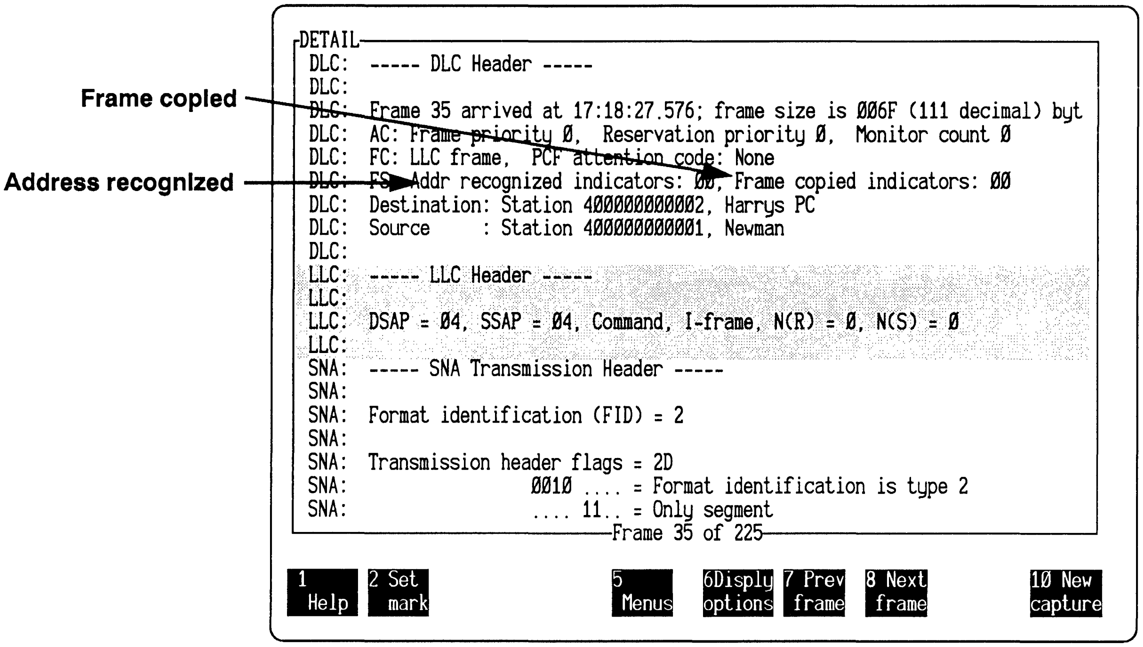
```
X.4ØØ: -- X.4ØØ Message Transfer Protocol (P2) --
X.4ØØ:
X.4ØØ: 1.1 Context-Specific Constructed [Ø], Length=Indefinite
X.4ØØ: 2.1 SET [of], Length=Indefinite
X.4ØØ: 3.1 Application Constructed [4], Length=Indefinite
X.4ØØ: 4.1 Application Constructed [3], Length=Indefinite
X.4ØØ: 5.1 Application Constructed [1], Length=Indefinite
X.4ØØ: 6.1 PrintableString, Length=2, Value = "US"
X.4ØØ: 5.2 Application Constructed [2], Length=Indefinite
X.4ØØ: 6.1 PrintableString, Length=7, Value = "ATTMAIL"
X.4ØØ: 5.3 PrintableString, Length=5, Value = "KANJI"
X.4ØØ: 4.2 IA5String, Length=19, Value = "VAX 88Ø726 14:53:53"
X.4ØØ: 3.2 Application Constructed [Ø], Length=Indefinite
X.4ØØ: 4.1 SEQUENCE [of], Length=Indefinite
X.4ØØ: 5.1 Application Constructed [1], Length=Indefinite
X.4ØØ: 6.1 PrintableString, Length=2, Value = "US"
X.4ØØ: 5.2 Application Constructed [2], Length=Indefinite
X.4ØØ: 6.1 PrintableString, Length=7, Value = "ATTMAIL"
X.4ØØ: 5.3 Context-Specific Constructed [2], Length=Indefinite
X.4ØØ: 6.1 PrintableString, Length=5, Value = "KANJI"
X.4ØØ: 5.4 Context-Specific Primitive [3], Length=3, Data = "VAX"
X.4ØØ: 5.5 Context-Specific Constructed [5], Length=Indefinite
X.4ØØ: 6.1 Context-Specific Primitive [Ø], Length=7, Data = "FRASIER"
X.4ØØ: 6.2 Context-Specific Primitive [1], Length=5, Data = "ALLEN"
X.4ØØ: 6.3 Context-Specific Primitive [2], Length=1, Data = "D"
X.4ØØ: 3.3 Application Constructed [5], Length=Indefinite
X.4ØØ: 4.1 Context-Specific Primitive [Ø], Length=3, Data = "<Ø4AØØØ>"
X.4ØØ: 3.4 Application Primitive [6], Length=1, Data = "<Ø2>"
X.4ØØ: 3.5 Application Primitive [1Ø], Length=15, Data = "88Ø726 14:53:53"
X.4ØØ: 3.6 Application Primitive [7], Length=1, Data = "<Ø2>"
X.4ØØ: 3.7 Application Primitive [8], Length=2, Data = "<Ø3CØ>"
X.4ØØ: 3.8 Context-Specific Constructed [2], Length=Indefinite
X.4ØØ: 4.1 SET [of], Length=Indefinite
X.4ØØ: 5.1 Application Constructed [Ø], Length=Indefinite
X.4ØØ: 6.1 SEQUENCE [of], Length=Indefinite
X.4ØØ: 7.1 Application Constructed [1], Length=Indefinite
X.4ØØ: 8.1 PrintableString, Length=2, Value = "US"
X.4ØØ: 7.2 Application Constructed [2], Length=Indefinite
X.4ØØ: 8.1 PrintableString, Length=7, Value = "ATTMAIL"
X.4ØØ: 7.3 Context-Specific Constructed [2], Length=Indefinite
X.4ØØ: 8.1 PrintableString, Length=5, Value = "kanji"
X.4ØØ: 7.4 Context-Specific Primitive [3], Length=3, Data = "sun"
X.4ØØ: 7.5 Context-Specific Constructed [5], Length=Indefinite
X.4ØØ: 8.1 Context-Specific Primitive [Ø], Length=8, Data = "danville"
X.4ØØ: 8.2 Context-Specific Primitive [1], Length=7, Data = "roberta"
X.4ØØ: 5.2 Context-Specific Primitive [Ø], Length=1, Data = "<Ø1>"
X.4ØØ: 5.3 Context-Specific Primitive [1], Length=2, Data = "<ØØA8>"
X.4ØØ: 4.2 SET [of], Length=Indefinite
X.4ØØ: 5.1 Application Constructed [Ø], Length=Indefinite
X.4ØØ: 6.1 SEQUENCE [of], Length=Indefinite
X.4ØØ: 7.1 Application Constructed [1], Length=Indefinite
X.4ØØ: 8.1 PrintableString, Length=2, Value = "US"
X.4ØØ: 7.2 Application Constructed [2], Length=Indefinite
X.4ØØ: 8.1 PrintableString, Length=7, Value = "ATTMAIL"
X.4ØØ: 7.3 Context-Specific Constructed [2], Length=Indefinite
X.4ØØ: 8.1 PrintableString, Length=5, Value = "kanji"
X.4ØØ: 7.4 Context-Specific Primitive [3], Length=3, Data = "sun"
X.4ØØ: 7.5 Context-Specific Constructed [5], Length=Indefinite
X.4ØØ: 8.1 Context-Specific Primitive [Ø], Length=7, Data = "frasier"
X.4ØØ: 8.2 Context-Specific Primitive [1], Length=5, Data = "allen"
X.4ØØ: 5.2 Context-Specific Primitive [Ø], Length=1, Data = "<Ø2>"
X.4ØØ: 5.3 Context-Specific Primitive [1], Length=2, Data = "<ØØDØ>"
X.4ØØ: 3.9 Application Constructed [9], Length=Indefinite
X.4ØØ: 4.1 SEQUENCE [of], Length=Indefinite
X.4ØØ: 5.1 Application Constructed [3], Length=Indefinite
X.4ØØ: 6.1 Application Constructed [1], Length=Indefinite
X.4ØØ: 7.1 PrintableString, Length=2, Value = "US"
X.4ØØ: 6.2 Application Constructed [2], Length=Indefinite
X.4ØØ: 7.1 PrintableString, Length=7, Value = "ATTMAIL"
X.4ØØ: 6.3 PrintableString, Length=5, Value = "KANJI"
X.4ØØ: 5.2 SET [of], Length=Indefinite
X.4ØØ: 6.1 Context-Specific Primitive [Ø], Length=17, Data = "88Ø726145358-Ø7ØØ"
X.4ØØ: 6.2 Context-Specific Primitive [2], Length=1, Data = "<ØØ>"
X.4ØØ: 3.1Ø Application Constructed [3Ø], Length=Indefinite
X.4ØØ: 4.1 SEQUENCE [of], Length=Indefinite
X.4ØØ: 5.1 PrintableString, Length=3, Value = "VAX"
X.4ØØ: 5.2 SET [of], Length=Indefinite
X.4ØØ: 6.1 Context-Specific Primitive [Ø], Length=17, Data = "88Ø726145358-Ø7ØØ"
X.4ØØ: 6.2 Context-Specific Primitive [2], Length=1, Data = "<ØØ>"
X.4ØØ: 2.2 Constructed OCTET STRING, Length=Indefinite
X.4ØØ: 3.1 OCTET STRING, Length=2Ø48, Value =
           "<AØ8Ø>1<8Ø>k<8Ø>`<8Ø>Ø<8Ø>a<8Ø13Ø2>US<ØØØØ>..."
X.4ØØ: 3.2 OCTET STRING, Length=85, Value =
           "<ØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØØ>
X.4ØØ:
```

```
X.4ØØ: -- X.4ØØ Message Transfer Protocol (P1) ---
X.4ØØ:
X.4ØØ: MPDU type = User (length = indefinite)
X.4ØØ: Envelope:
X.4ØØ: MPDU identifier:
            /C=US/ADMD=ATTMAIL/PRMD=KANJI/, VAX 88Ø726 14:53:53
X.4ØØ: Originator:
           /C=US/ADMD=ATTMAIL/PRMD=KANJI/O=VAX/PN=FRASIER.ALLEN.D/
X.4ØØ: Original encoded information types:
X.4ØØ: Basic information type = AØØØ
X.4ØØ: 1... .... .... .... = Undefined
X.4ØØ: .Ø.. .... .... .... = No tLX
X.4ØØ: ..1. .... .... .... = IA5Text
X.4ØØ: ...Ø .... .... .... = No g3Fax
X.4ØØ: .... Ø... .... .... = No tIFØ
X.4ØØ: .... .Ø.. .... .... = No tTX
X.4ØØ: .... ..Ø. .... .... = No videotex
X.4ØØ: .... ...Ø .... .... = No voice
X.4ØØ: .... .... Ø... .... = No sFD
X.4ØØ: .... .... .Ø.. .... = No tIF1
X.4ØØ: Content type = 2 (P2)
X.4ØØ: UA content id = 88Ø726 14:53:53
X.4ØØ: Priority = 2 (Urgent)
X.4ØØ: Per message flag = CØ
X.4ØØ: 1... .... = Disclose recipients
X.4ØØ: .1.. .... = Conversion prohibited
X.4ØØ: ..Ø. .... = No alternate recipient allowed
X.4ØØ: ...Ø .... = No content return request
X.4ØØ: Recipient info:
X.4ØØ: Recipient:
           /C=US/ADMD=ATTMAIL/PRMD=kanji/O=sun/PN=danville.roberta
           /
X.4ØØ: Extension identifier = 1
X.4ØØ: Per recipient flag = A8
X.4ØØ: 1... .... = responsibility flag on
X.4ØØ: .Ø1. .... = basic report request
X.4ØØ: ...Ø 1... = basic user report request
X.4ØØ: Recipient info:
X.4ØØ: Recipient:
           /C=US/ADMD=ATTMAIL/PRMD=kanji/O=sun/PN=frasier.allen/
X.4ØØ: Extension identifier = 2
X.4ØØ: Per recipient flag = DØ
X.4ØØ: 1... .... = responsibility flag on
X.4ØØ: .1Ø. .... = confirmed report request
X.4ØØ: ...1 Ø... = confirmed user report request
X.4ØØ: Trace information:
X.4ØØ: Global domain identifier: /C=US/ADMD=ATTMAIL/PRMD=KANJI/
X.4ØØ: Arrival = 26 Jul 1988 14:53:58-Ø7ØØ
X.4ØØ: Action = Ø (Relayed)
X.4ØØ: Internal trace info:
X.4ØØ: MTA name = VAX
X.4ØØ: Arrival = 26 Jul 1988 14:53:58-Ø7ØØ
X.4ØØ: Action = Ø (Relayed)
X.4ØØ:
```

Figure 4–37. ASN.1 syntactic and semantic interpretations of the same X.400 layer of an ISO frame.

Token Ring "Address Recognized" and "Frame Copied" Bits

As each frame circulates on the token ring, it has one extra "trailer" byte at the end. The trailer is used to check the frame's validity. It usually is not considered part of the frame and it does not appear in the Hex view. However, the Detail view reports the status of two indicators in the trailer: the address recognized bits and the frame copied bits. These bits are visible in Figure 4–38 as part of the Detail view's DLC report.



Frame copied

Address recognized

```
DETAIL
DLC:  ----- DLC Header -----
DLC:
DLC:  Frame 35 arrived at 17:18:27.576; frame size is ØØ6F (111 decimal) byt
DLC:  AC: Frame priority Ø,  Reservation priority Ø,  Monitor count Ø
DLC:  FC: LLC frame,  PCF attention code: None
DLC:  FS: Addr recognized indicators: ØØ, Frame copied indicators: ØØ
DLC:  Destination: Station 4ØØØØØØØØØØ2, Harrys PC
DLC:  Source     : Station 4ØØØØØØØØØØ1, Newman
DLC:
LLC:  ----- LLC Header -----
LLC:
LLC:  DSAP = Ø4, SSAP = Ø4, Command, I-frame, N(R) = Ø, N(S) = Ø
LLC:
SNA:  ----- SNA Transmission Header -----
SNA:
SNA:  Format identification (FID) = 2
SNA:
SNA:  Transmission header flags = 2D
SNA:                 ØØ1Ø .... = Format identification is type 2
SNA:                 .... 11.. = Only segment
                          Frame 35 of 225
```

Figure 4–38. Detail view showing token ring "address recognized" and "frame copied" bits.

When a station recognizes itself in the frame's destination, it sets the *address recognized* bits. If those bits are on when the frame reaches you, at least one station upstream from you has recognized itself as a recipient. (A frame sent to a functional address may have any number of recipients.)

When a station retains a copy of the frame, it sets the *frame copied* bits. Normally, a recipient both recognizes and records the frame, and sets both bits.

The values you see for *addressed recognized* and *frame copied* depend on where you are located. If a frame reaches you with *address recognized* bits already set, the frame must have reached the recipient before it reached you. When you're looking for problems at a particular portion of the ring, you may want to capture from different positions. The *address recognized* bits provide evidence of your position in the ring sequence. To verify that a station has accepted frames addressed to it, you have to be upstream from the sender and downstream from the recipient. (That is, you must not be between the sender and recipient in ring order.)

CHAPTER FIVE: MANAGING NAMES AND WORKING WITH FILES 5

Managing Names and Working with Files

Overview

This chapter describes how to manage the information in the Sniffer analyzer's name table and how to manage files that contain either captured frames or the various analyzer options and parameters you defined. It includes the following topics:

- Managing the name table to include station names in the displays.
- Saving captured frames to data files, which you can use to load the capture buffer or when using the **Traffic generator** feature.
- Saving the combination of options you define to the startup file or to setup files. The options in the startup file are automatically applied at system startup. You can apply the options in the setup files at any time, as necessary.

Managing Names

To make its displays more readable, the Sniffer analyzer displays the names associated with captured addresses. To find the names that correspond to the addresses, the analyzer refers to its name table, contained in the file STARTUP.xxD.

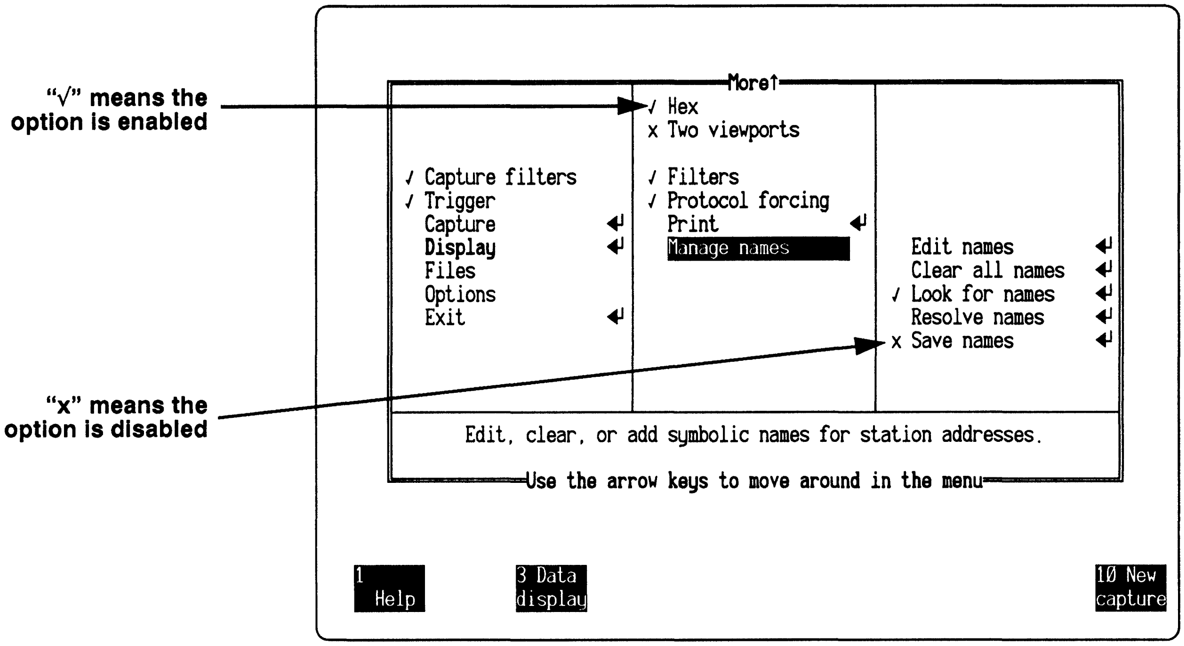
The name table can contain up to 500 pairs of addresses and names. There are various ways to associate names with addresses, including:

- Manually editing the name table
- Using external files to add user-defined names to DLC addresses
- Using a feature that automatically adds system-assigned names to higher-level addresses

Note: You can increase the number of addresses in the name table to a maximum of 8000 by resetting the value for the associated parameter. For instructions, refer to "Editing the Startup Parameters" on page 9–18.

Once the name table contains the addresses and names you need, you can save that table so that it is used automatically the next time you start up the Sniffer analyzer. The sections that follow explain these options in more detail.

Figure 5–1 shows the menu options associated with managing the name table.



Edit, clear, or add symbolic names for station addresses.

Use the arrow keys to move around in the menu

"√" means the option is enabled

"x" means the option is disabled

Figure 5–1. Managing the name table.

About the Name Table

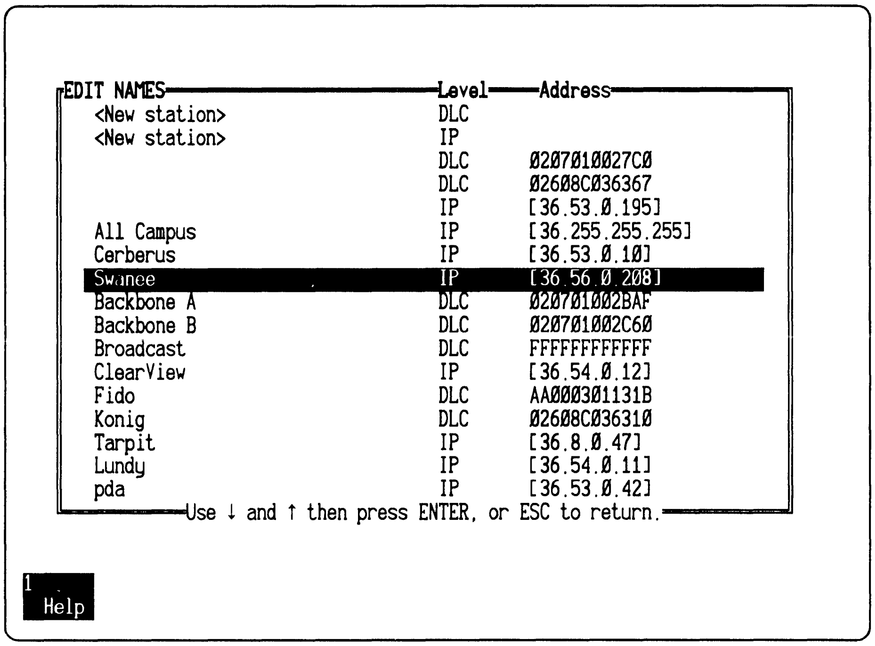
When you start the Sniffer analyzer, the name table is loaded from the startup file and becomes the working name table.

The name table contains three columns, shown in Figure 5–2:

Address layer The protocol in which the address can occur.

Station address The sequence of bytes of the numeric station address.

Symbolic name The name assigned to the address. If no name is assigned, this column is blank.



```
EDIT NAMES                                  Level    Address
   <New station>                            DLC
   <New station>                            IP
                                            DLC      Ø2Ø7Ø1ØØ27CØ
                                            DLC      Ø26Ø8CØ36367
                                            IP       [36.53.Ø.195]
   All Campus                               IP       [36.255.255.255]
   Cerberus                                 IP       [36.53.Ø.1Ø]
   Swanee                                   IP       [36.56.Ø.2Ø8]
   Backbone A                               DLC      Ø2Ø7Ø1ØØ2BAF
   Backbone B                               DLC      Ø2Ø7Ø1ØØ2C6Ø
   Broadcast                                DLC      FFFFFFFFFFFF
   ClearView                                IP       [36.54.Ø.12]
   Fido                                     DLC      AAØØØ3Ø1131B
   Konig                                    DLC      Ø26Ø8CØ3631Ø
   Tarpit                                   IP       [36.8.Ø.47]
   Lundy                                    IP       [36.54.Ø.11]
   pda                                      IP       [36.53.Ø.42]
          Use ↓ and ↑ then press ENTER, or ESC to return.

1
 Help
```

Figure 5–2. Sample working name table.

Note that a station address never exists alone. Instead, it is always paired with a specific protocol. A symbolic name is thus an equivalent not just for an address, but also for a particular pairing of a protocol and address.

How the Name Table Is Built

The working name table is built and used in a sequence of stages:

Initialization When the Sniffer analyzer is launched, it initializes the working name table with names and addresses in the file STARTUP.xxD. It also inserts its own address and assigns itself the name "This Sniffer," even when the saved table previously assigned it a different name.

Capture During capture, the capture views show either the station names, if they exist in the name table, or the stations addresses.

First display The first time you display interpreted data after a new capture, the Sniffer analyzer scans all the frames in the buffer for new addresses. It enters new addresses into the working name table with blank names.

Display During display, the analyzer checks its name table for the address of each frame that appears in the Summary or Detail view. If it finds unnamed addresses, it adds them to the name table, up to 50 for each address level.

Editing You can edit the working name table at any time during capture or display. This includes adding new addresses, naming addresses, editing existing names, or deleting names and addresses.

Taking Advantage of the Automatic Address Scan

The first time you display captured frames after a new capture, the Sniffer analyzer scans the capture buffer for addresses, including all address layers. During its scan for new addresses, the analyzer stops adding addresses when the table is full (default is 500 addresses, possible maximum is 8000). Also, it never adds more than 50 addresses at any level, even when there is room.

When the analyzer finds a new address, it adds that address to the top of the working name table, with a blank name field. Once an address exists in the name table you can assign it a name. (Of course, you can also add both the address and the name manually.)

Addresses that are not named are purged when you exit the Sniffer analyzer. Therefore, if you want to save new addresses, be sure to assign them a name.

Assigning Names to Addresses

There are three options that allow you to assign names to addresses.

Edit names You can manually enter a name for each unnamed address.

Resolve names The Sniffer analyzer searches a file that contains a previously saved name table for any named DLC addresses that match the unnamed addresses in the working name table. If it finds these addresses, it copies the names from the file to the working name table.

Look for names Certain protocols allow stations to exchange tables of higher-level addresses and associated names. This option scans the capture buffer for such messages and adds such pairs to the working name table.

Manually Editing the Name Table

The easiest way to manually edit the name table is to start a capture to compile a list of addresses automatically and then assign names to those addresses manually.

To edit the working name table:

1. Before you open the name table, compile a list of the addresses.

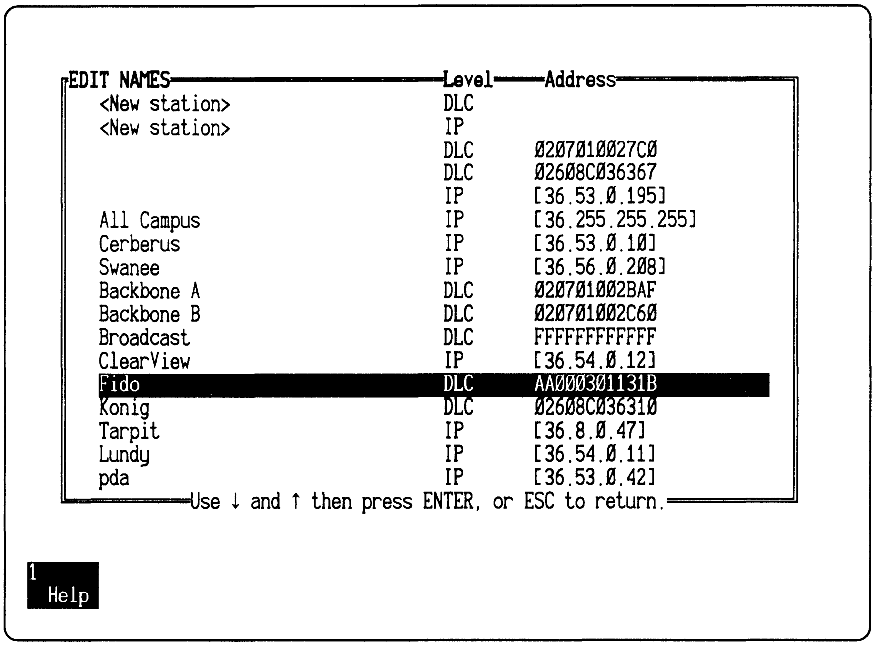
   a. Press F10 (**Start capture**) to capture frames (either live from the network or from a saved file). Press F10 (**Stop capture**) to stop the capture.

   b. Move to **Display** and press Enter (or press F3).

2. Press F6 (**Display options**).

3. Move to **Manage names** and press Enter to display the current name table.

   In this table (shown in Figure 5–3), each name consists of a pairing of a protocol layer and an address. For example, the name *Fido* is associated with the DLC layer and address AA0003 01131B. The name *Tarpit* is associated with the IP layer and address [36.8.0.47]. The DLC layer is always present.

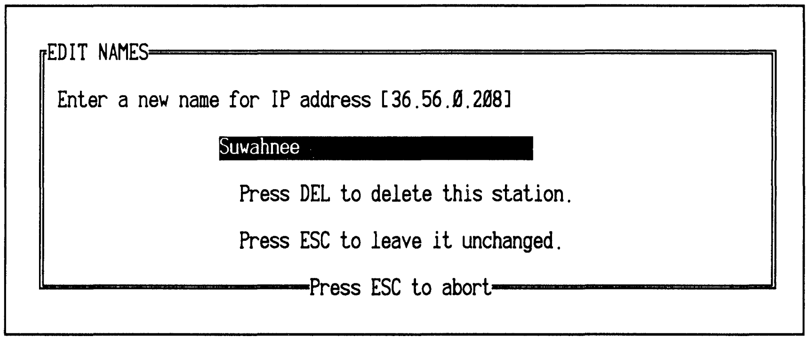


```
EDIT NAMES                                 Level   Address
   <New station>                           DLC
   <New station>                           IP
                                           DLC     Ø2Ø7Ø1ØØ27CØ
                                           DLC     Ø26Ø8CØ36367
                                           IP      [36.53.Ø.195]
   All Campus                              IP      [36.255.255.255]
   Cerberus                                IP      [36.53.Ø.1Ø]
   Swanee                                  IP      [36.56.Ø.2Ø8]
   Backbone A                              DLC     Ø2Ø7Ø1ØØ2BAF
   Backbone B                              DLC     Ø2Ø7Ø1ØØ2C6Ø
   Broadcast                               DLC     FFFFFFFFFFFF
   ClearView                               IP      [36.54.Ø.12]
   Fido                                    DLC     AAØØØ3Ø1131B
   Konig                                   DLC     Ø26Ø8CØ3631Ø
   Tarpit                                  IP      [36.8.Ø.47]
   Lundy                                   IP      [36.54.Ø.11]
   pda                                     IP      [36.53.Ø.42]
            Use ↓ and ↑ then press ENTER, or ESC to return.
```

Figure 5–3. Editing the working name table.

4. To edit an existing name, move to the item you want to change and press Enter.

   In the dialog box that appears, enter the new name (Figure 5–4).



```
EDIT NAMES

Enter a new name for IP address [36.56.Ø.2Ø8]

                  Suwahnee

                   Press DEL to delete this station.

                   Press ESC to leave it unchanged.

                          Press ESC to abort
```

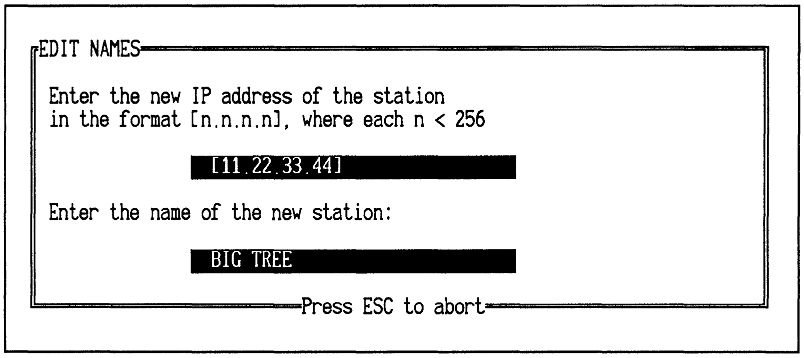
Figure 5–4. Changing an existing name.

5. To add a name to an unnamed address, move to that address near the top of the list and press Enter. In the dialog box that appears, enter the desired name.

6. To add an address that is not in the list, move to the top of the list to the line **<new station>** that has the appropriate protocol layer. Press Enter.

   Note: Each **<new station>** line is identified by its layer. There is always a line for the DLC layer. In addition, there is a line for each layer enabled in the **Address level** filter.

   In the dialog box that appears, enter the address (Figure 5–5).



```
EDIT NAMES

Enter the new IP address of the station
in the format [n.n.n.n], where each n < 256

            [11.22.33.44]

Enter the name of the new station:

            BIG TREE

              Press ESC to abort
```

Figure 5–5. Entering a station's name and address.

When you use the **Edit Names** option to edit the name table, only the *working name table is affected.* If the **Save names** option is enabled (the default), the Sniffer analyzer automatically updates the startup file with new address and name pairs. If the option is disabled, you can save manually by moving to **Save Names** and pressing Enter.

Using Name Files to Resolve Names

Instead of—or in addition to—manually editing the name table, you can use name files that contain name tables (saved under different names) that identify unnamed DLC addresses. These files have the same format as the file STARTUP.*xx*D.

You can create name files by copying and renaming the current version of the STARTUP.*xx*D file or by creating them with a text editor. Note that these files must have the identifying extension .*xx*D and that they must be in the same format as the STARTUP.*xx*D file. The requirements for name files are described in Chapter 9, "Using the Sniffer Analyzer Files."

How the Resolve Names Option Works

After scanning the capture buffer, the Sniffer analyzer adds to the working name table all addresses that are not named, at all address levels. This results in a list of unnamed stations, including unnamed stations in the capture buffer and unnamed stations in the name table.

For each address in this list of unnamed stations, the analyzer searches the name file you select. When it finds a name that corresponds to an unnamed address, it inserts that name into the name table.

At the end of the search, a message shows the number of unnamed addresses that were in the working name table and how many of those addresses were resolved by searching the selected name file.

To resolve unnamed stations by searching an external file:

1. Compile a list of the addresses. Press F10 (**New capture**) to capture some frames, either live from the network or from a file. Press F10 (**Stop capture**) to stop the capture.
2. Move to **Display\Manage names\Resolve names** and press Enter.
3. Press F6 (**Display options**). Move to **Manage names\Look for names** and press Enter.

   In response, the analyzer displays a list of name files. Move to the file you want to use and press Enter.
4. To preserve the names you have added, move to **Manage names \Save names** and press Spacebar to enable (√) the option (or simply press Enter). As a result, the names from the working name table are copied to the startup file when you exit. Addresses that still lack names will be discarded.

Looking for Names within the Captured Frames

Certain protocols, including Novell NetBIOS and TCP DNS, automatically assign names to higher-level addresses and allow stations to exchange the resulting tables. When the **Look for names** option is enabled (the default), the Sniffer analyzer automatically scans for such tables during capture and adds the following information to its working name table:

- Names for unnamed addresses that are already in the name table
- Both names and addresses for addresses not yet in the table

It does not, however, revise names for addresses that are already in the table. When it completes the search, the Sniffer analyzer reports the number of address and name pairs it added to the working name table. By using this option, you may also find higher-level addresses that were not sending or receiving frames during a particular period of capture.

If the **Look for names** option is enabled, the Sniffer analyzer automatically updates its working name table with various higher-level addresses and associated names.

To look for names within the frames in the capture buffer:

If the option is disabled, you can:

1. Press F10 (**New capture**) to capture some frames, either live from the network or from a file. Press F10 (**Stop capture**) to stop the capture.

2. Press F3 (**Data display**).
3. Press F6 (**Display options**) and move to **Manage names\Look for names** and press Enter.

   In response, the Sniffer analyzer scans the capture buffer for protocols that exchange name information and adds any new addresses and corresponding names to the working name table.

Names found with the **Look for names** option may be transitory. For example, you may find a name that a user assigned for a single work session. The user may then move to another machine and assign the name to a different address. Because such names are so readily changed, you may not want to save a name table constructed this way; it may be wrong the next time you use it.

Saving the Name Table

When the **Save names** option is enabled, the Sniffer analyzer automatically updates the startup file with the current working name table when you exit, thereby saving any new addresses and names, as well as any changes. If the option is disabled (the default), you must save manually. If you try to exit without saving the names that the Sniffer analyzer may have found and added, a warning message appears that allows you to cancel the Exit command.

Addresses that are not named are purged when you exit the Sniffer analyzer regardless of whether the **Save names** option is enabled. Therefore, if you want to save new addresses, be sure to assign them a name.

To automatically save the current working name table:

1. Move to **Display\Manage names\Save names** and press Spacebar to enable (√) the option.

To manually save the current working name table:

1. Move to **Display\Manage names\Save names** and press Enter.

   In response, the Sniffer copies all named addresses from the working name table to the file c:\xxSNIFF\STARTUP.*xx*D.

Clearing the Name Table

When the startup file contains names that are no longer appropriate, you can either edit them individually or clear all names and start over.

The **Clear all names** option removes both names and addresses from the working name table. Use this option when you want to start over, perhaps before resolving names from a name file or before looking for embedded names within higher-level protocols in the capture buffer.

Using the **Clear all names** followed by the **Save names** option would empty not only the working name table but also the name table in the startup file. Use with caution.

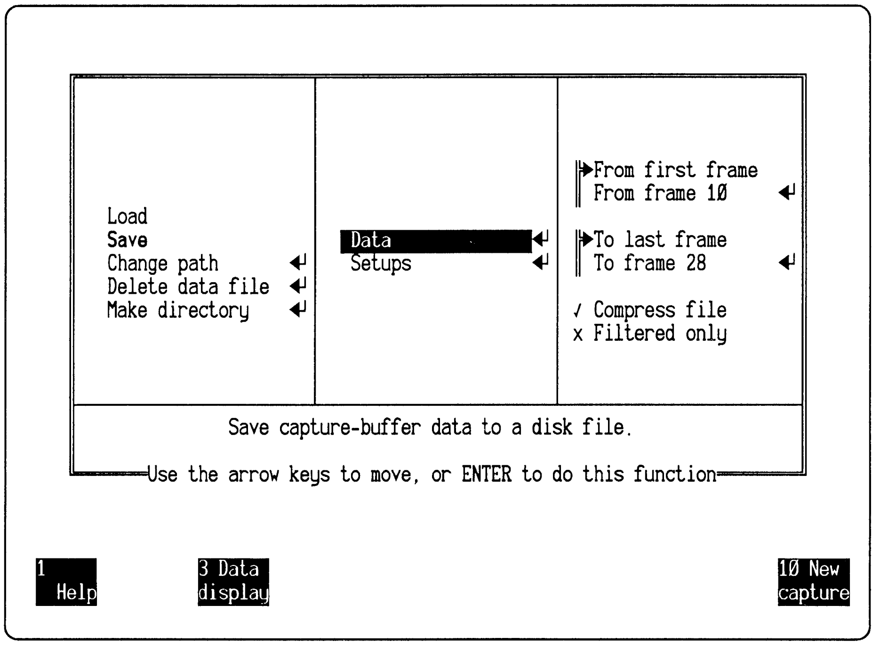
Saving Captured Frames as Data (Trace) Files

You can save the frames in the capture buffer to a file. When saving files, you have the following options:

- Saving everything in the capture buffer
- Saving only those frames that pass the current display filters
- Saving only those frames within a particular range
- Saving any frames you select individually

To save frames in the capture buffer to a file:

1. Press F5 (**Menus**) to return to the main menu. Move to **Files\Save\Data** (shown in Figure 5–6).



Save capture-buffer data to a disk file.

Use the arrow keys to move, or ENTER to do this function

Figure 5–6. Menu to save captured frames to a file.

2. (Optional) Set the range of frames to be saved. If you do not want to use the defaults (from first to last), move to the specific numbers and press Enter. In the dialog box that appears, enter the desired range.

   ▸ From first frame
   From frame xx

   ▸ From last frame
   To frame xx

3. (Optional) To save only those frames you specifically select, display the Summary view, move to each frame you want to select, and press F9 (**Select frame**). Also, make sure you enable the **Selected frames** display filter and redisplay. Continue with step 5.

4. (Optional) To save only those frames that pass the display filters, move to **Filtered only** and press Spacebar to enable (√) the option.

5. To determine whether the file will be saved compressed or uncompressed, move to **Compress files**. Press Spacebar to enable (√) or disable (x) the option.

6. Move to **Data** and press Enter.

   In the dialog box that appears, enter the desired file name (up to eight characters) and press Enter. Do not include an extension; the Sniffer analyzer automatically attaches the extension .*xx*C, where *xx* stands for the network, such as EN for Ethernet, FD for FDDI, or TR for token ring. If a file with that name already exists, you can abort the request or overwrite the existing file.

   The path shows the current drive with the current path (\CAPTURE unless you changed the path). You can backspace over any part of the display and enter the name of a different drive or directory.

Using Data Files to Load the Capture Buffer

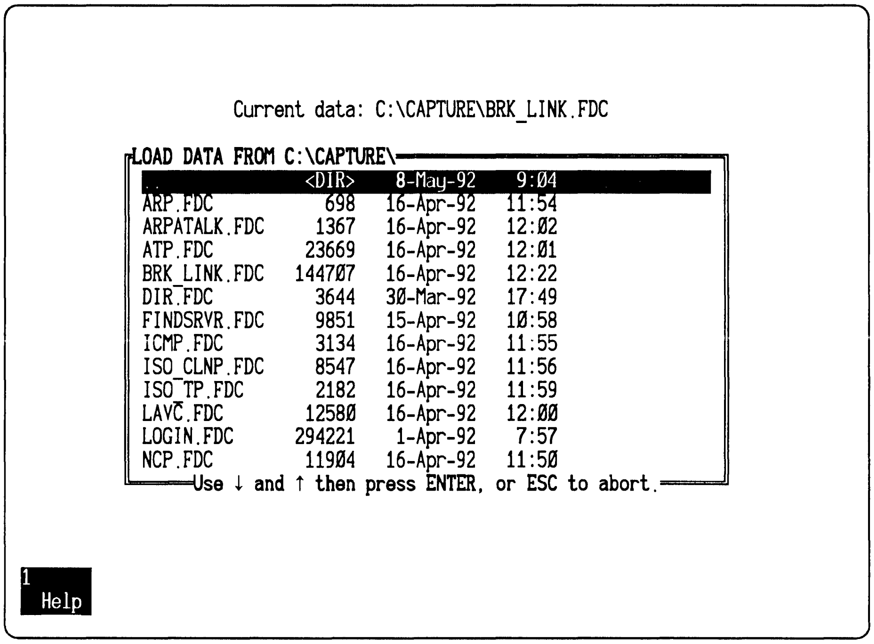
If you save all or part of the capture buffer to a file, you can use the resulting file to load the capture buffer. In this way, you can examine frames captured at another time or place, or frames sent to you for study.

You can load the capture buffer directly from a previously saved file, without starting a capture.

To load the capture buffer with a file of saved frames:

1. Move to **Files\Load\Data** and press Enter.

   In response, a dialog box appears that contains an alphabetical list of previously saved capture files and directories. Each filename includes a three-letter extension. The first two letters of this extension identify the network topology. In Figure 5–7, for example, the extension is FDC, which shows that the files were captured from an FDDI network. This list includes only those filenames with the proper extensions for the current Sniffer Analyzer.



```
                Current data: C:\CAPTURE\BRK_LINK.FDC

LOAD DATA FROM C:\CAPTURE\
 ..                <DIR>   8-May-92    9:04
 ARP.FDC             698  16-Apr-92   11:54
 ARPATALK.FDC       1367  16-Apr-92   12:02
 ATP.FDC           23669  16-Apr-92   12:01
 BRK_LINK.FDC     144707  16-Apr-92   12:22
 DIR.FDC            3644  30-Mar-92   17:49
 FINDSRVR.FDC       9851  15-Apr-92   10:58
 ICMP.FDC           3134  16-Apr-92   11:55
 ISO_CLNP.FDC       8547  16-Apr-92   11:56
 ISO_TP.FDC         2182  16-Apr-92   11:59
 LAVC.FDC          12580  16-Apr-92   12:00
 LOGIN.FDC        294221   1-Apr-92    7:57
 NCP.FDC           11904  16-Apr-92   11:50
      Use ↓ and ↑ then press ENTER, or ESC to abort.
```

Figure 5–7. Loading the capture buffer with a data file.

2. To change to a different directory, move to the top of the list, to one of the rows labeled **<DIR>**. This label lets you select the directory one step nearer the root directory. Other entries with the **<DIR>** label are subdirectories. To see the list of files in a subdirectory, move to the subdirectory name and press Enter.
3. Move to the desired file. (To jump directly to the entries that start with a given letter, type that letter and then move to the desired file.)
4. Press Enter to load the file.
5. Press F3 (**Data display**) to display the analyzed frames from that file, in the display views you defined.

Deleting Data Files

You can delete data files that contain saved frames for the network for which your Sniffer analyzer is configured.

To delete a data file:

1. Move to **Files\Delete data file** and press Enter.
2. In the dialog box that appears, move to the file you want to delete and press Enter. (To move to the desired file quickly, type the first letter of that file. The display jumps to that section of the list.)

   In response, the analyzer displays a Warning dialog box that allows you to cancel the deletion.
3. Press ESC to cancel the deletion or press Enter to complete it.

4. To delete files in other subdirectories, move to **<DIR>** in the top row and press Enter to see the files in that subdirectory. You can then delete any files in that directory.

Using Setup Files to Define System Options

In addition to saving files that contain captured data, you can save the "setup" that includes the particular combination of display options, filters, and controls you defined.

If you want to automatically start your analyzer with a particular combination of options, you can save those options to the STARTUP.*xx*S file in the CAPTURE directory. You can also save options to any number of setup files and then load those file to apply particular settings to a capture session.

Contents of a Setup File

The setup file records every option you enabled or disabled, the choices associated with vertical lines (radio control), and all values associated with various options, such as thresholds, file sizes, and so on.

The following options are included in the setup file:

- General system options, such as the **Audible clicks** option
- Capture options, including the capture mode, screen format, and so on.
- Capture filters, including any pattern matches you defined
- Trigger options, including the options associated with the **Disk snapshot** feature
- Display options, including views to be displayed and any associated options
- Display filters, including any pattern matches you defined
- Printer options, such as range of pages to be printed and the file format
- Protocol forcing rules

The following options are not included in a setup file:

- The path you may have set for locating the directory of files to be loaded or saved. However, you can record this path with the DOS "Set Path" command.
- The capture buffer. You can save the contents of the capture buffer as a data file (**Files\Save\Data**).
- The name table. You can save the current working name table with the **Display\Manage names\Save names** option.

Note: Your setup may refer to addresses (for example, in a station address filter). When you display the filter, you may see the station's symbolic name rather than its numeric address. However, the saved filter does contain the numeric address. The symbolic name will be generated during display, when the Sniffer analyzer checks the name table for names that correspond to addresses.

Saving the Current Options in the STARTUP File

If the options you need are different from the Network General default options, and if you want your options to be in effect automatically, you can save the options you define to the STARTUP file. As a result, whenever you start the Sniffer analyzer, it automatically applies the options in that file.

To save your current setup to the STARTUP file:

1. Check your setup to make sure it defines all options as you want them, especially the filters.
2. Move to **Files\Save\Setup** and press Enter.
3. In the dialog box that appears, type \CAPTURE\STARTUP at the **c:** prompt. Don't include an extension; the Sniffer analyzer automatically attaches the extension .*xx*S

Note: You should always specify a subdirectory (the default is \CAPTURE) after the **c:** prompt, in which you save your data and setup files.

Saving the Current Options as a Setup File

If you want to save a combination of options, but not have them applied automatically at system startup, you can save them to a setup file and then apply them to a particular capture session.

To save your current setup as a setup file:

1. Check your setup to make sure it defines all options as you want them.
2. Move to **Files\Save\Setup** and press Enter.
3. In the dialog box that appears, type a file name, using no more than eight characters. Don't include an extension; the Sniffer analyzer automatically attaches the extension .*xx*S. If that file name is already in use, you can abort the request or overwrite the existing file.

Note: You should always specify a subdirectory (the default is \CAPTURE) after the **c:** prompt, in which you save your data and setup files.

Note: You can delete setup files from the DOS command line, if you like.

Applying a Setup File

When you first start the Sniffer analyzer, it uses the settings in the STARTUP.*xx*S file. If you want to override these settings with a setup file you created, you can do so.

To apply a saved setup file:

1. Move to **Files\Load\Setup** and press Enter.

2. In the dialog box that appears, move to the desired setup file and press Enter.

   In response, the Sniffer analyzer loads the setup file. Although there is no message, the analyzer resets all options as specified in the chosen setup file.

Restoring the Network General Default Options

You may want to restore the default options with which your Sniffer analyzer was shipped. This is particularly useful if you are getting unexpected results and you want to start from a known state. The default options are illustrated in Appendix A.

To restore Network General's default options:

1. Move to **Options\Use defaults** and press Enter.

Caution: This command clears any settings you may have defined. If you think you might want to use these settings again later, save the current settings as a setup file.

CHAPTER SIX: USING PROTOCOL FORCING 6

Using Protocol Forcing

Overview

Protocol forcing is an advanced Sniffer analyzer function that allows you to alter the standard interpretive flow through the stacked data found within a predefined set of frames. The set of frames to which the forcing action is applied and the new direction the interpretation will take are defined by up to four rules you can specify prior to displaying the captured data.

This chapter describes how to use the protocol forcing feature. Topics include:

- Specifying a protocol forcing rule
- Applying a protocol forcing rule
- Undoing protocol forcing

Protocol forcing is an advanced tool for network managers to interpret non-standard (e.g., proprietary) protocol stacks. For protocol forcing to yield meaningful results, a thorough knowledge of the targeted protocol stack, as well as the way it deviates from the standard, is essential.

How Protocol Forcing Works

Under normal data display, the Sniffer analyzer displays your captured data based on the parameters you set up in the Display menu options. If you have a non-standard protocol stack that deviates from a given standard, you can use protocol forcing to set up protocol decoding rules that apply to your networking environment. Once these rules are set up, you can apply them to subsequent data displays and file loading.

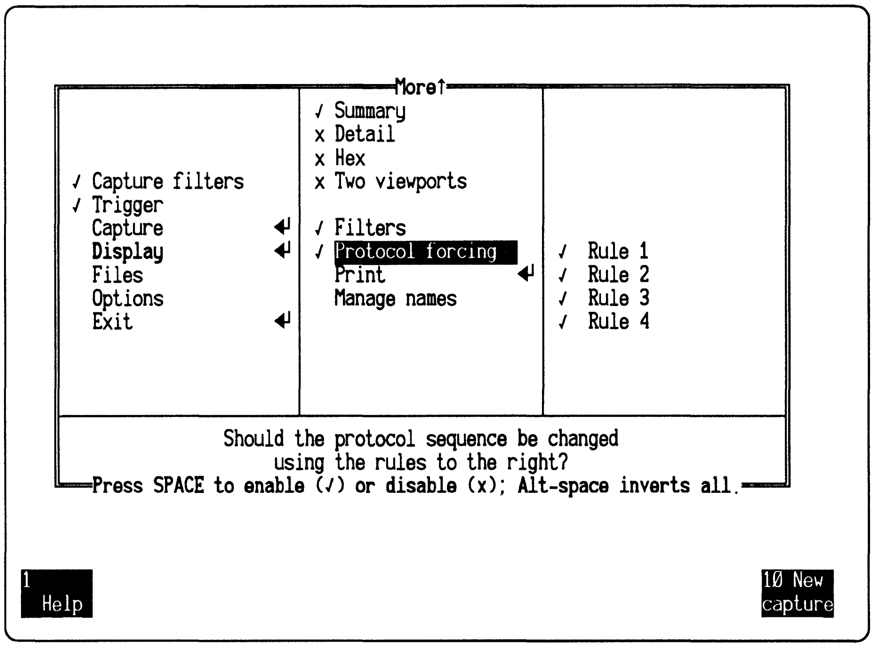
Protocol forcing affects the data display rather than the data in the capture buffer. The type of protocols available depends on the type of analyzer you have. Protocol forcing is available with the following topologies:

- Ethernet
- Token ring
- FDDI
- Sniffer Internetwork Analyzer (WAN/Synchronous)

Specifying a Protocol Forcing Rule

To specify a protocol forcing rule:

1. In the **Display** menu, enable protocol forcing. Move the highlight to **Protocol forcing** and press Spacebar to toggle between disabled (x) and enabled (√). Figure 6–1 displays the menu options for Protocol forcing.

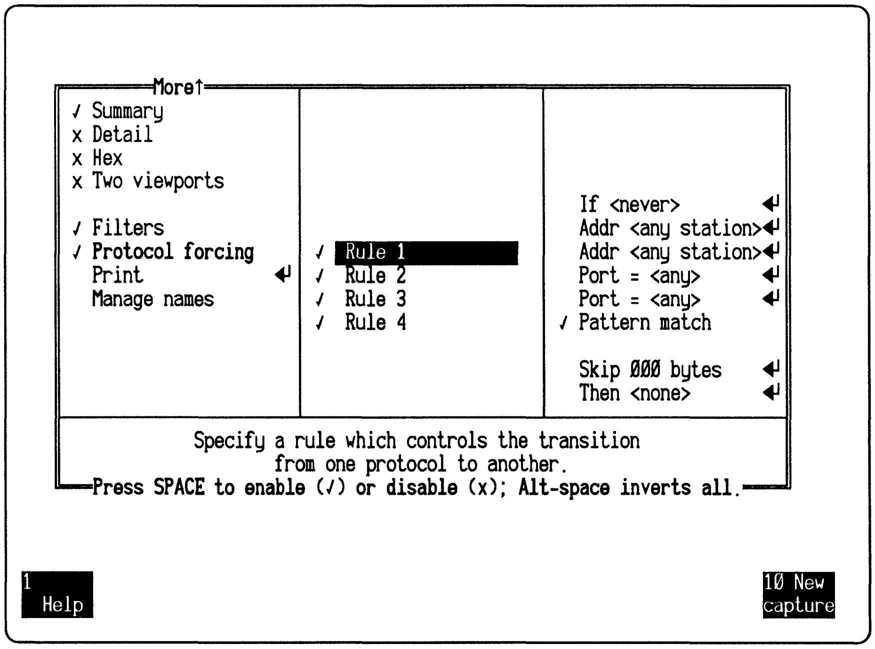


```
                                More↑
                        ✓ Summary
                        x Detail
                        x Hex
 ✓ Capture filters      x Two viewports
 ✓ Trigger
   Capture          ↵   ✓ Filters
   Display          ↵   ✓ Protocol forcing      ✓ Rule 1
   Files                  Print            ↵    ✓ Rule 2
   Options                Manage names          ✓ Rule 3
   Exit             ↵                           ✓ Rule 4

                 Should the protocol sequence be changed
                       using the rules to the right?
 Press SPACE to enable (✓) or disable (x); Alt-space inverts all.

1                                                          10 New
 Help                                                      capture
```

Figure 6–1. Protocol forcing menu options.

2. Move to the panel on the right. **Rule 1** will be highlighted.

   Figure 6–2 displays the options available for **Rule 1**.



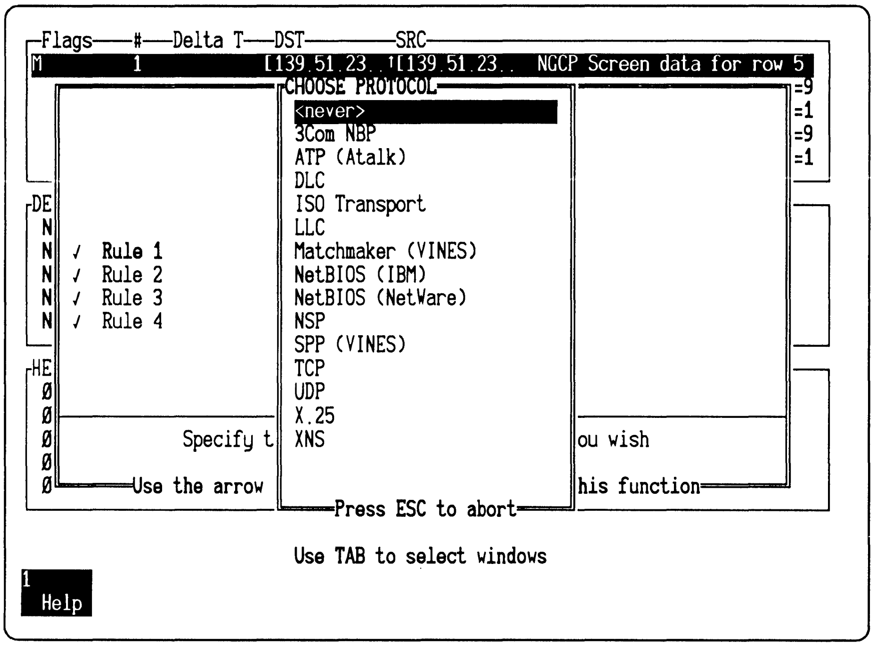
```
            More↑
 ✓ Summary
 x Detail
 x Hex
 x Two viewports
                                                If <never>           ↵
 ✓ Filters                                      Addr <any station>↵
 ✓ Protocol forcing     ✓ Rule 1                Addr <any station>↵
   Print            ↵   ✓ Rule 2                Port = <any>         ↵
   Manage names         ✓ Rule 3                Port = <any>         ↵
                        ✓ Rule 4              ✓ Pattern match

                                                Skip ØØØ bytes       ↵
                                                Then <none>          ↵

              Specify a rule which controls the transition
                        from one protocol to another.
 Press SPACE to enable (✓) or disable (x); Alt-space inverts all.

1                                                          1Ø New
 Help                                                      capture
```

Figure 6–2. Protocol forcing rule options.

3. Specify the rule you want the analyzer to use.

   a. In the panel to the right, select the protocol you want to force.

Move the highlight to the **If** option and press Enter. The list of protocols available through the set of protocol interpreter suites installed in this analyzer is displayed. This selection is considered the "force from" protocol (Figure 6–3). Scroll through the list to highlight the protocol you want to force and press Enter.



```
Flags──#──Delta T──DST─────────SRC──────────────────────────────────
M      1              [139.51.23..?[139.51.23..  NCCP Screen data for row 5
                          CHOOSE PROTOCOL                              =9
                          <never>                                      =1
                          3Com NBP                                     =9
                          ATP (Atalk)                                  =1
                          DLC
DE                        ISO Transport
 N                        LLC
 N  ✓ Rule 1              Matchmaker (VINES)
 N  ✓ Rule 2              NetBIOS (IBM)
 N  ✓ Rule 3              NetBIOS (NetWare)
 N  ✓ Rule 4              NSP
                          SPP (VINES)
HE                        TCP
 Ø                        UDP
 Ø                        X.25
 Ø            Specify t   XNS                      ou wish
 Ø
 Ø        Use the arrow                            his function
                          Press ESC to abort

                          Use TAB to select windows
1
 Help
```

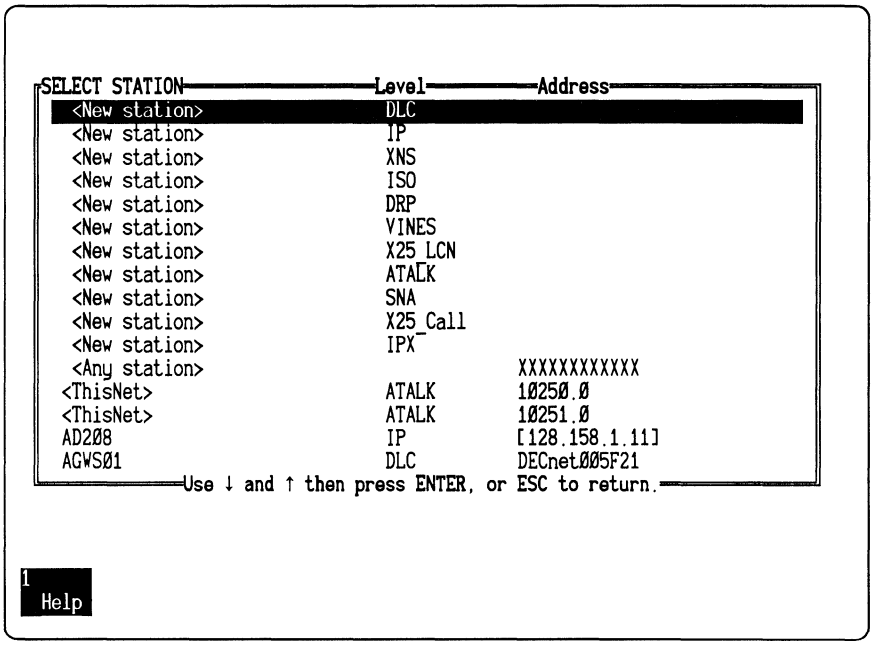
Figure 6–3. Protocol forcing If menu.

b. Press Enter at the **Addr** option(s) to specify a frame address to restrict the use of the rule.

   A name table is displayed (Figure 6–4). The name table is the same for both the source and destination stations. If you have already displayed your data, the name table highlights the source or destination frame from the display. You can restrict the use of the rule to both the source and destination stations.

   Scroll through the name table to highlight the station you want and press Enter. Select the second **Addr** option if you want to select the destination station.

   Note: This field name is based on the **If** protocol selected.

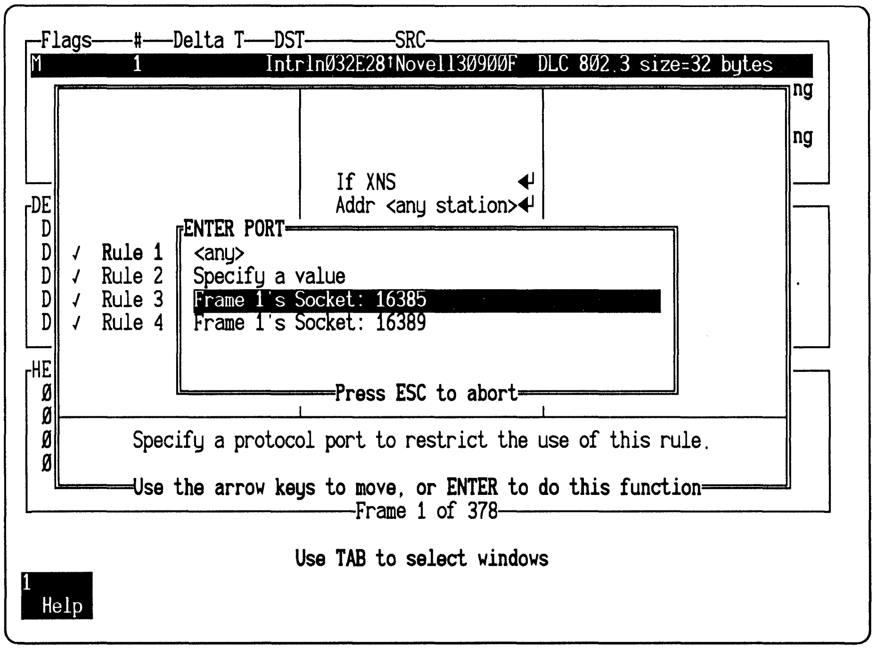


```
SELECT STATION                Level        Address
  <New station>               DLC
  <New station>               IP
  <New station>               XNS
  <New station>               ISO
  <New station>               DRP
  <New station>               VINES
  <New station>               X25_LCN
  <New station>               ATALK
  <New station>               SNA
  <New station>               X25_Call
  <New station>               IPX
  <Any station>                            XXXXXXXXXXXX
 <ThisNet>                    ATALK        10250.0
 <ThisNet>                    ATALK        10251.0
 AD208                        IP           [128.158.1.11]
 AGWS01                       DLC          DECnet005F21
          Use ↓ and ↑ then press ENTER, or ESC to return.

1
 Help
```

Figure 6–4. Select Station address name table.

c. Press Enter at the **Port** option(s) to specify a protocol port to restrict the use of the rule.

   A pop-up window displays the current valid port type (Figure 6–5). This is the connection identifier for the two stations. The Sniffer analyzer provides the current socket number of the frame. You can select **Specify a value** to specify your own value. The protocol port type varies depending on the **If** protocol selected.



```
Flags   #   Delta T   DST          SRC
M       1             Intrln032E28↑Novell30900F  DLC 802.3 size=32 bytes
                                                                    ng

                                                                    ng

                                 If XNS          ↵
DE                               Addr <any station>↵
 D                  ENTER PORT
 D   √  Rule 1     <any>
 D   √  Rule 2     Specify a value
 D   √  Rule 3     Frame 1's Socket: 16385
 D   √  Rule 4     Frame 1's Socket: 16389

HE
 0                           Press ESC to abort
 0
 0       Specify a protocol port to restrict the use of this rule.
 0
         Use the arrow keys to move, or ENTER to do this function
                            Frame 1 of 378

                       Use TAB to select windows
1
 Help
```

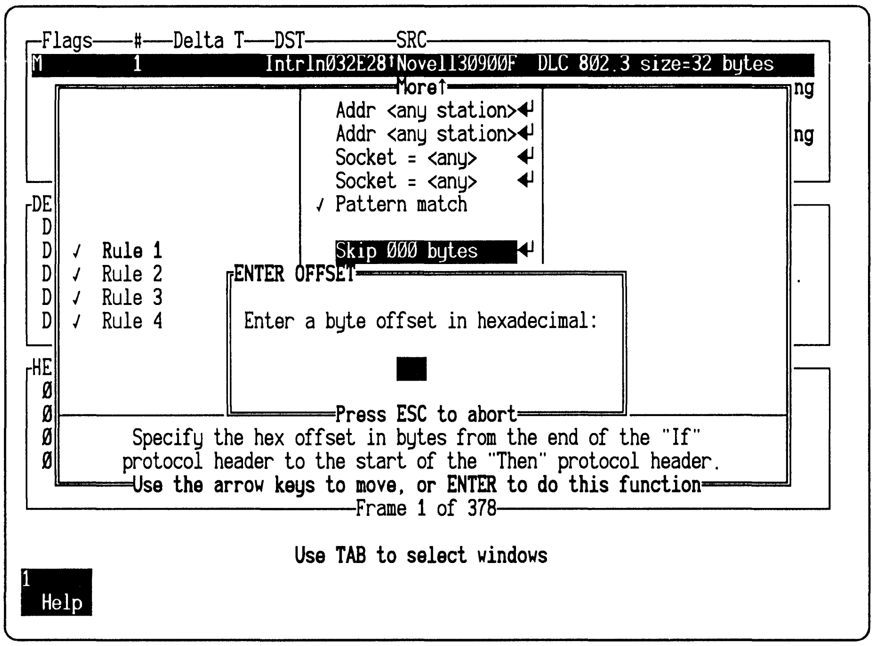
Figure 6–5. Port option window.

d. Specify a pattern that must be present in a frame for the rule to be used.

Refer to the section "Pattern Match Filter" on page 3–39 of this manual for information on using the pattern match options.

e. Specify the hex offset in bytes from the end of the **If** protocol header to the start of the **Then** protocol header.

Figure 6–6 displays the pop-up window where you can specify a hex offset.

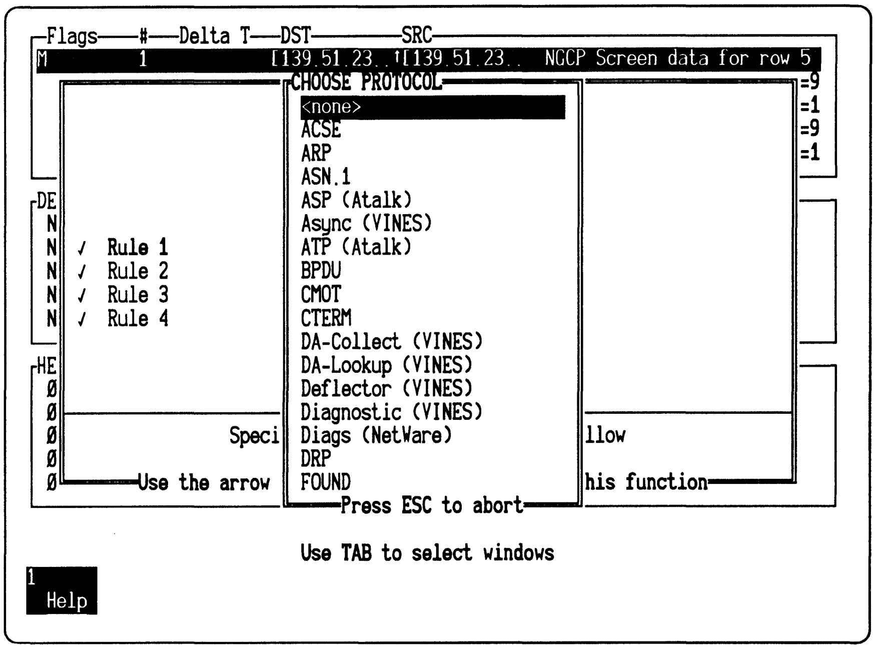


```
Flags──#──Delta T──DST──────SRC──────────────────────────────
M      1          Intrln032E28↑Novell30900F  DLC 802.3 size=32 bytes
                                  More↑                        ng
                                Addr <any station>↵
                                Addr <any station>↵            ng
                                Socket = <any>   ↵
                                Socket = <any>   ↵
DE                            ✓ Pattern match
 D
 D  ✓ Rule 1                    Skip 000 bytes  ↵
 D  ✓ Rule 2          ENTER OFFSET
 D  ✓ Rule 3
 D  ✓ Rule 4           Enter a byte offset in hexadecimal:
HE
 0                                    ■
 0                     ════Press ESC to abort════
 0        Specify the hex offset in bytes from the end of the "If"
 0       protocol header to the start of the "Then" protocol header.
      ══Use the arrow keys to move, or ENTER to do this function══
                              Frame 1 of 378

                        Use TAB to select windows
1
 Help
```

Figure 6–6. Byte offset window.

f. Press Enter at the **Then** option to specify the protocol that should be used as the "force to" protocol.

A list of available protocol options is displayed. This selection is considered the "force to" protocol (Figure 6–7). Scroll through the list to highlight the protocol that should be used as the "force to" protocol and press Enter.



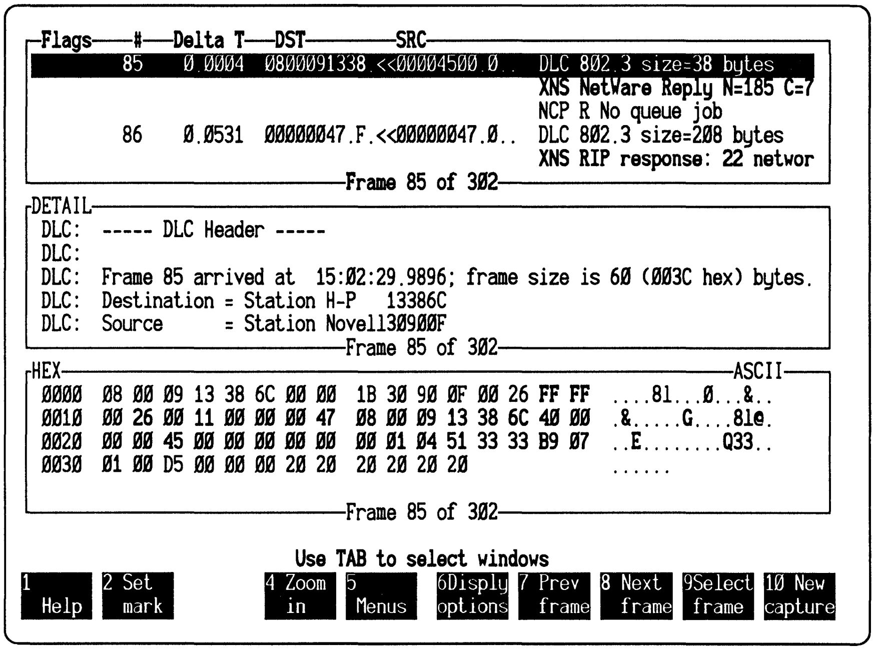
```
Flags——#——Delta T——DST————SRC————————————————————————————
M        1          [139.51.23..↑[139.51.23..  NCCP Screen data for row 5
                             CHOOSE PROTOCOL                          =9
                             <none>                                   =1
                             ACSE                                     =9
                             ARP                                      =1
                             ASN.1
DE                           ASP (Atalk)
N                            Async (VINES)
N   ✓ Rule 1                 ATP (Atalk)
N   ✓ Rule 2                 BPDU
N   ✓ Rule 3                 CMOT
N   ✓ Rule 4                 CTERM
                             DA-Collect (VINES)
HE                           DA-Lookup (VINES)
Ø                            Deflector (VINES)
Ø                            Diagnostic (VINES)
Ø               Speci        Diags (NetWare)              llow
Ø                            DRP
Ø    Use the arrow           FOUND                        his function
                             Press ESC to abort

                             Use TAB to select windows
```

Figure 6–7. Protocol forcing Then menu.

4. Repeat step 3 if you want to specify additional rules (Rule 2 to Rule 4).

Applying a Protocol Forcing Rule

Under normal data display, the Sniffer analyzer displays your captured data in a manner similar to Figure 6–8. The procedure below uses protocol forcing to change the display.



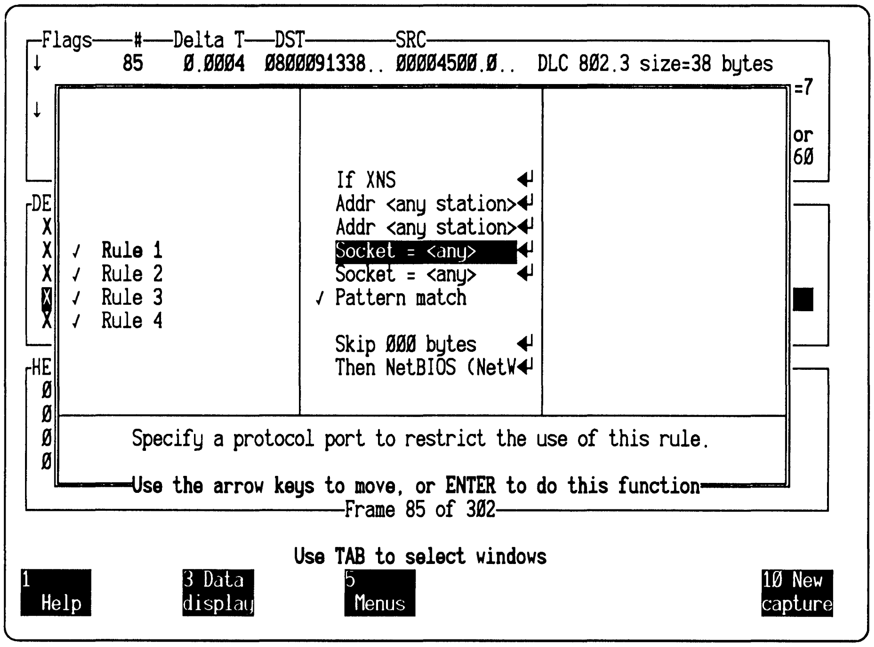
```
Flags——#——Delta T——DST————SRC——————————————————————————————————
        85    Ø.ØØØ4  Ø8ØØØ91338.<<ØØØØ45ØØ.Ø..  DLC 8Ø2.3 size=38 bytes
                                                 XNS NetWare Reply N=185 C=7
                                                 NCP R No queue job
        86    Ø.Ø531  ØØØØØØ47.F.<<ØØØØØØ47.Ø..  DLC 8Ø2.3 size=2Ø8 bytes
                                                 XNS RIP response: 22 networ
——————————————————————————————Frame 85 of 3Ø2——————————————————————
DETAIL————————————————————————————————————————————————————————————
 DLC:  ----- DLC Header -----
 DLC:
 DLC:  Frame 85 arrived at  15:Ø2:29.9896; frame size is 6Ø (ØØ3C hex) bytes.
 DLC:  Destination = Station H-P    13386C
 DLC:  Source      = Station Novell3Ø9ØØF
——————————————————————————————Frame 85 of 3Ø2——————————————————————
HEX——————————————————————————————————————————————————————————ASCII——
 ØØØØ  Ø8 ØØ Ø9 13 38 6C ØØ ØØ  1B 3Ø 9Ø ØF ØØ 26 FF FF  ....81...Ø...&..
 ØØ1Ø  ØØ 26 ØØ 11 ØØ ØØ ØØ 47  Ø8 ØØ Ø9 13 38 6C 4Ø ØØ  .&.....G....8l@.
 ØØ2Ø  ØØ ØØ 45 ØØ ØØ ØØ ØØ ØØ  ØØ Ø1 Ø4 51 33 33 B9 Ø7  ..E........Q33..
 ØØ3Ø  Ø1 ØØ D5 ØØ ØØ ØØ 2Ø 2Ø  2Ø 2Ø 2Ø 2Ø              ......

——————————————————————————————Frame 85 of 3Ø2——————————————————————

                             Use TAB to select windows
```

Figure 6–8. Display without protocol forcing.

To apply a protocol forcing rule:

1. Enable protocol forcing from the **Display** menu. Move the highlight to **Protocol forcing** and press Spacebar to toggle between disabled (x) and enabled (√).

2. Select the rule you want to use. Move the highlight to that rule and press Spacebar to toggle between disabled (x) and enabled (√). Refer to "Specifying a Protocol Forcing Rule" on page 6–3 for information on setting a protocol forcing rule. Figure 6–9 displays the rule used in this procedure.



```
┌Flags──#──Delta T──DST────────SRC──────────────────────────────────┐
 ↓      85   Ø.ØØØ4  Ø8ØØØ91338.. ØØØØ45ØØ.Ø..  DLC 8Ø2.3 size=38 bytes
                                                                    =7
 ↓
                                                                    or
                                                                    6Ø
                       If XNS               ↵
┌DE                    Addr <any station>↵
 X                     Addr <any station>↵
 X  √ Rule 1           Socket = <any>      ↵
 X  √ Rule 2           Socket = <any>      ↵
 X  √ Rule 3         √ Pattern match
 X  √ Rule 4
                       Skip ØØØ bytes      ↵
┌HE                    Then NetBIOS (NetW↵
 Ø
 Ø
 Ø     Specify a protocol port to restrict the use of this rule.
 Ø
   ─────Use the arrow keys to move, or ENTER to do this function─────
└──────────────────────────Frame 85 of 3Ø2──────────────────────────┘

                        Use TAB to select windows
1           3 Data       5                                   1Ø New
  Help      display       Menus                              capture
```

Figure 6–9. Protocol forcing rule.

3. Select **Flags** in the Summary menu.

   Activating Flags allows you to see quickly which frames in the Display/Summary view are affected by protocol forcing. For additional information on the flags options, refer to the section "Flags Display Option" on page 4–27.

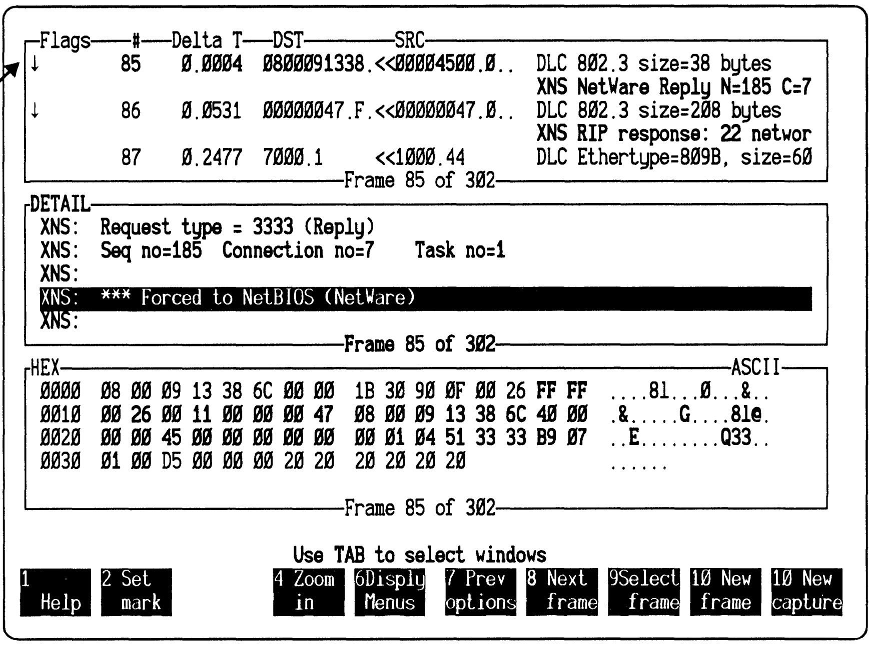
4. Press F3 to display frames in the capture buffer. To make use of **Protocol forcing**, it is generally useful to enable **Summary, Detail,** and **Hex** views.

   The **Summary** view displays a down arrow before each frame with a forced protocol. Also, the color display changes from its normal display to indicate a forced protocol.

   The **Detail** view displays a "Forced to <protocol>" in the protocol field corresponding to the **Then** option of your rule.

   Figure 6–10 shows the data display with protocol forcing applied to it.

Notice the protocol forcing flag



```
┌Flags───#───Delta T───DST──────────SRC─────────────────────────────────────────────
↓        85    Ø.ØØØ4  Ø8ØØØ91338.<<ØØØØ45ØØ.Ø..  DLC 8Ø2.3 size=38 bytes
                                                  XNS NetWare Reply N=185 C=7
↓        86    Ø.Ø531  ØØØØØØ47.F.<<ØØØØØØ47.Ø..  DLC 8Ø2.3 size=2Ø8 bytes
                                                  XNS RIP response: 22 networ
         87    Ø.2477  7ØØØ.1      <<1ØØØ.44      DLC Ethertype=8Ø9B, size=6Ø
└──────────────────────────────Frame 85 of 3Ø2──────────────────────────────────
┌DETAIL────────────────────────────────────────────────────────────────────────
 XNS:  Request type = 3333 (Reply)
 XNS:  Seq no=185  Connection no=7    Task no=1
 XNS:
 XNS:  *** Forced to NetBIOS (NetWare)
 XNS:
└──────────────────────────────Frame 85 of 3Ø2──────────────────────────────────
┌HEX─────────────────────────────────────────────────────────────────ASCII───────
 ØØØØ  Ø8 ØØ Ø9 13 38 6C ØØ ØØ  1B 3Ø 9Ø ØF ØØ 26 FF FF  ....81...Ø...&..
 ØØ1Ø  ØØ 26 ØØ 11 ØØ ØØ ØØ 47  Ø8 ØØ Ø9 13 38 6C 4Ø ØØ  .&.....G....8le.
 ØØ2Ø  ØØ ØØ 45 ØØ ØØ ØØ ØØ ØØ  ØØ Ø1 Ø4 51 33 33 B9 Ø7  ..E.........Q33..
 ØØ3Ø  Ø1 ØØ D5 ØØ ØØ ØØ 2Ø 2Ø  2Ø 2Ø 2Ø 2Ø              ......

└──────────────────────────────Frame 85 of 3Ø2──────────────────────────────────

                          Use TAB to select windows
```

Figure 6–10. Display using protocol forcing.

Disabling Protocol Forcing

Protocol forcing has a temporary effect on the display. If you close the display, or replace the contents of the capture buffer, the analyzer discards any protocol forcing you did earlier. When you save the capture buffer, the saved file does not contain any record of the protocol forcing you may have applied to it.

While a display is active, the **Display options** menu gives you a way to undo the forcing of individual frames.

To undo a forced protocol:

1. From the **Display options** menu, highlight **Protocol forcing**. Move the highlight to the right of the Display options and to Protocol forcing.
2. Disable protocol forcing entirely or disable one or more individual rules. Move the highlight to either **Protocol forcing** or a rule you want to disable and press Spacebar to toggle from √ (enabled) to x (disabled).

   The analyzer returns the display to its previous form.

Special Considerations for Protocol Forcing

There are some special considerations that apply to the protocol forcing process:

- You cannot use protocol forcing to interpret a protocol that occurs prior to the end of a DLC header.
- For most networks,the expert system can use the protocol forcing rules only if SNAP is the protocol *from* which you are forcing (that is, if you have selected SNAP from the **If** list).

On a Sniffer Internetwork Analyzer, the expert system can use the protocol forcing rules if you are forcing *from* any of the following protocols:

DLC
HDLC
PPP
X.25
FrameRelay
SNAP
Embedded Ethernet

- When you capture from a trace file, you should enable the protocol forcing rules before you start the capture. In this way you will assure that the interpetation of the frames will benefit from any available information involving interframe dependencies.

  If you find that you have captured from a trace file without enabling the desired protocol forcing rules, you can correct the situation by pressing **Disply Options** (F6) and selecting **Reinterpret**. You can also use **Reinterpret** after changing your rule selection to avoid having to capture the file again.

CHAPTER SEVEN: GENERATING TRAFFIC 7

Generating Traffic

Overview

On Ethernet, token ring, ARCNET, PC Network, and StarLAN networks, the **Traffic generator** lets you load a portion of the network with background traffic. This allows you to observe how other stations respond to delays introduced by a large volume of unrelated traffic, to test the response of an individual station to heavy traffic of a particular type, or to test gateways and bridges.

Frames generated by the Traffic generator obey the network's normal rules for transmitting. For a CSMA/CD network such as Ethernet, that means using the standard collision-detection and back-off algorithms. For a token-passing network, it means waiting for a free token and following the appropriate low-level transmission protocol.

You can use the Traffic generator in two ways:

- Sending the same frame repeatedly (**Single frame mode**)
- For Ethernet, token ring, and FDDI networks, sending the contents of the capture buffer (**Buffer mode**)

If you send the capture buffer, you can choose whether to send all frames or only those that pass the display filters. You can also send the buffer only once or continuously.

If you send the same frame repeatedly, you can specify the frame's destination, size, interval between frames, the maximum number of frames sent, and the content of the first 32 data bytes. By specifying the data bytes appropriately, you can generate frames that appear to the recipient to have a particular SAP or Ethertype address. You can also generate frames to which no station should respond.

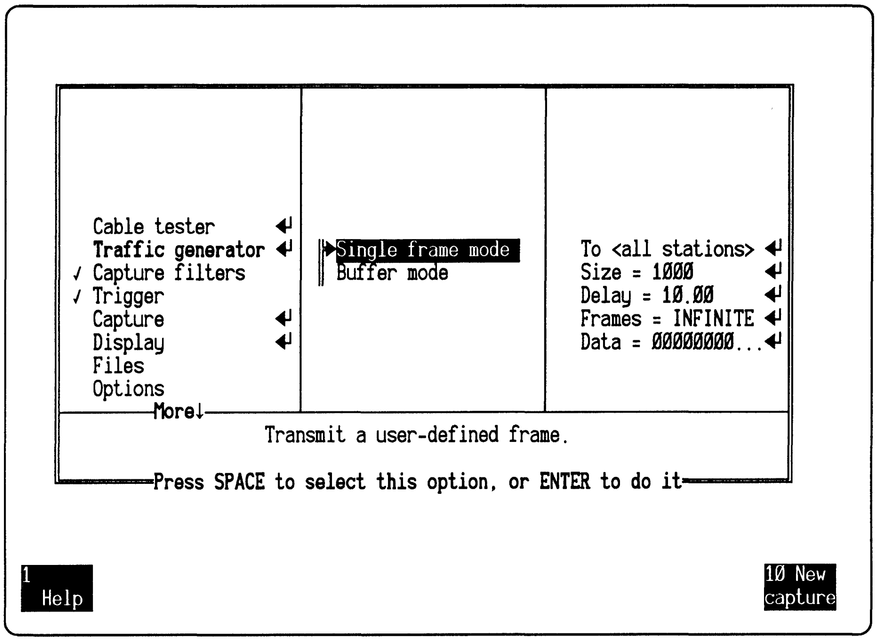
Traffic Generator Menu Overview

Figure 7–1 provides an overview of the basic menu items associated with the Traffic generator menu, including those items associated with the **Single frame mode**. Note that, although the figure shows the menu as it appears for an Ethernet network, the basic Traffic generator menu items are the same for all networks.

As with all Sniffer menu options, you press the Cursor keys to move the highlight to the desired option and then define that option.

- For options marked with the √ and x symbols, you can press Spacebar to enable (√) or disable (x) the option.
- For options connected with a vertical bar, you can choose one of those options by moving to it and pressing Spacebar.

- For options where you must define a specific value, such as the transmission delay, you can either choose that value from a list or enter the desired value into a dialog box.



```
  Cable tester      ↵
  Traffic generator ↵  ▶Single frame mode    To <all stations> ↵
✓ Capture filters       Buffer mode          Size = 1000       ↵
✓ Trigger                                    Delay = 10.00     ↵
  Capture           ↵                        Frames = INFINITE ↵
  Display           ↵                        Data = 00000000...↵
  Files
  Options
  ───────More↓──────
                   Transmit a user-defined frame.

──────Press SPACE to select this option, or ENTER to do it──────
```

Figure 7–1. Overview of the Traffic generator menu options.

Preparing to Generate Traffic: Single Frame Mode

When you choose the **Single frame mode** option, the Sniffer analyzer repeatedly sends the same frame to the destination you specify. You can also specify the frame's contents, including:

- Destination address
- Size of the frame
- Delay, which is the interval between frames
- The maximum number of frames sent
- Data, which consists of the 32 data bytes

Specifying Destination

The destination must be a DLC-level address. The default is **To <all stations>**, which is a broadcast address, but you can also choose the address of a specific station. Depending on the network, there may also be various classes of group addresses.

To specify the destination of the generated frames:

1. Move to **Traffic generator\Single frame mode\To ...** and press Enter.

In response, the Sniffer analyzer displays the list of DLC addresses currently in the working name table.

2. Move to the desired destination address and press Enter. Note that the **To** field now shows the name of that address (such as To "James") or the numeric address if the station is not named (such as "To "IBM 002FEB").
3. To add a new address to the working name table, move to **<New station>** and press Enter.
4. In the dialog box that appears, enter the new DLC address and a corresponding name. To select the new address as the destination, repeat step 2.

Specifying Frame Size

The **Size** option determines the total length of the frame to be generated. The minimum and maximum permissible size values depend upon the network, as shown in Figure 7–2.

	Ethernet	Token Ring		FDDI
		4 Mbits/s	16 Mbits/s	
Minimum bytes	12	18	18	18
Maximum bytes	1514	4458	17954	4500

Figure 7–2. Size ranges of generated frames.

On Ethernet, the length of the smallest valid frame is 60 bytes. Shorter frames normally occur only as collision fragments. However, the Sniffer analyzer can generate short frames. When you specify a length shorter than 60 bytes, the analyzer displays a warning that other stations may see these as collision fragments and therefore report them as network errors.

Note that the length is written in decimal, which is how the Sniffer reports the lengths of captured frames: that is, the total length ignoring the physical header and trailer.

To specify the size of the frames to be generated:

1. Move to **Traffic Generator\Single frame mode\Size=** and press Enter.
2. In the dialog box that appears, enter the desired length and press Enter.

Specifying the Delay Between Generated Frames

The **Delay** option determines the interval between the time after the Sniffer finishes sending one frame until it starts to send another. The interval is the *minimum* interval between the transmitted frames. The *actual* interval may be longer, since the Sniffer analyzer may have to wait its turn if other stations are also transmitting.

To specify the delay between generated frames:

1. Move to **Traffic Generator\Single frame mode\Delay** and press Enter.
2. In the dialog box that appears, type the desired length of the delay (in milliseconds) and press Enter.

The minimum and maximum interval values are shown in Figure 7–3.

Note: On the Model 55, the minimum delay is 0.02.

	Ethernet	Ethernet-II	Token Ring
Minimum delay, milliseconds	0.04	0.025	1.0
Maximum delay, milliseconds	1000	1000	1000

Figure 7–3. Interval ranges between consecutive generated frames.

Specifying the Number of Frames to Generate

The **Frames** option determines the number of frames to be sent, from 1 to 999999999. The default is "Infinite," which means the Sniffer transmits frames until you press Esc.

To specify the number of frames to be generated:

1. Move to **Traffic Generator\Single frame mode\Frames** and press Enter.
2. In the dialog box that appears, type the number of frames you want to transmit and press Enter. To return to the default "Infinite," type 0.

Defining the Frame's Data Field

The generated frame's destination and source fields use the first twelve bytes, as shown in Figure 7–4. The rest of the frame is considered "data," of which you can specify the first 32 bytes. The last four bytes in the data field shows the frame sequence number.

When defining the contents of the data field, you must consider whether the frame will contain routing information. For more information, refer to "Specifying the RI Bit in Generated Frames" on page 7–7.

Structure of a Generated Frame

Figure 7–4 shows the fields in a generated frame.

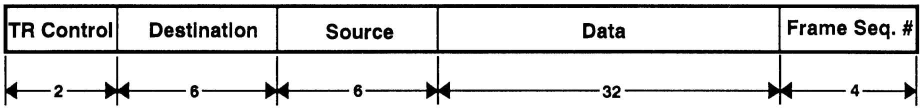


Figure 7–4. Structure of a generated frame.

Control (Token ring only) Two bytes that specify media access and frame control.

Destination Six bytes that specify the destination, chosen with the **To <all stations>** option.

Source Six bytes generated by the Sniffer to identify itself.

Data Up to 32 bytes available for data. If you do not specify all 32 bytes, the remaining bytes are padded with 00 hex.

Frame Seq. # The last four bytes, generated automatically by the Sniffer (one for the first transmitted frame of a series, increased by one for each additional frame to correspond with the decimal frame number).

To specify the contents of the data field:

1. Move to **Traffic Generator/Single frame mode/Data** = and press Enter.

   In response, the Sniffer displays a dialog box that contains 64 zeros (32 repetitions of 00 hex).

2. Type the data you want, in hex, and press Enter. Any positions you don't specify remain as 0.

   If the total length of the data field is less than 32 bytes, the Sniffer analyzer takes the number needed and ignores the rest. If the total length of the data field is greater than 32 bytes, the analyzer fills the additional space with 00 hex.

   The Sniffer analyzer also inserts the sequence number for the generated frame into the last four bytes of the data field. Thus, when the total length of the data field is less then 32 bytes, the sequence number overwrites those positions of the data field.

If the generated frames are sent to a real station and you expect that station to read them, you must supply reasonable values in the first part of the data field. For example, an Ethernet recipient will expect to see an Ethertype, an 802.3 recipient will expect to see length information and an 802.2 header, and so on.

Specifying the RI Bit in Generated Frames

A frame that originates on a token ring network may also include an RI field. The RI fields, which contain a record of each intermediate station that forwarded the frame, are located after the usual DLC source and destination fields. (For a more detailed description of the routing field, see "About the Interpret RI Option" on page 2–6.)

Modifying the Source Address for RI Fields

To indicate that these optional fields are present, the source address must be modified by forcing a 1 in the bit that (in a destination address) indicates a "broadcast." You cannot control the source address of a generated frame because that frame automatically uses the source address of the analyzer that sent it. However, you can force the analyzer to insert the "RI present" bit.

If you choose to generate frames with the RI bit enabled, it is your responsibility to include a consistent RI header at the beginning of the data field.

To turn on the RI bit in the source address of a generated frame:

1. Move to **Traffic Generator\Single frame mode\Data\RI present** and press Spacebar to enable the option.

Specifying the Length of the RI Field

When the data you specify includes an RI field, you must specify the number of bytes the RI field occupies. The RI field starts with a 2-byte header, followed by a range from zero to eight 2-byte segment addresses.[1] Thus, the total length of the RI field may range from 2 to 18 bytes. The length (mod 32) is encoded in the low-order five bits of the first byte.

Effect of Routing Information on the Data Field's Layout

When a frame contains an RI field, that field starts in the third byte after the source address. If there is no routing information, the 802.2 header or the Ethernet data starts with the third byte.

You cannot specify what goes into the first 32 bytes until you decide whether the generated frame contains routing information. Moreover, if the frame does contain routing information, the RI field can be of variable length. Unless you declare its length correctly, the recipient cannot locate the fields that follow.

Figure 7–5 summarizes the factors that affect the data field for Ethernet and token ring networks.

[1] These are not DLC addresses, but segment identifiers adopted by mutual agreement.

<table>
<tr><th colspan="2">Ethernet</th><th>Token Ring</th></tr>
<tr><td colspan="2">The hex characters you enter specify the first 32 data bytes; that is, those that follow the 6-byte destination and 6-byte source address.</td><td>The hex characters you enter specify the first 32 data bytes; that is, those that follow the 1-byte access control, the 1-byte frame control, the 6-byte destination and the 6-byte source address.</td></tr>
<tr><td colspan="2">If the RI field is enabled, the variable length source routing information follows the first two bytes of user-definable data.</td><td>If the RI field is enabled, the first byte of the 32 bytes contains the source routing information.</td></tr>
<tr><td colspan="2">The interpretation of the first two data bytes depends on whether you generate Ethertype or IEEE 802.3 frames.</td><td>The first data byte (following the RI field, if enabled) identifies the destination SAP, the second identifies the source SAP. The next one or two bytes are control bytes that indicate the type of transmission.</td></tr>
<tr><td><b>Ethertype</b>
The first two bytes are the Ethertype. For example, 0800 identifies the IP Ethertype, while 0600 identifies XNS.</td><td><b>802.3</b>
The first two bytes are the 802.2 length, followed by the variable-length RI field, followed by the 802.2 header.</td><td></td></tr>
</table>

Figure 7–5. Location of the user-definable data in a generated frame.

The placement of the RI field within an Ethertype frame and within an IEEE 802.3 frame is summarized in Figure 7–6.

<table>
<tr><th></th><th>Based on <To xxxxxx></th><th>Automatic</th><th colspan="4">Controlled by what you specify for the first 32 bytes</th></tr>
<tr><td>Ethertype</td><td>Destination 6 bytes</td><td>Source 6 bytes</td><td>Etype 2 bytes</td><td>RI 0-32 bytes</td><td colspan="2">Rest of data</td></tr>
<tr><td>802.3</td><td>Destination 6 bytes</td><td>Source 6 bytes</td><td>Length 2 bytes</td><td>RI 0-32 bytes</td><td>802.2 header 3-4 bytes</td><td>Rest of data</td></tr>
</table>

Figure 7–6. Position of RI field in Ethertype and IEEE 802.3 frames.

Sequence Numbers

The last four bytes of each frame transmitted by the **Traffic generator** contain a sequence number. Each time you start the **Traffic generator**, the sequence numbers start at 1. If the last four bytes overlap the first 32 data bytes, the sequence number overwrites some of the data you specified for the first 32 bytes.

Preparing to Generate Traffic: Buffer Mode

Buffer mode is available for Ethernet, token ring, and FDDI networks. When you choose the **Buffer mode** option, the Sniffer analyzer sends the contents of the capture buffer instead of specified frames. Depending on the network, some frames are not transmitted. On token ring networks, for example, the analyzer transmits no MAC frames. On FDDI networks, the analyzer transmits all frames in the buffer except MAC frames and Void frames.

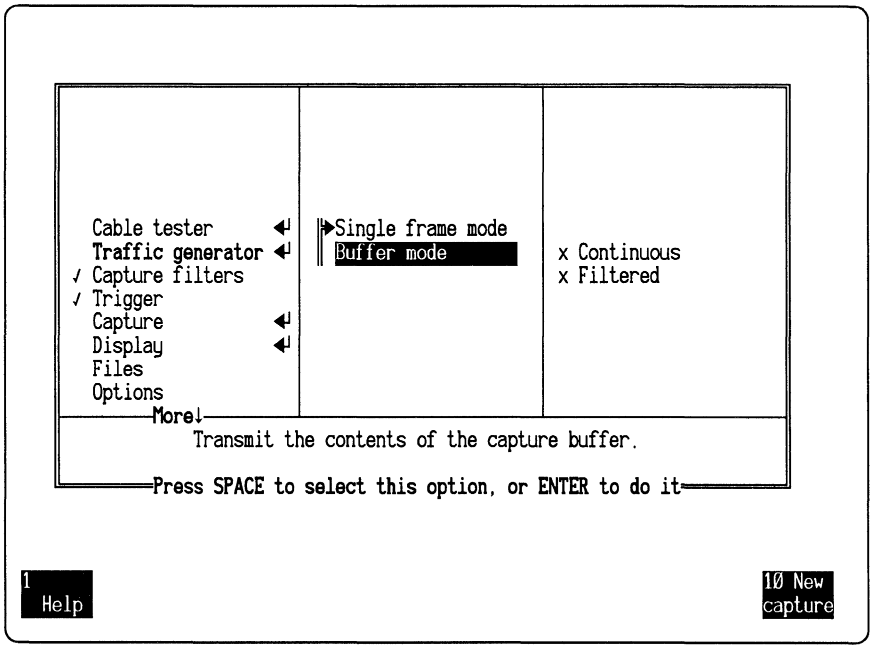
Note: FDDI analyzers and analyzers with Ethernet-II adapter cards can also transmit frames with CRC errors.

You can use the **Buffer mode** option in conjunction with the **Frame editing** option—which allows you to edit the contents of the frames in the capture buffer—to build and send a complex capture buffer. For more information about this option, see "Using Hexadecimal View to Edit Frames" on page 4–38.

In this mode, you can define:

- Whether to send the buffer contents once or continuously
- Whether to send all frames or only those that pass the Display filters.

Figure 7–7 shows the options associated with the **Buffer mode** option when using the **Traffic generator**.



Transmit the contents of the capture buffer.

Press SPACE to select this option, or ENTER to do it

Figure 7–7. Using the Traffic generator to transmit the capture buffer.

To generate traffic in buffer mode:

1. Move to **Traffic generator\Buffer mode** and press Spacebar to enable (√) the option.
2. Move to **Continuous** and press Spacebar to enable (√) or disable (x) the option.

   If this option is disabled, the buffer contents are transmitted just once, starting with the first frame through the last frame in the buffer. If the option is enabled, the buffer contents are transmitted repeatedly until you press Esc.
3. Move to **Filtered** and press Spacebar to enable (√) or disable (x) the option.

   If this option is disabled, all frames in the capture buffer are transmitted. If this option is enabled, only those frames that pass the display filters are transmitted. Whether the frames are transmitted continuously or just once depends on the **Continuous** option.
4. FDDI only: Move to **Override SRC Addr** and press Spacebar to enable (√) or disable (x) the option.

   If this option is enabled, the source addresses of all frames in the buffer are replaced with the address of this analyzer. If it is disabled, the analyzer transmits the frames exactly as they are in the buffer.

   Enabling this option assures that the traffic you generate will be stripped off the ring, rather than going around the ring more than once.

   However, overriding the source address does not change the source address in the upper layer fields. Therefore, using the traffic generator to send SMT frames, which also contain a source address, can cause strange behavior on the ring, such as reconfiguring ring maps.

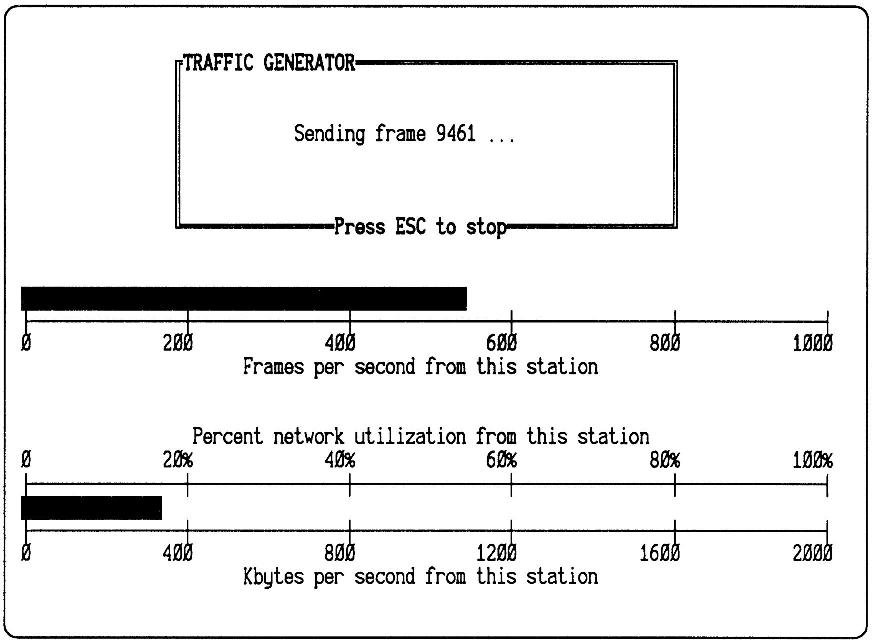
Starting and Stopping Traffic Generation

After you choose the desired **Traffic generator** mode and define the options associated with that mode, you can start to generate traffic.

To start the Traffic generator:

1. Move to **Traffic generator** and press Enter.

   The Sniffer starts to transmit frames, as shown in Figure 7–8. This screen updates a counter that shows the current frame number, as well as three thermometer-style bar graphs that show the number of frames transmitted, the number of Kbytes transmitted, and the percentage of network utilization.



```
TRAFFIC GENERATOR

        Sending frame 9461 ...

        Press ESC to stop
```

Ø 2ØØ 4ØØ 6ØØ 8ØØ 1ØØØ
Frames per second from this station
Percent network utilization from this station
Ø 2Ø% 4Ø% 6Ø% 8Ø% 1ØØ%
Ø 4ØØ 8ØØ 12ØØ 16ØØ 2ØØØ
Kbytes per second from this station

Figure 7–8. Generating frames on a token ring network.

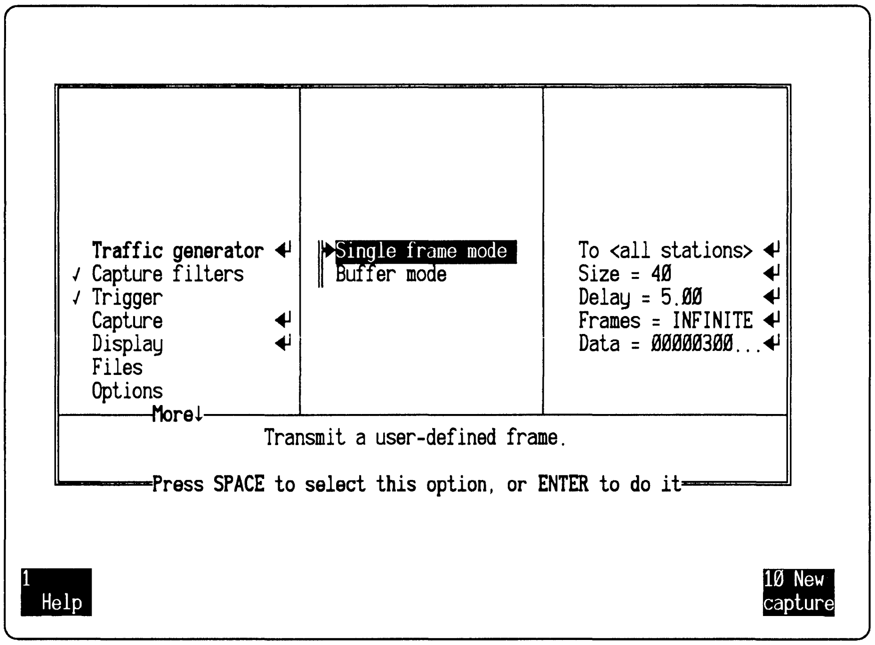
Note: While the Sniffer analyzer generates traffic, it does not perform any other Sniffer functions. However, on a token ring network, the Sniffer analyzer can be the "active monitor" for the ring as it continues to forward incoming frames from its upstream neighbor.

To stop the Traffic generator:

1. Press Esc.

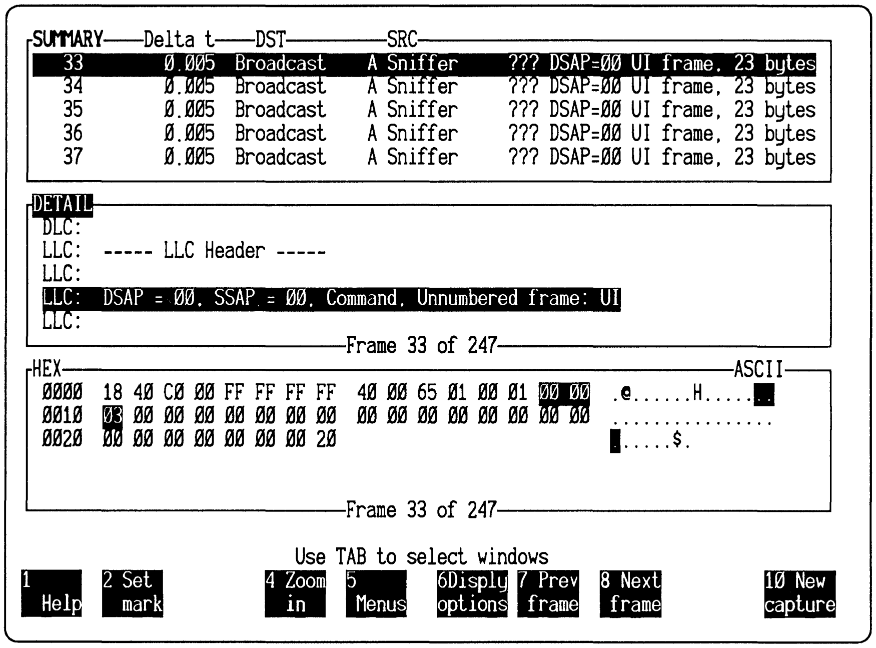
Example: Format of the Generated Frame

The generated frame's format depends on the network. Figure 7–9 shows how a frame to be generated in **Single Frame mode** was defined. Figure 7–10 shows how that frame appears when captured by another Sniffer analyzer. (On a different network, the frame would differ slightly.)



```
  Traffic generator ↵   ▶Single frame mode     To <all stations> ↵
✓ Capture filters        Buffer mode           Size = 4Ø         ↵
✓ Trigger                                      Delay = 5.ØØ      ↵
  Capture           ↵                          Frames = INFINITE ↵
  Display           ↵                          Data = ØØØØØ3ØØ...↵
  Files
  Options
        More↓
                 Transmit a user-defined frame.
        Press SPACE to select this option, or ENTER to do it

1                                                            1Ø New
 Help                                                        capture
```

Figure 7–9. Defining a token ring frame to be generated.



```
SUMMARY——Delta t——DST—————SRC——————————————————————————————
  33        Ø.ØØ5  Broadcast  A Sniffer  ??? DSAP=ØØ UI frame, 23 bytes
  34        Ø.ØØ5  Broadcast  A Sniffer  ??? DSAP=ØØ UI frame, 23 bytes
  35        Ø.ØØ5  Broadcast  A Sniffer  ??? DSAP=ØØ UI frame, 23 bytes
  36        Ø.ØØ5  Broadcast  A Sniffer  ??? DSAP=ØØ UI frame, 23 bytes
  37        Ø.ØØ5  Broadcast  A Sniffer  ??? DSAP=ØØ UI frame, 23 bytes

DETAIL
DLC:
LLC:  ----- LLC Header -----
LLC:
LLC:  DSAP = ØØ, SSAP = ØØ, Command, Unnumbered frame: UI
LLC:
                         Frame 33 of 247
HEX————————————————————————————————————————————————————ASCII——
ØØØØ  18 4Ø CØ ØØ FF FF FF FF  4Ø ØØ 65 Ø1 ØØ Ø1 ØØ ØØ  .e......H......
ØØ1Ø  Ø3 ØØ ØØ ØØ ØØ ØØ ØØ ØØ  ØØ ØØ ØØ ØØ ØØ ØØ ØØ ØØ  ................
ØØ2Ø  ØØ ØØ ØØ ØØ ØØ ØØ ØØ 2Ø                          ......$.

                         Frame 33 of 247

                     Use TAB to select windows
1     2 Set        4 Zoom 5     6Disply 7 Prev 8 Next        1Ø New
 Help  mark         in    Menus options frame  frame         capture
```

Figure 7–10. Appearance of the generated token ring frame.

As shown above, each generated frame consists of the following information:

- The first two bytes are the AC and FC bytes of the standard DLC header, visible in the Hex view as the characters 18 40.
- The next six bytes are the destination address (in this case, C0 00 FF FF FF FF, which means "Broadcast").

- The next six bytes are the source address (in this example, 40 00 65 01 00 01, which is the address of the Sniffer analyzer that generated the frame).
- The next 32 bytes contain the data specified for the data field, starting with 00 00 03 00 ... 00. (On token ring, this default remains in effect unless you enter other values for the data field.) Following the standard header and whatever bytes you specify for the data field, the remainder of the frame consists of as many repetitions of 00 (hex) as necessary to create the total size you requested.
- The last four bytes show the sequence number 00 20.

In the Detail view, which shows the interpreted frame, the DSAP and SSAP fields are both 00. Since those values do not match any protocol known to the Sniffer analyzer, it shows the protocol as "???". The analyzer interprets the first 4 bytes as UI and attaches the explanatory text "Unnumbered information."

In the Hex view, the first three of those four bytes are highlighted. (The fourth is not highlighted because the preceding bytes are sufficient to identify the UI command, and the protocol interpreter knows that UI makes no use of the fourth byte.) Note that the frame sequence number is 24 FS, which corresponds to the decimal frame sequence number that appears in Figure 7–8 as 9461.

CHAPTER EIGHT: THE SNIFFER—LM2000 CONVERSION UTILITY 8

The Sniffer–LM2000 Conversion Utility

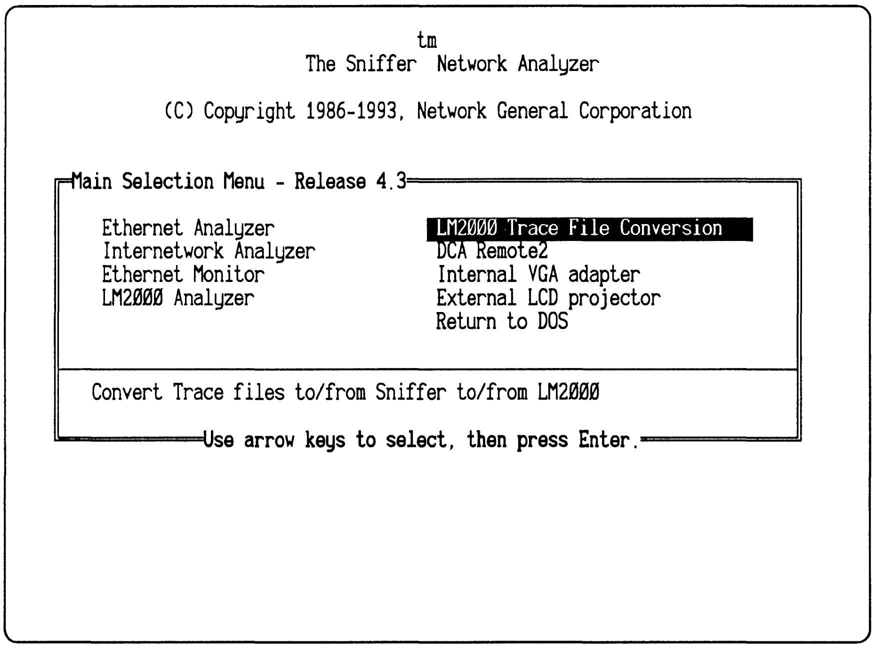
Overview

The Sniffer Internetwork Analyzer includes a conversion utility that allows you to convert trace files between Sniffer Internetwork Analyzer format and LM2000 Analyzer format. In this way, you can capture a trace file with one application and still use the analysis features offered by the other application.

This section does not provide information on how to capture a trace file. For information on how to capture and save a trace file using the Sniffer Network Analyzer, see "Saving Captured Frames as Data (Trace) Files" on page 5–11. For information on how to capture and save a trace file using the LM2000 Analyzer, see the *LM2000 Protocol Analyzer User's Manual.*

Using the Conversion Utility

The Sniffer—LM2000 Conversion Utility is accessed from the Main Selection Menu of the Sniffer Network Analyzer. Figure 8–1 shows a sample Main Selection Menu with the Sniffer—LM2000 Conversion Utility highlighted.



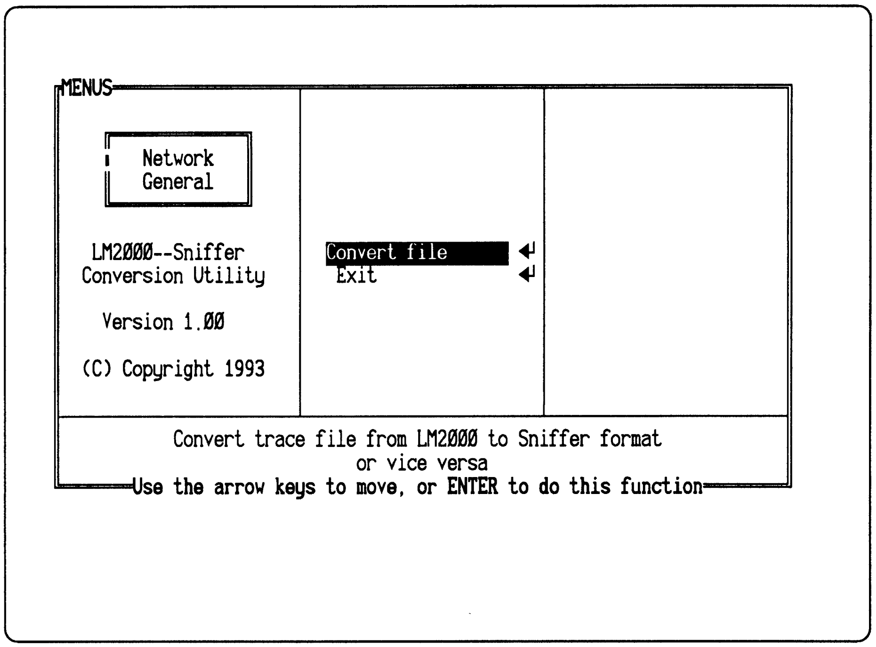
```
                          tm
             The Sniffer   Network Analyzer

      (C) Copyright 1986-1993, Network General Corporation

 Main Selection Menu - Release 4.3

   Ethernet Analyzer              LM2000 Trace File Conversion
   Internetwork Analyzer          DCA Remote2
   Ethernet Monitor               Internal VGA adapter
   LM2000 Analyzer                External LCD projector
                                  Return to DOS

  Convert Trace files to/from Sniffer to/from LM2000

           Use arrow keys to select, then press Enter.
```

Figure 8–1. Main Menu of the Sniffer Network Analyzer.

To convert a trace file between Sniffer Internetwork Analyzer and LM2000 formats:

1. From the Main Selection Menu of the Sniffer Network Analyzer, use the cursor keys to highlight the **LM2000 Trace File Conversion** entry, as in Figure 8–1. Press Enter.

Result: The main menu of the LM2000—Sniffer Conversion Utility appears, as in Figure 8–2.



Convert trace file from LM2000 to Sniffer format or vice versa

Use the arrow keys to move, or ENTER to do this function

Figure 8–2. Main menu of the LM2000—Sniffer Conversion Utility.

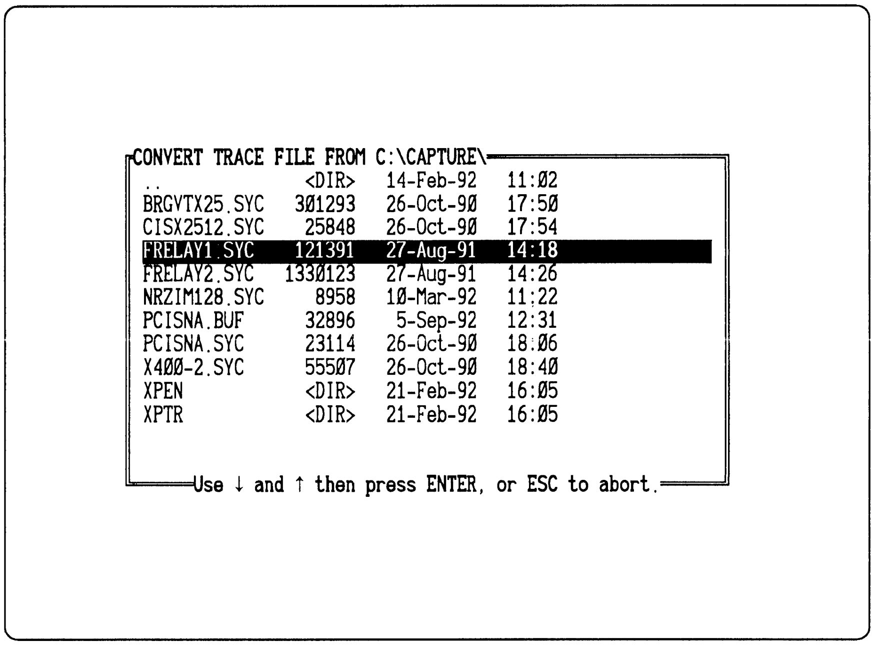
2. By default, the cursor appears on the **Convert file** menu entry. Press Enter.

   Result: A window (shown in Figure 8–3) appears listing the files available for conversion in the current directory. You can use the cursor and Enter keys to move among the various directories.

Note: The utility lists only those files eligible for conversion by the LM2000—Sniffer Conversion Utility. The only files eligible for conversion are those captured by the Sniffer Internetwork Analyzer or those captured by the LM2000 Analyzer.

- Files captured by the Sniffer Internetwork Analyzer have the three-letter extension .SYC. For example, a sample trace file could be titled *SAMPLE*.SYC.
- Files captured by the LM2000 Analyzer have the three-letter extension .BUF. For example, a sample trace file could be titled *SAMPLE*.BUF.

Figure 8–3 shows the window listing files available for conversion. Notice that all files listed have either a .BUF or .SYC extension.



```
CONVERT TRACE FILE FROM C:\CAPTURE\
 ..               <DIR>   14-Feb-92   11:Ø2
 BRGVTX25.SYC    3Ø1293   26-Oct-9Ø   17:5Ø
 CISX2512.SYC     25848   26-Oct-9Ø   17:54
 FRELAY1.SYC     121391   27-Aug-91   14:18
 FRELAY2.SYC    133Ø123   27-Aug-91   14:26
 NRZIM128.SYC      8958   1Ø-Mar-92   11:22
 PCISNA.BUF       32896    5-Sep-92   12:31
 PCISNA.SYC       23114   26-Oct-9Ø   18:Ø6
 X4ØØ-2.SYC       555Ø7   26-Oct-9Ø   18:4Ø
 XPEN             <DIR>   21-Feb-92   16:Ø5
 XPTR             <DIR>   21-Feb-92   16:Ø5

      Use ↓ and ↑ then press ENTER, or ESC to abort.
```

Figure 8–3. Window for specifying trace file to be converted.

3. Use the cursor and Enter keys to highlight the trace file you want to convert. Trace files for the Sniffer analyzer are, by default, stored in the C:\CAPTURE directory. Trace files for the LM2000 Analyzer are, by default, stored in the C:\LM2000 directory. When you have highlighted the trace file you want to convert, press Enter.

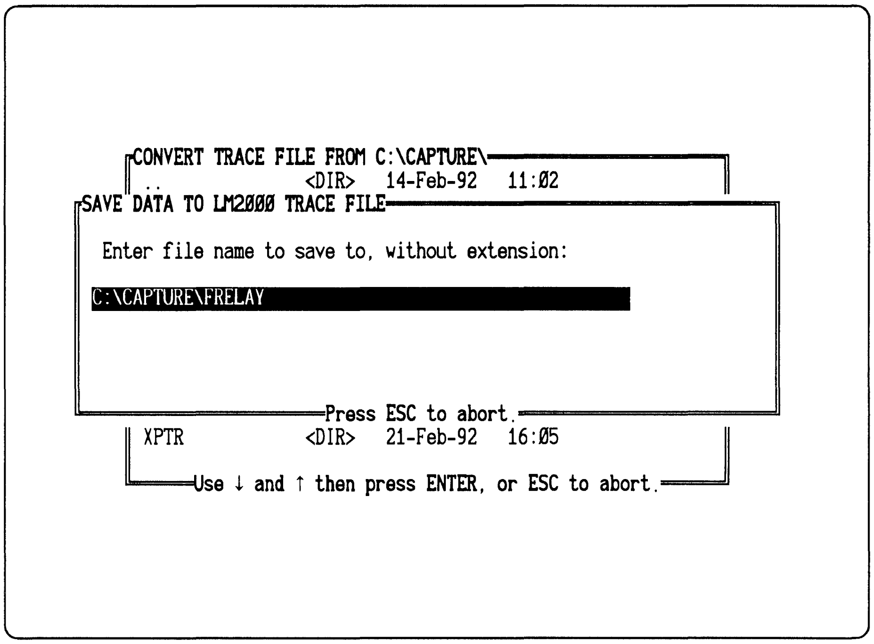
   Note: Source trace files for conversion may be located in any directory on the C:\ drive. You cannot, however, convert from trace files located on a floppy diskette. To convert a trace file from a floppy diskette, you must first use the COPY command to copy the desired trace file to the Sniffer analyzer's hard disk. For example, to copy the file A:\TRACE.SYC to the C:\CAPTURE directory, you might type the following command to the C:\CAPTURE> prompt:

   ```
   C:\CAPTURE> COPY A:\TRACE.SYC
   ```

4. The conversion utility prompts you to supply the name and DOS path for the converted file it will create. Do not supply an extension — the utility automatically appends the extension appropriate to the type of trace file it is creating. For example, if an LM2000 trace file is to be created, the extension .BUF is automatically appended to the filename you specify. If a Sniffer Internetwork Analyzer trace file is to be created, the extension .SYC is automatically appended to the filename you specify. Figure 8–4 shows the dialog box in which you name the file to be created.

   Note: If the file you name already exists, the conversion utility will display a warning. You can either overwrite the existing file or press ESC if you want to rename the target file.

Note: Although you cannot convert a trace file from a drive other than the hard drive (C:\), you can specify a target drive other than C:\. For example, you could elect to write the converted file directly to a floppy diskette. Simply backspace over the provided path and type in the desired path.



```
 CONVERT TRACE FILE FROM C:\CAPTURE\
  ..             <DIR>   14-Feb-92   11:Ø2
SAVE DATA TO LM2ØØØ TRACE FILE
 Enter file name to save to, without extension:

C:\CAPTURE\FRELAY

                 Press ESC to abort.
  XPTR           <DIR>   21-Feb-92   16:Ø5

       Use ↓ and ↑ then press ENTER, or ESC to abort.
```

Figure 8–4. Dialog box for naming converted trace file.

5. Once you have named the file to be created, press Enter. A window will appear indicating the progress of the file conversion. When conversion is complete, the window listing trace files eligible for conversion reappears. From here, you can convert another trace file, or press ESC to return to the main menu of the conversion utility.

A Word About the Dates of Converted Trace Files

When you convert a trace file from LM2000 format to Sniffer analyzer format, the DOS creation date of the new file will be whatever the current date is (that is, the date to which the computer is currently set[1]). However, when you convert a Sniffer analyzer trace file to LM2000 format, the DOS creation date of the new file will be the timestamp (date of capture) stored inside the Sniffer analyzer trace file. Accordingly, if on September 2, 1993, you converted a Sniffer analyzer trace file with a timestamp of 10-May-91, the created LM2000 file would show a creation date of 10-May-91 rather than 2-Sep-93.

[1] You can use the DOS command, DATE, to change the date the computer regards as current.

CHAPTER NINE: USING THE SNIFFER ANALYZER FILES 9

Using the Sniffer Analyzer Files

Overview

During everyday use of the Sniffer analyzer, you should have little need for the information in this chapter. However, knowledge of the system files may prove useful for a general understanding, as well as for importing and exporting files.

This chapter describes:

- The use of file names and extensions
- The Sniffer analyzer directories and associated files
- Procedures for working with these files
- The file formats used to store name tables, setups, and saved data
- The Sniffer analyzer parameters

About File Names and Extensions

With DOS, a file's name consists of two parts, separated by a dot. The first part (base name) may contain up to eight characters. The second part (extension) consists of three letters. Certain extensions have special significance to DOS. For example, all executable files have the extension .EXE, .COM, or .BAT—DOS won't execute a file with another extension. Other extensions identify a file's use or the type of data in the file. Figure 9–1 summarizes these extensions.

Extenslon	Flle type
.EXE	Executable file. This extension may be omitted from the command that invokes its execution.
.BAT	Batch file, which is an executable file that consists of commands in the DOS shell language. The extension may be omitted from the command that invokes its execution.
.PRN	Output file generated for printing, directed either to a printer or to a file.
.CSV	Output file generated as "comma separated values," used to import or export data.
.TXT	Script that generates the menus, used by the executable MENUX.EXE.
.MNU	Script used to generate a particular analyzer entry in the menu.
.CFG	Configuration file that specifies the protocol interpreters for a particular network.
.HLP	File that contains on-line help information for the Sniffer analyzer.

Figure 9–1. General DOS extensions.

Each of the executable files is specific to a single network, as indicated by an extension that identifies the network (first two letters) and the type of file (last letter), as shown in Figure 9–2. For example, if you save frames captured on an Ethernet network to a file called MYDATA, the Sniffer analyzer assigns the extension .ENC, resulting in the file MYDATA.ENC.

First two letters	**Type of network**
EN	Ethernet and Ethernet-II
TR	Token Ring
FD	FDDI
SY	WAN/Synchronous
AR	ARCNET
LT	LocalTalk
SL	StarLAN
PC	PC Network
Last letter	**Type of file**
C	Captured frames
S	Setup values used to define various system options
D	Station names, the symbolic equivalents for numeric addresses
I	Manufacturer IDs, the symbolic equivalents for the manufacturer codes within numeric addresses
B	Binary type, used only by the Sniffer Monitor application

Figure 9–2. Sniffer analyzer extensions.

The Sniffer Analyzer Directories and Files

Figure 9–3 summarizes the Sniffer analyzer directories for the analyzer on the hard disk (drive C).

Directory	Files
DOS operating system	Required DOS files
TOOLS	Miscellaneous utility programs
CONFIG	The files that list the facilities available to the Sniffer
xxSNIFF	Monitor executable files Analyzer executable files Startup files Configuration files Help files
CAPTURE	Files of captured frames (trace files Setup files, including STARTUP.*xx*S Output files .PRN and .CSV
REMOTE2	Required DCA Remote2 files, used for remote operation

Figure 9–3. The Sniffer analyzer directories.

Root Directory

The root directory contains the files AUTOEXEC.BAT and CONFIG.SYS. The system refers to them automatically each time you reboot or restart following a power-down.

The AUTOEXEC.BAT file establishes the path: that is, the list of directories in which the operating system searches for executable files. This file also invokes the main selection menu. From there, you select which of the programs you want to use (Monitor, Analyzer, or DCA Remote2).

DOS Directory

The DOS directory contains the files that belong to the operating system (except for the few DOS files that are in the root directory). The path includes the DOS directory, which the operating system uses to find its own files. Normally, you won't need to change any files in the DOS directory.

TOOLS Directory

The TOOLS directory contains various utilities. The DOS path directs the operating system to the \TOOLS directory, so you won't usually need to make any explicit reference to it.

CONFIG Directory

The CONFIG directory contains the files that generate the selection menu and the Sniffer analyzer's main menu.

*xx*SNIFF Directory

This directory contains the principal executable files, both for the Sniffer monitor and for the various Sniffer analyzer configurations. The directory's name is formed from the two-letter network abbreviation, followed by the letters SNIFF, such as TRSNIFF for token ring. The Sniffer analyzer contains whichever of these directories is appropriate to your network, but none of the others.

Files and Subdirectories within the xxSNIFF Directory

Each executable file is accompanied by a menu file with the same base name, but with the extension .MNU rather than .EXE. The executable files reside in the xxSNIFF directory (that is, ENSNIFF, FDSNIFF, or TRSNIFF). However, all .MNU files reside in the \CONFIG directory.

The Sniffer analyzer uses the various menu files to generate entries in the main selection menu. Each menu file is responsible for the menu entry corresponding to one Sniffer analyzer or monitor. The .EXE files and the .MNU files are already supplied by Network General. In addition to the Monitor and Analyzer executable files, the xxSNIFF directory contains the following files and subdirectories:

- STARTUP.xxD: Contains the name table with all addresses and associated symbolic names. For more information about the STARTUP files, see "STARTUP Files" on page 9–8.
- STARTUP.xxI: Contains the table of the manufacturer's IDs.
- DEFAULTS.xxS: Contains the factory default values for various options, such as filters, triggers, and screen formats. *Do not alter this file.*
- xxSNIFF.HLP subdirectory: Contains the files that generate the analyzer and monitor help systems, which are displayed when the user presses F1 (**Help**).
- xxSNIFF.CFG subdirectory: Lists the facilities available to the Sniffer analyzer and encodes all the protocol interpreter suites that can be installed. **Note:** This is a binary file—*do not* alter it.

CAPTURE Directory

The \CAPTURE directory contains the files that contain captured frames (trace files). It is also the default destination for output files such as .PRN files or .CSV files.

For trace files, you assign the filename and the Sniffer analyzer automatically assigns a three-letter extension. The first two letters identify the network (as shown in Figure 9–2), and the last letter is C, which identifies the file as a trace file that contains captured frames.

Note that trace files have the same internal format as the capture buffer. You cannot read a capture file as text.

REMOTE2 Directory

The REMOTE2 directory contains the files used for remote operation of the Sniffer analyzer.

Configuring the Remote^2 Host

To configure Remote^2 to answer calls from a remote Sniffer Analyzer, you must have a System Manager password. Network General provides Remote^2 Manager with the following default System Manager ID and password:

Default System Manager ID	MANAGER
Default System Manager Password	MANAGER

To configure Remote^2 Host to answer calls from a remote Sniffer Network Analyzer:

1. From the Main Selection Menu of the Sniffer Network Analyzer, highlight **DCA Remote^2** and press Enter.

   Result: The **TeleSniffer Selection Menu for Remote^2** appears.

2. Highlight **Configure Sniffer Host** and press Enter.

   Result: The Remote^2 Manager prompts for a User ID and password.

3. Type in the default System Manager ID and password as provided by Network General.

   Result: The main menu of the Remote^2 Manager appears. From here, you can decide on the Remote^2 Host operating configuration and set up or change the operating parameters for Remote^2 Host users. For more information on the Remote^2 Manager, see the *DCA Remote2 Supplement*, provided with your Sniffer Network Analyzer.

   Note: You can use the Remote^2 Manager to change the default password.

Working with Files

Creating Alternate Directories for Saved Files

To keep your trace files organized, you may want to set up directories in addition to the default directory \CAPTURE.

To create a new directory:

1. Move to **Files\Make directory** and press Enter.

   The Sniffer analyzer opens a dialog box to receive the name of the new directory. The analyzer displays the current path, which is C:\CAPTURE\, unless you previously changed the path.

2. Type the new directory name to the right of the final \ to create a subdirectory of \CAPTURE. You can also backspace over all or part of the path and replace it with whatever you prefer. Press Enter to record the name and create the directory. Do not specify an extension.

Because the Sniffer analyzer limits the file name to eight alphabetic characters, you can't specify an extension for a directory created in this way. If you write a longer name, it is truncated to the first 8 characters.

The Sniffer analyzer accepts the path you specify without verifying that it is syntactically valid or that the directory actually exists. If the path is not valid, you will get the error message "Invalid path" when you subsequently try to read or write a file.

Setting the Path to a Directory for Saved Files

All dialog boxes that let you select an existing file or enter a filename for a new file show the path to the current directory. Initially, this path is C:\CAPTURE\.

To specify the initial path to saved files:

1. Move to **Files\Change path** and press Enter.
2. In the dialog box that appears, type the desired path and press Enter. Note that the path should start with a subdirectory and end with a \ character. As a result, all dialog boxes that are displayed will specify the path you defined.

Note: Specify a directory rather than simply a drive. For example, instead of specifying, "A:\" as the new path, specify, "A:\CAPTURE," or whatever the name of the particular directory may be.

Note: The Sniffer analyzer accepts the path you specify without verifying that it is syntactically valid or that the directory actually exists. If the path is not valid, you will get the error message "Invalid path" when you subsequently try to read or write a file.

STARTUP Files

For information about names associated with addresses or about setups of user-defined options, the Sniffer analyzer refers to four kinds of files, which are identified by the last letter of the extension. Each time the Sniffer analyzer executes, it refers to one or more of these files. Figure 9–4 lists the various startup files.

File name	Contains	How used
STARTUP.xxD	Symbolic names for addresses	At startup, it builds the working name table by reading \xxSNIFF\STARTUP.xxD.
STARTUP.xxI	Symbolic names for manufacturer IDs	At startup, it reads the table of manufacturer IDs from \xxSNIFF\STARTUP.xxI.
STARTUP.xxS	Values for setups of user-defined options.	At startup, it reads from \CAPTURE\STARTUP.xxS to determine values for various options such as filters. This file is user-definable; any options saved with this file name will be automatically applied at startup.

Figure 9–4. The Sniffer analyzer startup files.

Each time you start a Sniffer analyzer, the software automatically checks for the startup files in the *xx*SNIFF directory. If it finds them, it uses them to set its working name table, or to initialize the Sniffer analyzer's filters and settings.

The three types of files (name files, manufacturer ID files, and setup and startup files) use different mechanisms for loading and saving, as shown in Figure 9–5.

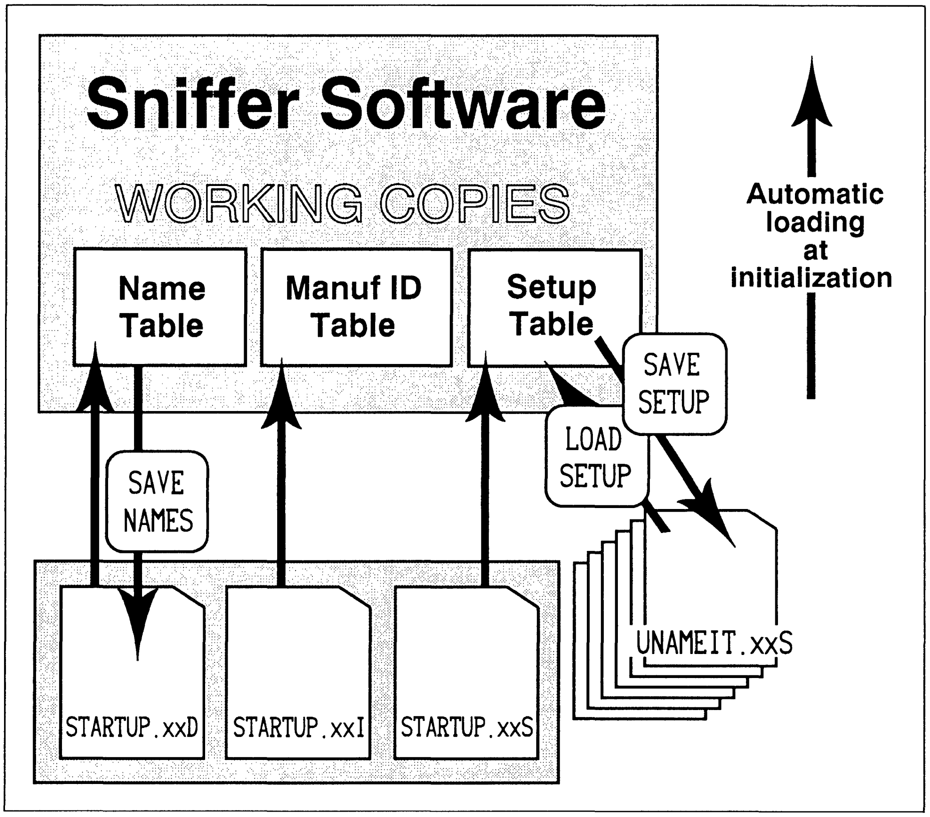


Figure 9–5. Stored files and working copies of name tables and setups.

Modifying the STARTUP.xxS File

The STARTUP.xxS file determines which settings and options are applied at startup. The Sniffer analyzer does not require a startup file. When the analyzer starts, it checks to see whether a STARTUP.*xxS* file exists and uses it. If it doesn't exist, the analyzer uses the default values coded into the Sniffer analyzer executable.

To define the options in effect at startup:

1. Define all options as desired.
2. Move to **Files\Save\Setup** and press Enter.
3. In the dialog box that appears, overwrite the existing path as follows:

   C:\CAPTURE\STARTUP

   Don't include an extension; the Sniffer analyzer automatically attaches the extension .*xx*S (where *xx* is the two-letter network abbreviation). If the file already exists, a warning dialog box appears. You can either abort the request or overwrite the existing file.

Restoring the Factory Defaults

If you have used a customized setup and want to revert to a known state, you can reapply the default setup with which Network General shipped the Sniffer analyzer.

To restore the factory defaults:

1. Move to **Options\Use defaults** and press Enter.

About the Name Tables

Procedures for assigning names to stations are described in Chapter 5, starting on page 5–6. This section describes the format of files that contain name tables.

While it runs, the Sniffer analyzer uses an internal directory called the *working name table*. Each time you start the analyzer thereafter, it initializes the working name table by reading from a file. Ordinarily, the file it reads is *xx*SNIFF\STARTUP.*xx*D.

If the Sniffer analyzer can't find *xx*SNIFF\STARTUP.*xx*D, it looks in the current directory (that is, the directory identified by the **Change path** command). The batch file that starts the Sniffer analyzer normally makes \CAPTURE the default directory, so the Sniffer analyzer looks next for \CAPTURE\STARTUP.*xx*D.

If it doesn't find that file, the Sniffer analyzer sets up an empty name table, containing only the address of the adapter card and the name "This Sniffer."

You may have additional reference files of names and station addresses. These are either renamed copies of what was once a STARTUP.*xx*D file, or files in the same format created by an editor and loaded in the Sniffer analyzer. When you create such a file, you must name it something other than STARTUP, although it will have the same extension as a startup file.

You can read from these additional name files by executing the **Resolve names** command (see page 5–8).

In all cases, the extra name files are used as a source of names to fill blanks in the working name table. There is no command to load an entire substitute name file, the way you load a setup. If you want to maintain several independent name files, use the DOS commands to give them arbitrary names. Before you start the Sniffer analyzer, assign a new name to your existing file STARTUP.*xx*D, and then copy the file you want to make active and name it STARTUP.*xx*D.

Creating Name Files

A name file is identified by an extension consisting of the two-letter network code followed by the letter "D". There are two principal ways to create a name file: by saving and then renaming the working name table, and by writing a name file from scratch with a text editor.

To create a name file from the current working name table:

1. Move to **Display\Manage names\Edit names** and press Enter.
2. Edit the name table that appears, as described in "To edit the working name table:" on page 5–6. When you are finished, press Esc to return to the menus.
3. Move to **Save names** and press Enter. The Sniffer analyzer saves a file called \xxSNIFF\STARTUP.*xx*D, which contains names and addresses for all named stations. Any stations that are not named are discarded.
4. Move to **Exit** and press Enter. Move to **Return to DOS** and press Enter.
5. At the DOS prompt, copy and rename the file as follows:

   ```
   COPY \xxSNIFF\STARTUP.xxD \CAPTURE\newname.*
   ```

Creating your own Name File

You can create your own name file directly. This section describes a name file's internal format.

All name files have the same format, which applies both to the file called STARTUP.*xx*D and any other name files you may use as sources. Figure 9–6 shows part of a name file. Since a name file is a standard ASCII file, you can build it on the Sniffer analyzer or any other PC, using any standard text editor.

```
station "Broadcast"    = addrtype "DLC" C000FFFFFFFF
station "Error Log"    = addrtype "DLC" C00000000008
station "ipS1"         = addrtype "IP" [36.10.0.13]
station "ipS2"         = addrtype "IP" [36.11.0.14]
station "ipS3"         = addrtype "IP" [36.11.0.23]
station "ipS4"         = addrtype "IP" [36.2.0.5]
station "ipS5"         = addrtype "IP" [36.22.0.20]
station "Long, 31-Character Station Name" = addrtype "DLC" 400000000002
station "Mary"         = addrtype "DLC" 10005A0033BF
station "This Sniffer" = addrtype "DLC" 48000A000001
station "Tom"          = addrtype "DLC" 10005A002FEB
station "Faquard"      = addrtype "XNS" 08000AC7CEFE
```

Figure 9–6. Sample name file.

For convenience during subsequent display, the **Save names** command sorts the rows of the table alphabetically by name. However, the analyzer does not require a name file to be in alphabetical order.

The following features of a name table are illustrated in Figure 9–6 and Figure 9–7.

Type

Each line starts with a word or symbol that identifies its type. The three line types are distinguished by the following as their first non-blank characters:

`station` The balance of the line describes one station's name and address.

`addrtype` The balance of the line sets the default address type (protocol) that applies to subsequent lines that don't include it explicitly.

/* A line that starts with /* and ends with */ is a comment and is not executed.

Name

The station's name appears to the right of the word "station." The name must be enclosed in double quotes.

Address type

Each address must be assigned to a specific type (that is, protocol). The type can be stated in either of two ways:

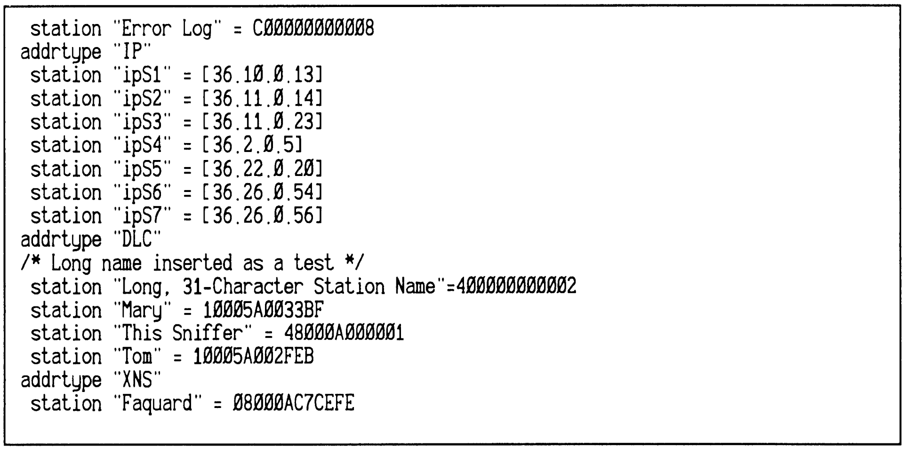
- Explicitly for each address, by including the phrase
  `addrtype "DLC"`
  to the left of the address (as shown in Figure 9–6). A name file generated by the **Save names** command is entirely in this form.
- Implicitly, using the current default type (Figure 9–7).An address that has no explicit type is presumed to belong to the current default type. The default type is initially "DLC". The default type is set by each use of **addrtype**, and remains in effect until another **addrtype**.

Address

There is an = sign between the name and the address. An address is not enclosed in quotes. Each address is written in a form appropriate to its type (the same way the Sniffer displays it in the detail view). For example, a 6-byte DLC address is written as 12 hexadecimal digits. A 4-byte IP address is written as four decimal numbers separated by dots and entirely surrounded by square brackets.

Name Table with Default Types

Figure 9–7 shows the same information as Figure 9–6, but makes use of *default types*. To improve readability, the file may contain redundant blanks or blank lines, as well as comments. A comment starts with /* and ends with */.



```
 station "Error Log" = C00000000008
addrtype "IP"
 station "ipS1" = [36.10.0.13]
 station "ipS2" = [36.11.0.14]
 station "ipS3" = [36.11.0.23]
 station "ipS4" = [36.2.0.5]
 station "ipS5" = [36.22.0.20]
 station "ipS6" = [36.26.0.54]
 station "ipS7" = [36.26.0.56]
addrtype "DLC"
/* Long name inserted as a test */
 station "Long, 31-Character Station Name"=400000000002
 station "Mary" = 10005A0033BF
 station "This Sniffer" = 48000A000001
 station "Tom" = 10005A002FEB
addrtype "XNS"
 station "Faquard" = 08000AC7CEFE
```

Figure 9–7. The name file of Figure 9–6 rewritten with default types.

Alphabetization of Station Names

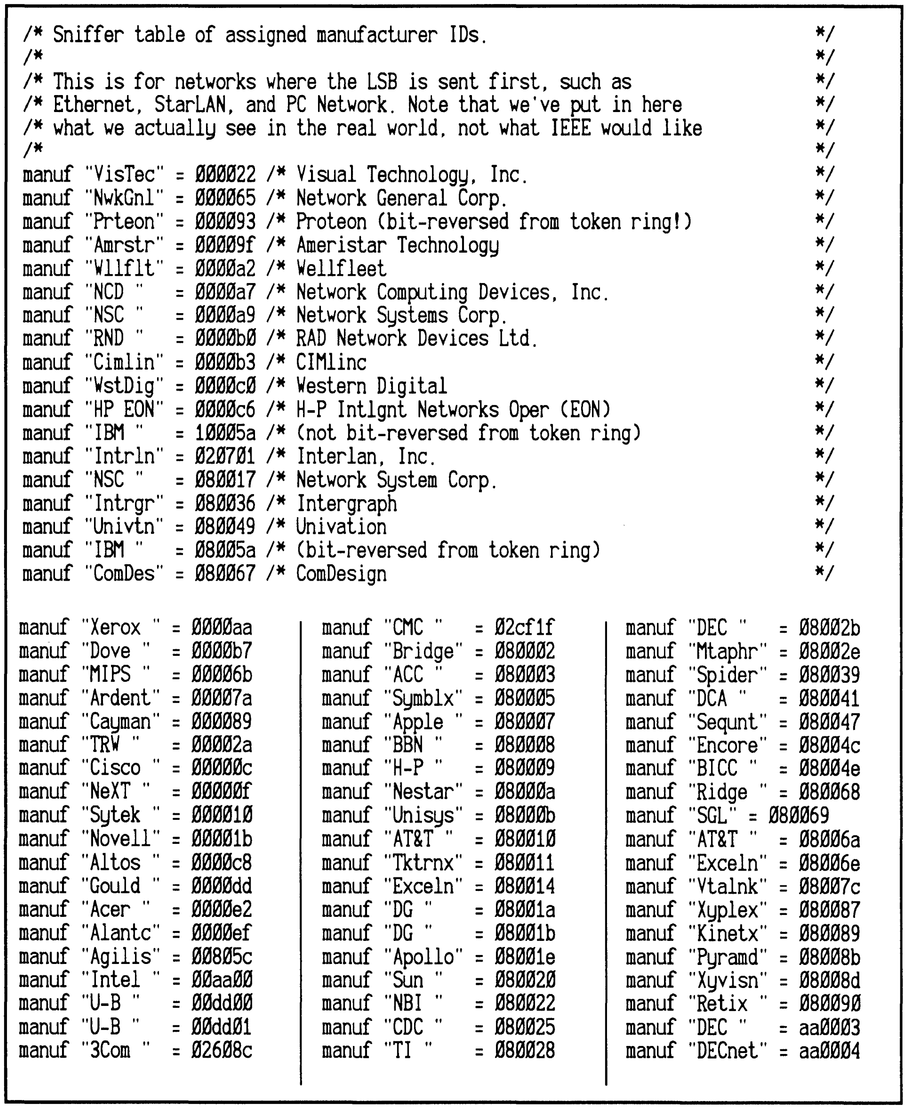
You can enter names in any order. When the Sniffer builds and displays its working name table, it shows the list in alphabetical order by name. Addresses that you haven't named (and therefore have blank names) appear at the top of the list.

Each time you edit the working name table, the Sniffer re-alphabetizes the list. When you execute **Save names,** the saved file preserves the alphabetical order of the working name table. However, entries that are not named are discarded.

Table of Manufacturer ID Codes and Abbreviations

On most LANs, an address consists of six bytes. The first three represent the manufacturer. The Sniffer attempts to represent the first three bytes by a six-character abbreviation of the manufacturer's name. The address then appears as six characters of manufacturer abbreviation followed by six characters of hexadecimal, for example Intrln031EF7.

The table of manufacturer codes and names is located in the file startup.*xx*I, where *xx* is the two-letter code for the network, and I indicates the ID table. The file's internal format is illustrated in Figure 9–8. The figure shows the content of the file STARTUP.*xx*I for a network that transmits least significant bit first (for example, Ethernet but not token ring). The comments in the file are for the convenience of the user and have no effect on the Sniffer analyzer's use of the file. (For compactness, the lower part of the table is shown here with three entries per line. In the file, each entry has a line of its own.)



```
/* Sniffer table of assigned manufacturer IDs.                            */
/*                                                                        */
/* This is for networks where the LSB is sent first, such as              */
/* Ethernet, StarLAN, and PC Network. Note that we've put in here         */
/* what we actually see in the real world, not what IEEE would like       */
/*                                                                        */
manuf "VisTec" = 000022 /* Visual Technology, Inc.                        */
manuf "NwkGnl" = 000065 /* Network General Corp.                          */
manuf "Prteon" = 000093 /* Proteon (bit-reversed from token ring!)        */
manuf "Amrstr" = 00009f /* Ameristar Technology                           */
manuf "Wllflt" = 0000a2 /* Wellfleet                                      */
manuf "NCD "   = 0000a7 /* Network Computing Devices, Inc.                */
manuf "NSC "   = 0000a9 /* Network Systems Corp.                          */
manuf "RND "   = 0000b0 /* RAD Network Devices Ltd.                       */
manuf "Cimlin" = 0000b3 /* CIMlinc                                        */
manuf "WstDig" = 0000c0 /* Western Digital                                */
manuf "HP EON" = 0000c6 /* H-P Intlgnt Networks Oper (EON)                */
manuf "IBM "   = 10005a /* (not bit-reversed from token ring)             */
manuf "Intrln" = 020701 /* Interlan, Inc.                                 */
manuf "NSC "   = 080017 /* Network System Corp.                           */
manuf "Intrgr" = 080036 /* Intergraph                                     */
manuf "Univtn" = 080049 /* Univation                                      */
manuf "IBM "   = 08005a /* (bit-reversed from token ring)                 */
manuf "ComDes" = 080067 /* ComDesign                                      */

manuf "Xerox " = 0000aa  |  manuf "CMC "   = 02cf1f  |  manuf "DEC "   = 08002b
manuf "Dove "  = 0000b7  |  manuf "Bridge" = 080002  |  manuf "Mtaphr" = 08002e
manuf "MIPS "  = 00006b  |  manuf "ACC "   = 080003  |  manuf "Spider" = 080039
manuf "Ardent" = 00007a  |  manuf "Symblx" = 080005  |  manuf "DCA "   = 080041
manuf "Cayman" = 000089  |  manuf "Apple " = 080007  |  manuf "Sequnt" = 080047
manuf "TRW "   = 00002a  |  manuf "BBN "   = 080008  |  manuf "Encore" = 08004c
manuf "Cisco " = 00000c  |  manuf "H-P "   = 080009  |  manuf "BICC "  = 08004e
manuf "NeXT "  = 00000f  |  manuf "Nestar" = 08000a  |  manuf "Ridge " = 080068
manuf "Sytek " = 000010  |  manuf "Unisys" = 08000b  |  manuf "SGL" = 080069
manuf "Novell" = 00001b  |  manuf "AT&T "  = 080010  |  manuf "AT&T "  = 08006a
manuf "Altos " = 0000c8  |  manuf "Tktrnx" = 080011  |  manuf "Exceln" = 08006e
manuf "Gould " = 0000dd  |  manuf "Exceln" = 080014  |  manuf "Vtalnk" = 08007c
manuf "Acer "  = 0000e2  |  manuf "DG "    = 08001a  |  manuf "Xyplex" = 080087
manuf "Alantc" = 0000ef  |  manuf "DG "    = 08001b  |  manuf "Kinetx" = 080089
manuf "Agilis" = 00805c  |  manuf "Apollo" = 08001e  |  manuf "Pyramd" = 08008b
manuf "Intel " = 00aa00  |  manuf "Sun "   = 080020  |  manuf "Xyvisn" = 08008d
manuf "U-B "   = 00dd00  |  manuf "NBI "   = 080022  |  manuf "Retix " = 080090
manuf "U-B "   = 00dd01  |  manuf "CDC "   = 080025  |  manuf "DEC "   = aa0003
manuf "3Com "  = 02608c  |  manuf "TI "    = 080028  |  manuf "DECnet" = aa0004
```

Figure 9–8. Manufacturer ID translation.

Manufacturer IDs in the table are shown as they appear in the computer once they have been captured. The IEEE assignment of IDs specifies the sequence in which bits are transmitted on the wire. For networks that transmit each byte low-order-bit first (such as Ethernet) the address you see after it has been captured is the byte-by-byte reverse of what was transmitted on the wire. For example, the code used by IBM is transmitted on the network by the sequence 00010000 00000000 01011010. It appears to a token ring Sniffer analyzer as 10 00 5A, but to an Ethernet Sniffer analyzer as 08 00 5A.

File Formats

The contents of the capture buffer (before or after filtering) may be saved in a file or sent to a printer. If saved in a file, the contents may be in a printer format (with or without page titles and page numbers), or in the CSV format recognized by standard spread sheets. The files thus produced have the extension .PRN for printer files and .CSV for spread sheet files. (For details of this procedure, see, "To create a report:" on page 4–47.)

Format of Saved Data Files

You can use a saved data file for data analysis. For example, you can write a program that reads through a file of saved frames. The easiest format to work with is the ASCII file you get when you "print" the capture buffer to a file. This can be especially helpful if you choose the option to omit page titles. The resulting file will contain the information you want in an easily-accessible format.

Alternatively, you may prefer to operate directly on the trace file that the Sniffer analyzer writes in response to the **Save data** command. This section describes the format of such a trace file.

Each trace file consists of sequences of variable length binary records. Since all 256 byte values are possible within the data, you cannot edit this file using an ordinary text editor.

The first 16 bytes of a trace file contain a text message identifying the file as one containing data collected by the Sniffer analyzer.[1] The message is followed by an end-of-file character (hex 1A, also called Ctrl-Z). Even if you accidentally type the file to the screen, or otherwise treat it as a text file, the display reaches a terminator before reaching unprintable characters.

Structures within the Data File

Following the text message string, the file contains an arbitrary number of variable-length records. Each record has a type, identified in its first two bytes. The three principal types are:

- Version record
- Frame record
- End-of-file record

The first record in the file is always a version record, the last is always an end-of-file record, and those in between are usually (but not necessarily) frame records.

There is no explicit encoding of the file's total length (except as part of its directory entry).

[1] For historical reasons, the message in all such files is "TRSNIFF data", regardless of the network on which the frames were collected.

Header

Every record of any type begins with the following header:

```
struct f_rec_struc {    /* Standard record header.                       */
int    type;            /* Type of this record. (Int = 2 bytes)          */
int    length;          /* Length of remainder of this record.           */
int    rsvd;            /* Reserved word, currently 0.                   */
};
```

The header's first field indicates what type of record follows. The three principal types are identified by the following values:

```
#define REC_VERS          1   /* Version record (f_vers).              */
#define REC_FRAME2        4   /* Frame data (f_frame2).                */
#define REC_EOF           3   /* End-of-file record (no data follows). */
```

Types other than these are reserved for future or other use. If you write a program to process data files, you should have it skip any record that is not one of these types. The length field indicates how much data to skip.

Format of a Version Record

```
struct f_vers_struct   {
int        maj_vers;          /* Major version of the Sniffer          */
int        min_vers;          /* Minor version of the Sniffer          */
struct     date_struct date   /* Date & time (4 bytes, DOS format[1])   */
char       type;              /* What type of records follow.          */
char       network;           /* An indicator of the network type.     */
char       format;            /* An indicator of the format version.   */
char       timeunit;          /* An indicator of the frame timestamp unit. */
int        rsvd[3];           /* Reserved words.                       */
};
```

The possible values of **network** are as follows:

```
#define        NETWORK_TRING        0    /* Token ring             */
#define        NETWORK_ENET         1    /* Ethernet               */
#define        NETWORK_ARCNET       2    /* ARCNET                 */
#define        NETWORK_STARLAN      3    /* StarLAN                */
#define        NETWORK_PCNW         4    /* PC Network broadband   */
#define        NETWORK_LOCALTALK    5    /* LocalTalk              */
#define        NETWORK_ZNET         6    /* Znet                   */
```

The possible values of **timeunit** are as follows:

```
#define    TIMEUNIT_UNSPEC    0   /*   Unspecified; default by network type. */
#define    TIMEUNIT_PC        1   /*   0.838096       microsecond units      */
```

[1] Standard DOS format for dates is *mm-dd-yy*. Standard DOS format for times is *hh:mm*, followed by a one-letter designation for *AM/PM*.

```
#define    TIMEUNIT_3COM     2   /*   15.000000     microsecond units     */
#define    TIMEUNIT_MICOM    3   /*    0.500000     microsecond units     */
#define    TIMEUNIT_SYTEK    4   /*    2.000000     microsecond units     */
```

Format of a Frame Data Record

Each record starts with a header, as described above, followed by data in the following structure:

```
struct     f_frame2_struct    {
unsigned   time_low;       /* Low time, network-dependent units.          */
unsigned   time_mid;       /* Mid time, network-dependent units.          */
char       time_high;      /* High time, network-dependent units.         */
char       time_day;       /* Time in days since start of capture.        */
int        size;           /* Number of bytes actually written in this file
                              (may be less than frame's original length).  */
char       fs;             /* Frame error status bits.                    */
char       flags;          /* Buffer flags; for internal use.             */
int        true_size;      /* If nonzero, the size of the original frame
                                 (since this frame has been truncated).    */
int        rsvd;   }       /* Reserved; currently 0.
                              The frame data follows.                      */
```

All multibyte arithmetic fields (computed by the Sniffer analyzer during capture) are stored with the least significant byte first. Frame data are stored in the byte order transmitted.

Format of an End-of-file Record

The end-of-file record has no data; it consists only of the record header.

The Startup Parameters

A number of parameters affect the Sniffer analyzer's operation. Some parameters reflect the particular platform and network interface card, so they should not be changed. Others reflect the way you use the analyzer, which may change with circumstances. For those parameters that are likely to change, there are items in the menu. The sections that follow describe how to alter software parameters that are not represented in the menus.

Caution: In many cases, a change in a startup parameter must be accompanied by a corresponding change in the physical equipment. For example, changing the software record of parameters such as the NIC's interrupt request makes no sense unless you also make the appropriate changes to jumpers or dip switches on the interface card. Such changes are probably necessary only when you introduce non-standard variations in the equipment you are using. Before you make changes to the Sniffer analyzer's hardware, we strongly advise you to consult the Technical Support Department at Network General Corporation.

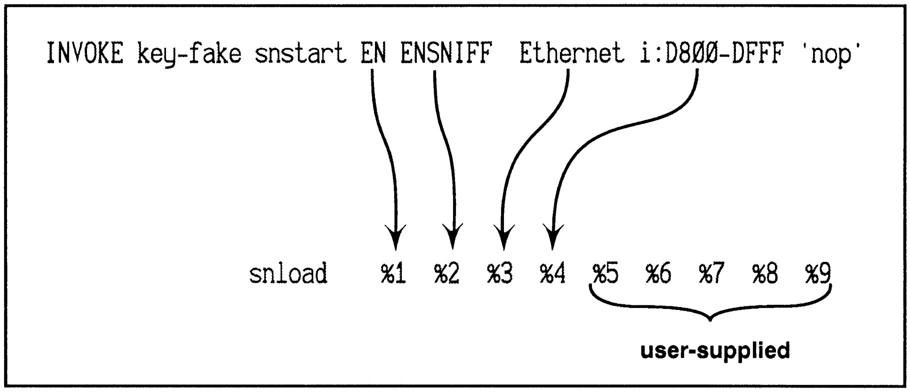
How the Parameters are Passed

Startup parameters are passed to the Sniffer analyzer as part of the statement that invokes the analyzer's executable file *xx*SNIFF.EXE. Ordinarily you don't type that statement, or even see it. The statement that launches the analyzer receives input from three sources. Depending on the sort of change you want, there are three places at which you might make revisions to the files. Each is described below.

The command to launch a Sniffer analyzer is located inside the batch file that is executed whenever you select an analyzer in the main selection menu and press **Enter**. That file is SNSTART.BAT (located in the \TOOLS directory). Thus, to make a change that affects the operation of *every* analyzer available on your machine, modify SNSTART.BAT (as described below).

The file SNSTART.BAT does not contain the startup parameters directly. It receives them as arguments, or by referring to DOS environment variables. For each item in the selection menu, there is a separate file with a name ending in .MNU. The various .MNU files all reside in the \CONFIG directory. Each .MNU file describes a single item on the screen of the selection menu. It specifies both the text you see on screen and the action to be taken when you select that item. An item's .MNU file specifies the arguments that will be passed to SNSTART.BAT. Thus to make a change that is specific to a particular executable file (that is, to a single item in the main selection menu) you might edit its .MNU file (as described below).

The location of startup parameters in the files SNSTART.BAT and *xx*SNIFF.MNU is illustrated in Figure 9–9.



```
INVOKE key-fake snstart EN ENSNIFF  Ethernet i:D800-DFFF 'nop'

                  snload    %1  %2  %3  %4  %5  %6  %7  %8  %9
```

Figure 9–9. Passing parameters from TOOLS \ SNSTART.BAT to \ TOOLS \ SNLOAD.BAT.

Editing the Startup Parameters

You can edit the startup parameters in one of three ways.

To edit the startup parameters:

1. Modify parameters for a specific Sniffer analyzer by editing its .MNU file.

This modification affects a single executable file. In the \CONFIG directory, locate the appropriate .MNU file. In its last line, replace the characters "NOP" with one or more parameters, each enclosed in double quotes and set off from each other by blanks.

For example, to specify a maximum of 800 names in the address table and a capture buffer of 40 Kbytes, replace "NOP" by "MAXSTNS=800" "BUF=40k".

Caution: If you increase the maximum number of stations to more than 5000 names, your network is heavily loaded, and you want to use the **Look for names** and **Edit names** functions, use the following precaution:

Do not use the **Look for names** and the **Edit names** feature after displaying analyzed data. If you need to edit, save the file and then reload it. *Do not* display it at this point—use **Edit names** to change the name table and *then* display.

2. Modify parameters for all Sniffer analyzers by editing SNSTART.BAT.

   Locate the line that begins with **snload**. Append your parameters at the end of the line, following **%9**. Put double quotes around each parameter.

   In the line that begins with **snload**, the entries **%5** through **%9** are there to pass any additional parameters that may have been inserted in .MNU files. Do *not* delete these parameters unless you are certain that none of your .MNU files have been modified to include additional parameters.

3. Set screen parameters by setting DOS environment variables.

   You can use DOS environment variables to set values for SCR (which specifies the type of monitor) or SCRMODE (which controls the way the scrolling is shown as you move from one menu panel to another). At the DOS prompt, type "set scr=" or "set scrmode=" followed by one of the possible values.

Caution: The environment variables are lost when you reset the machine or turn off power. To have them automatically regenerated at each power-on, insert a statement in \AUTOEXEC.BAT. Choosing any of the screen options in the main selection menu also sets the environment variable SCR (and therefore overwrites any earlier setting of SCR).

Position and Duplication of Parameters

The first four parameters passed to SNSTART.BAT are interpreted by position. That is, the first *must* be a two-letter network abbreviation, the second *must* be the name of the executable file, the third *must* be the name of the network, and the fourth *must* be a memory specification for FIXEMM. After the first four, there is no required order for the others.

The Sniffer analyzer receives its parameters as specified by the line in SNSTART.BAT that begins with **snload**. It scans the parameters in order from left to right. If you supply duplicate or contradictory parameters, a later one (that is, one further to the right) overrides an earlier one.

The way SNSTART.BAT is written (Figure 9–9), the first parameter passed to the analyzer is the value of the DOS environment variable SCR, followed by the value of SCRMODE, followed by up to five parameters that may have been substituted for "**NOP**" in the .MNU file. If you edited SNSTART.BAT by appending more parameters at the end of the line, being further to the right they are evaluated later, and can overwrite those to the left.

Listing of the Startup Parameters

The tables that follow show the parameters for which you can define values. Figure 9–10 shows the startup parameters that affect the context of use, Figure 9–11 shows the parameters that affect expanded memory, and Figure 9–12 shows the startup parameters that report the configuration of the adapter card.

Parameter	Values
Screen display attributes (DOS environment variable SCR). To optimize attributes in the analyzer's display screens, the analyzer selects color or shading attributes to match the capabilities of various devices. GRAY is intended for Compaq monochrome gray scale, LCD for liquid crystal displays with black characters on a clear background, and LCDR for the reverse.	MONO COLOR/COLOU R GRAY/GREY LCD LCDR PLASMA
Scrolling during panel-to-panel movement (DOS environment variable SCR mode). On a local screen during transition to a new panel, the analyzer redraws the screen in stages to convey the effect of motion. When you control the analyzer from a remote station, it may be preferable to eliminate the transition display to save time.	NOSCROLL
Typeahead. By default, the analyzer does not accept new keystrokes during display. You may permit typeahead up to the limit of the DOS input buffer (15 characters).	TYPEAHEAD
Buffer size limit. Ordinarily, the analyzer allocates all available expanded memory for the capture buffer and reports an error when it finds less than 50K. You may set the size explicitly, but not to less than 10K.	BUF=*nnn*K
Maximum number of stations in the name table. You can reserve space for the working name table, making it either smaller or larger than its default capacity of 500 station addresses. The maximum will be 8000.	MAXSTNS=*nnn*

Number of rows or columns in the display screen. The analyzer automatically detects the size of the display. These parameters permit you to declare some other size.	ROWS=*nnn*
	COLS=*nnn*

CGA flicker adjustment. Some early CGA monitors will flicker unless access to the screen is confined to retrace. To force the display drivers to wait until retrace, choose WAIT; the analyzer's default is NOWAIT.	WAIT NOWAIT

Figure 9–10. Startup parameters affecting the context of use.

Parameter	Values
Expanded memory allocation. The parameters I= and E= do not affect the analyzer itself but rather the expanded memory manager. Within SNSTART.BAT, the line that begins FIXEMM contains two uses of I=. These are followed by a reference to %4, which passes a use of I= or E= from the .MNU file that invoked SNSTART. The parameter I= or E= is followed by a pair of hexadecimal addresses specifying the beginning and end (inclusive) of a block of extended memory to be included (I) or excluded (E) from the memory made available to the Sniffer analyzer. The starting address must be on a 16K boundary and at least A0000; each is written in 16-byte units, so that (for example) the address C8ff0 appears simply as C8FF (without the trailing 0, or a final H).	**I=*hhhh-hhhh*** **E=*hhhh-hhhh***

Figure 9–11. Startup parameters that affect expanded memory.

Parameter	Values
Report the Network Interface Card's interrupt level. The parameter IRQ= informs the Sniffer software which interrupt line the adapter card is using.	**IRQ=n**
Report the Network Interface Card's I/O Addresses. The parameter IOBASE= reports the start of I/O memory. The argument must be written as four hexadecimal digits, without a following H.	**IOBASE=*hhhh***
Report the Network Interface Card's RAM Addresses. The parameter RAMBASE= reports the start of addressable RAM. The argument must be written as four hexadecimal digits, without a following H.	**RAMBASE=*hhh h***
Report the Network Interface Card's DMA Channel. The parameter DMA= reports the number assigned to the adapter card's direct memory access channel. The argument is a one- or two-digit decimal number.	**DMA=*n***

Important: These parameters do not *set* characteristics of the adapter card; they simply report to the Sniffer analyzer a description of the card's characteristics. In most cases, those characteristics are controlled or modified by setting DIP switches or jumpers on the card.

Figure 9–12. Startup parameters that report the configuration of the adapter card.

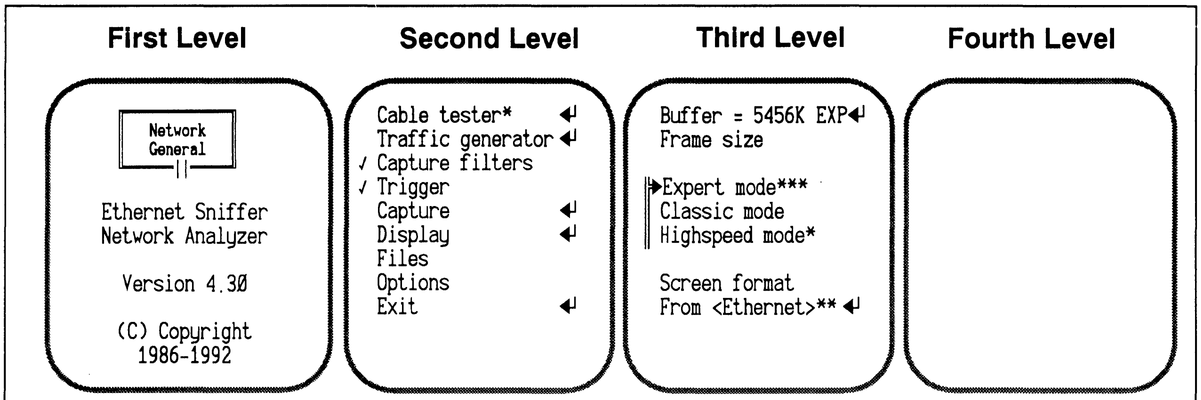
APPENDIX A: OVERVIEW OF MENU OPTIONS

A

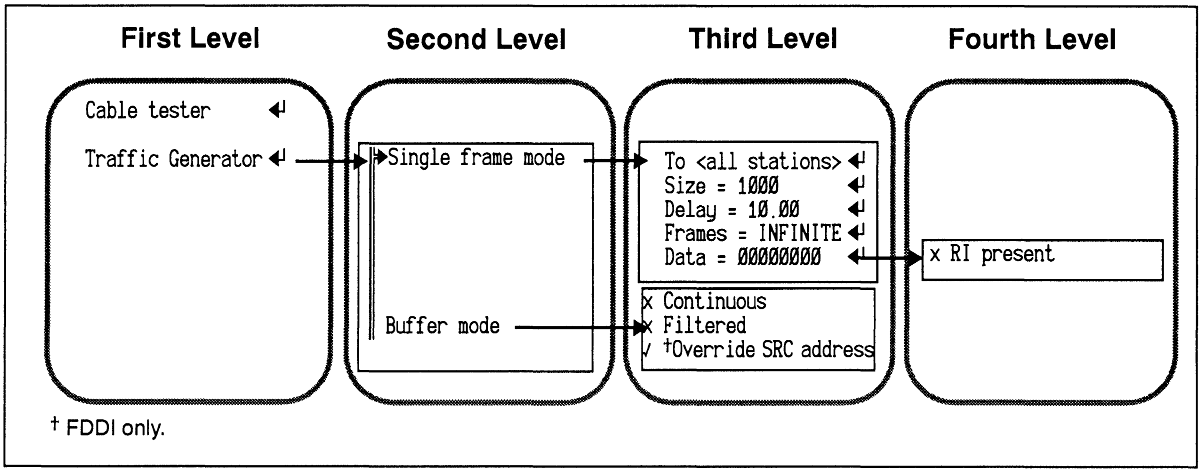
Network General

Appendix A. Overview of Menu Options

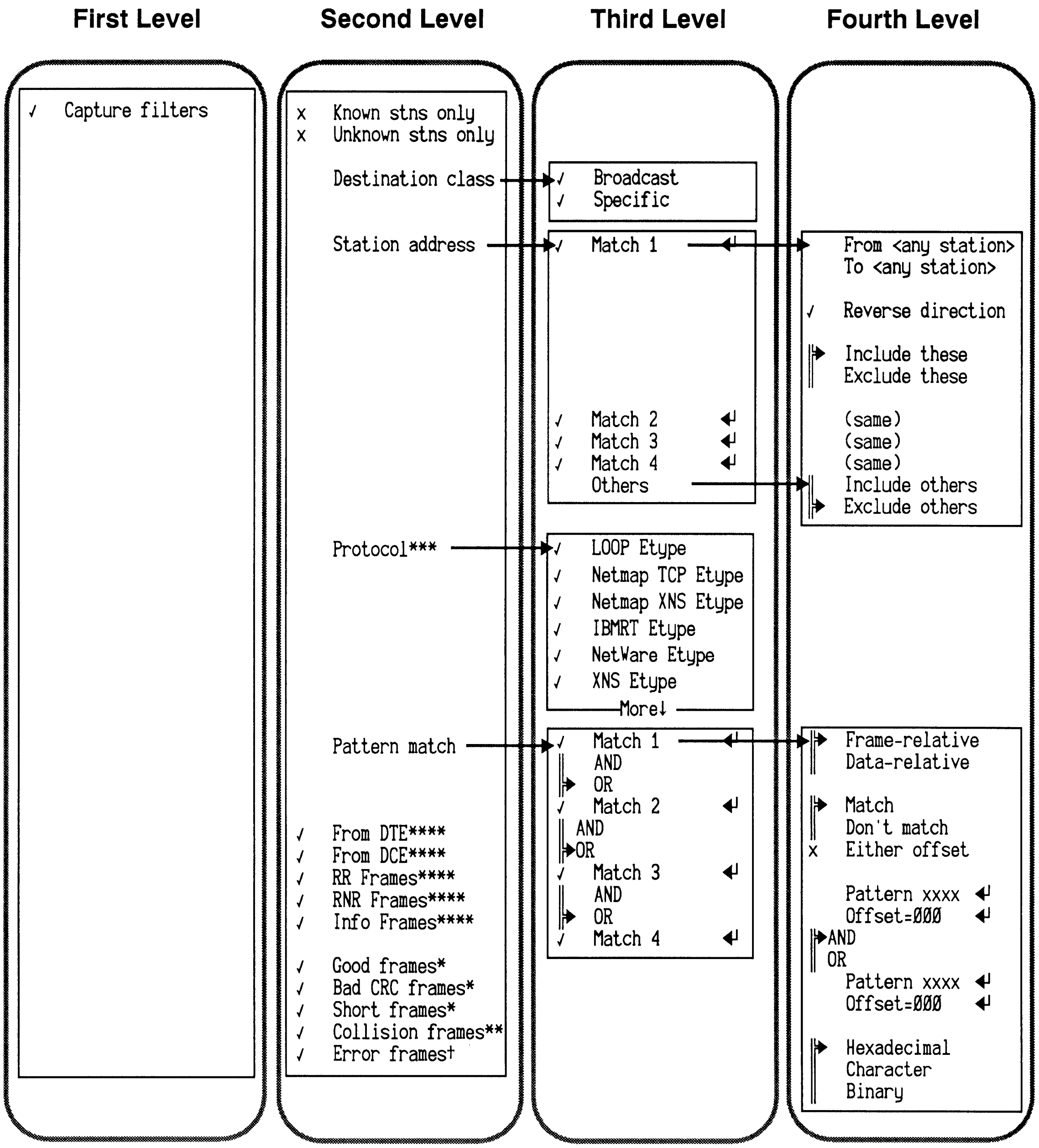
This appendix provides an overview of all menu items associated with the analysis application of the Sniffer Network Analyzer. The defaults shown in these illustrations are the factory default values with which your analyzer is shipped. You can restore these values at any time by using the **Use defaults** command.



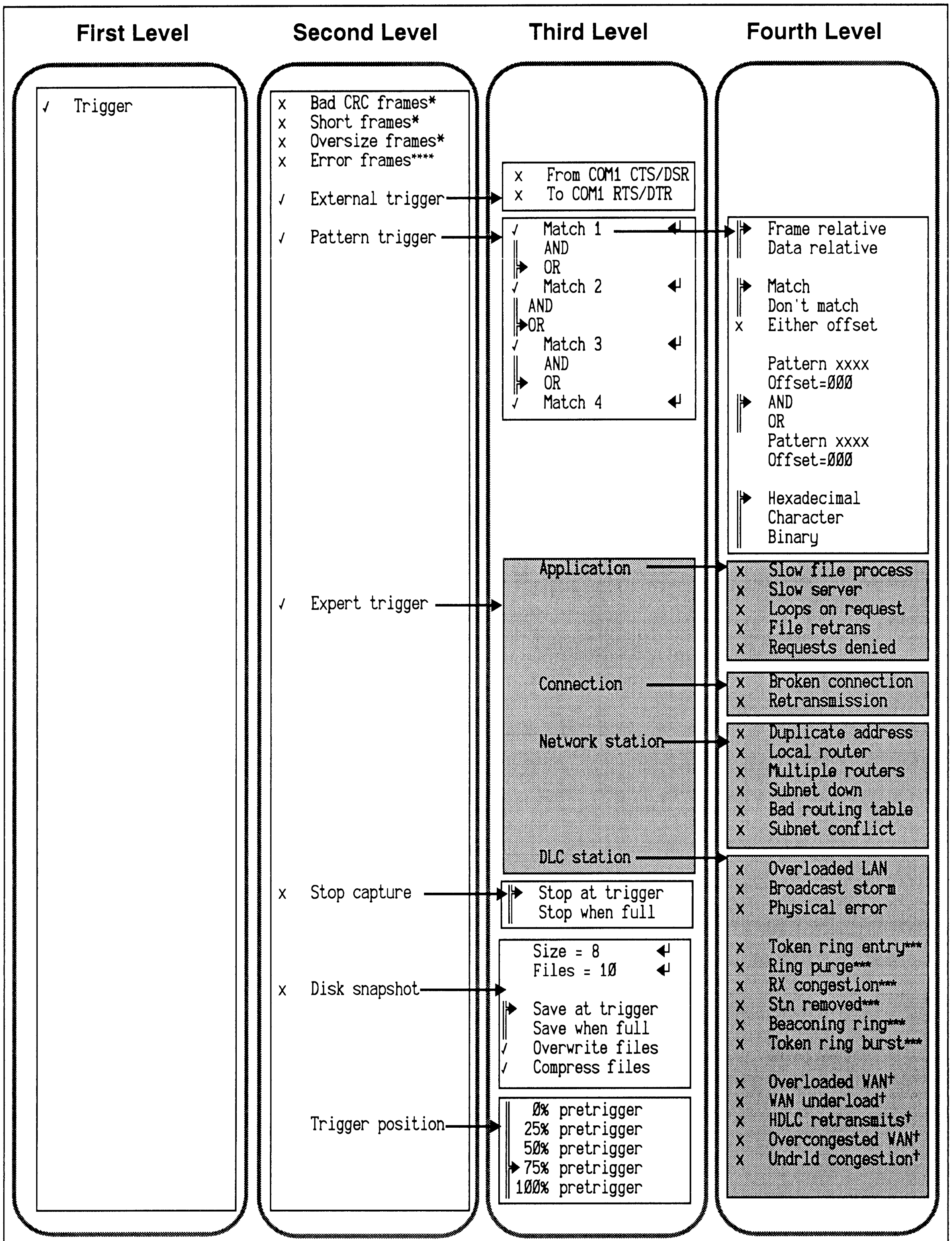
*Ethernet only.
**Shows your network.
***Expert analyzer only



† FDDI only.



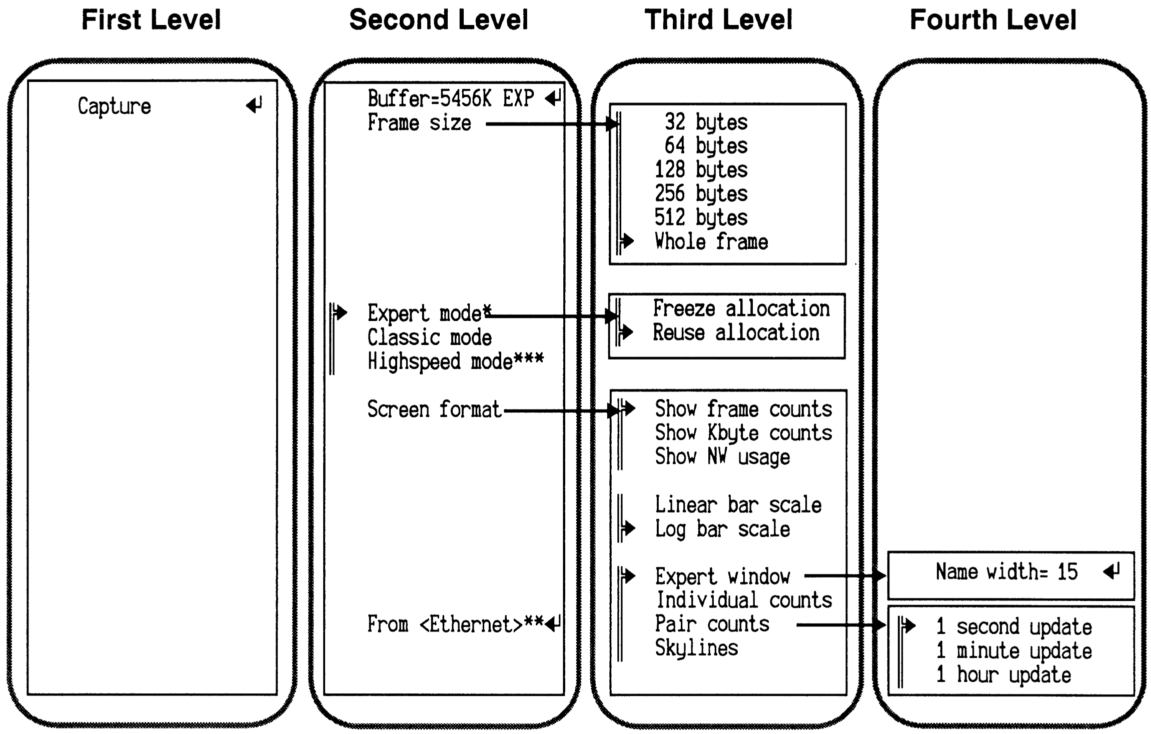
*Ethernet only.
**Ethernet II only.
***Will vary depending on network.
****Internetwork Analyzer (WAN/Synchronous).
† FDDI only.



*Ethernet only.
**Ethernet II only.

*** Token ring only
† Internetwork analyzer only.

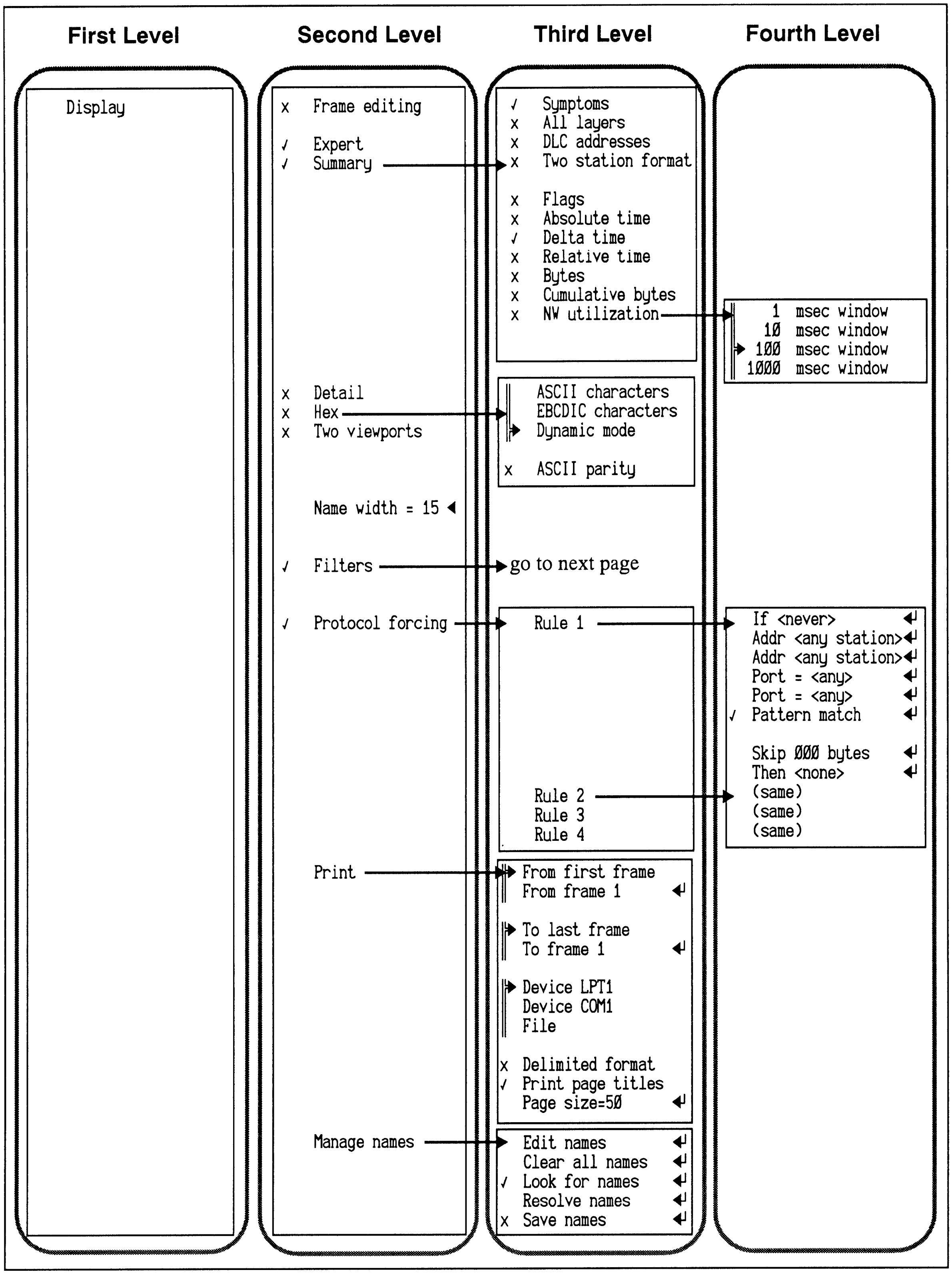
▨ Expert analyzer only.
**** FDDI only

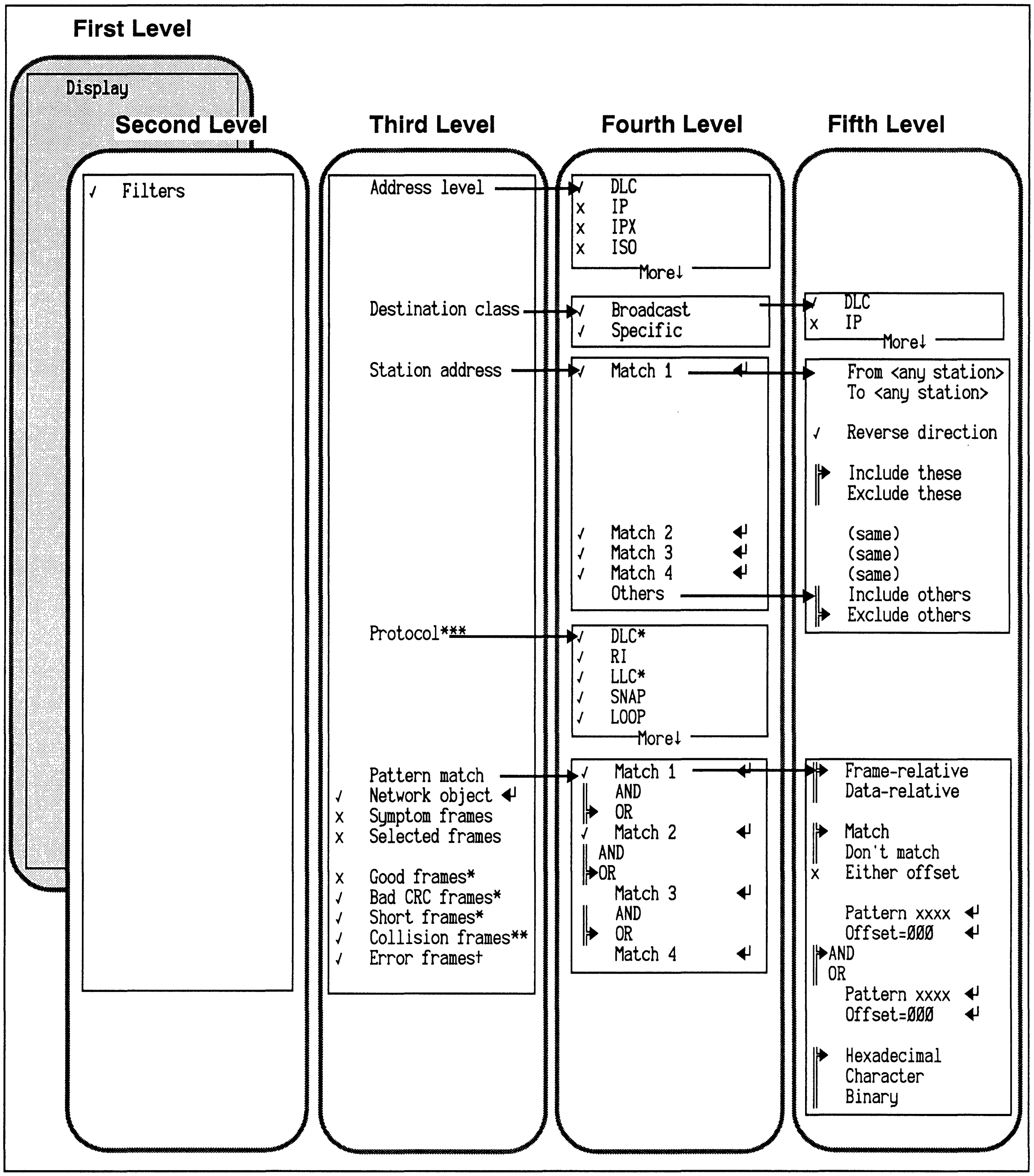


* Expert analyzer only.

** Shows your network.

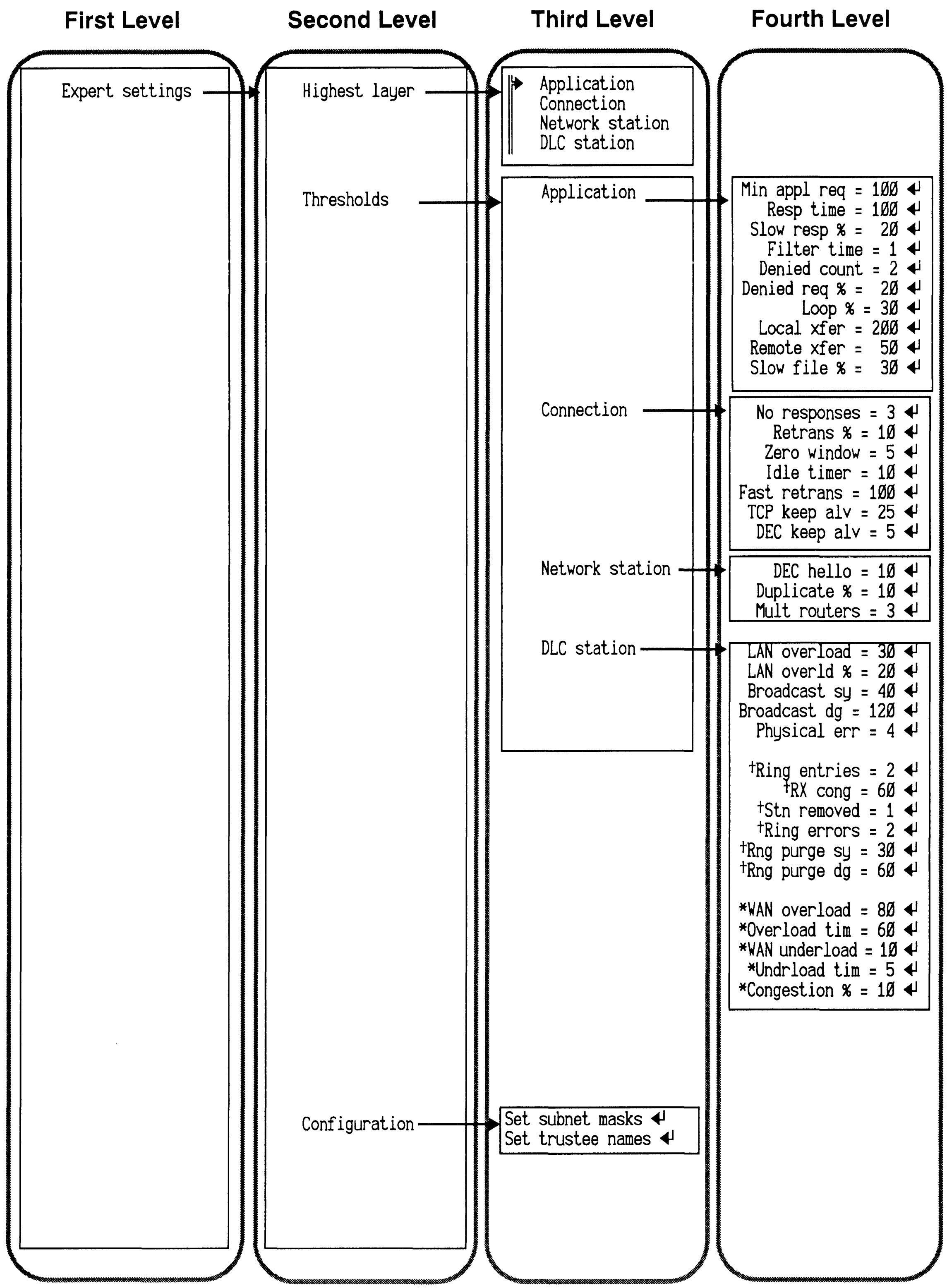
*** Ethernet and PC-Net only.


First Level
Second Level
Third Level
Fourth Level
Display
x Frame editing
√ Expert
√ Summary
√ Symptoms
x All layers
x DLC addresses
x Two station format
x Flags
x Absolute time
√ Delta time
x Relative time
x Bytes
x Cumulative bytes
x NW utilization
1 msec window
10 msec window
100 msec window
1000 msec window
x Detail
x Hex
x Two viewports
ASCII characters
EBCDIC characters
Dynamic mode
x ASCII parity
Name width = 15
√ Filters
go to next page
√ Protocol forcing
Rule 1
Rule 2
Rule 3
Rule 4
If <never>
Addr <any station>
Addr <any station>
Port = <any>
Port = <any>
√ Pattern match
Skip 000 bytes
Then <none>
(same)
(same)
(same)
Print
From first frame
From frame 1
To last frame
To frame 1
Device LPT1
Device COM1
File
x Delimited format
√ Print page titles
Page size=50
Manage names
Edit names
Clear all names
√ Look for names
Resolve names
x Save names



*Ethernet only.
**Ethernet II only.
***Will vary depending on network.

† FDDI only.



Min appl req = 100 ↵
Resp time = 100 ↵
Slow resp % = 20 ↵
Filter time = 1 ↵
Denied count = 2 ↵
Denied req % = 20 ↵
Loop % = 30 ↵
Local xfer = 200 ↵
Remote xfer = 50 ↵
Slow file % = 30 ↵

No responses = 3 ↵
Retrans % = 10 ↵
Zero window = 5 ↵
Idle timer = 10 ↵
Fast retrans = 100 ↵
TCP keep alv = 25 ↵
DEC keep alv = 5 ↵

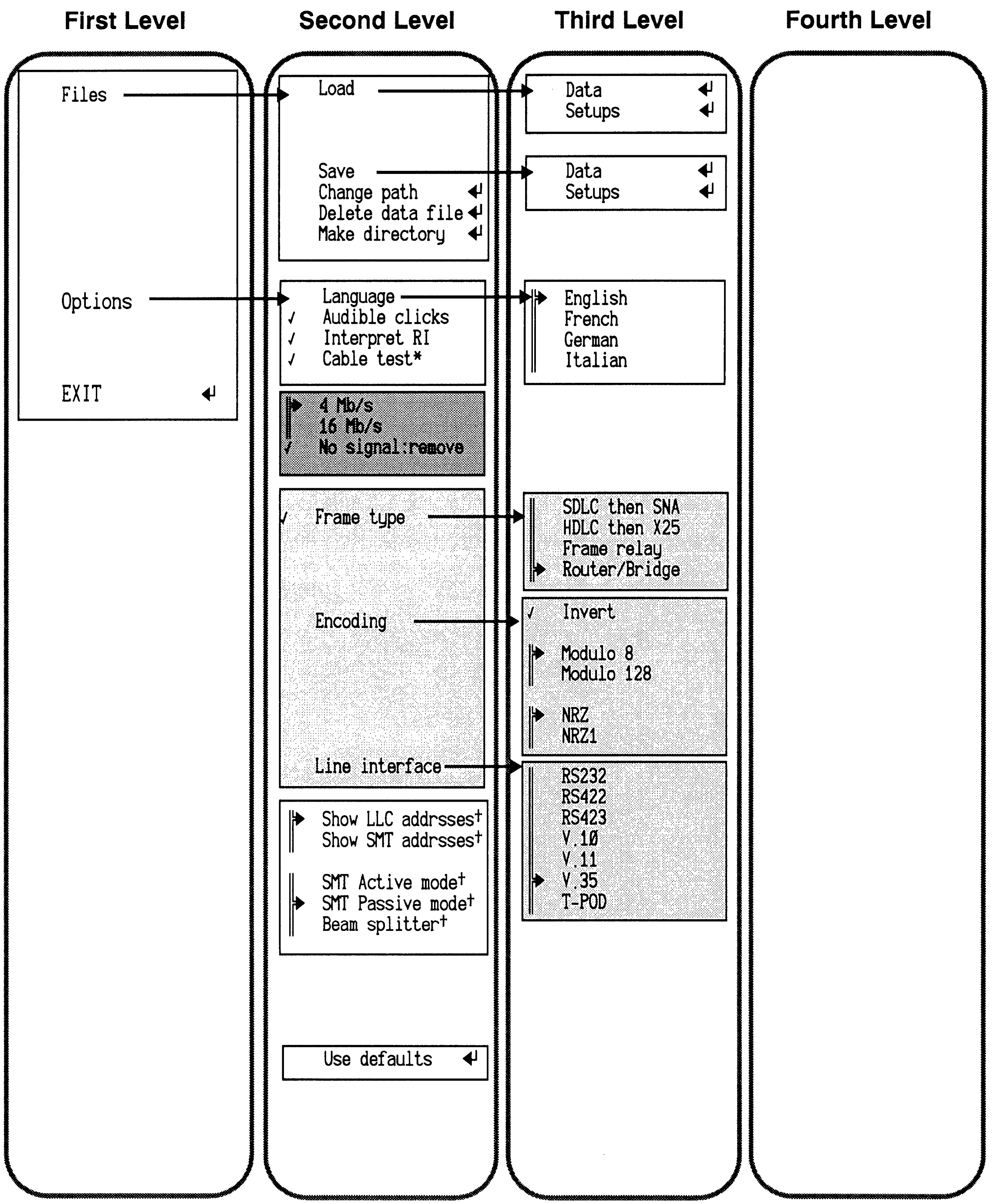
DEC hello = 10 ↵
Duplicate % = 10 ↵
Mult routers = 3 ↵

LAN overload = 30 ↵
LAN overld % = 20 ↵
Broadcast sy = 40 ↵
Broadcast dg = 120 ↵
Physical err = 4 ↵

†Ring entries = 2 ↵
†RX cong = 60 ↵
†Stn removed = 1 ↵
†Ring errors = 2 ↵
†Rng purge sy = 30 ↵
†Rng purge dg = 60 ↵

*WAN overload = 80 ↵
*Overload tim = 60 ↵
*WAN underload = 10 ↵
*Undrload tim = 5 ↵
*Congestion % = 10 ↵

Entire menu found only on Expert analyzer. * Internetwork analyzer only. † Token ring only



▨ Represents token ring only.

░ Represents Internetwork Analyzer (WAN/Synchronous) only.

*Ethernet only.

† FDDI only.

APPENDIX B: TROUBLESHOOTING GUIDE B

Appendix B. Troubleshooting Guide

This appendix lists some common problems and solutions. When you suspect a problem with the Sniffer analyzer, please look through this checklist before contacting NGC. Correcting a simple oversight could save you lots of time.

If the suggestions in this chapter do not solve your problem, Technical Support personnel can be reached from 6 a.m.. to 6 p.m. Pacific time, weekdays.

Before you call, please note the unit and network interface card serial numbers located on the initialization screen of the Sniffer analyzer. Also, please have the following information immediately available:

- A record of any error messages exactly, word for word.
- An accurate description of all symptoms of any problem and, if possible, a description of how to replicate the problem.
- An accurate, up-to-date map of your network that includes LANs as well as interconnecting devices.
- Information and analysis from a trace file should also be provided, if appropriate.

Phone for Network General's Technical Support Department:	(800) 395-3151
FAX	(415) 327-9436
Email Address	support@ngc.com

Troubleshooting Checklist

If	There is nothing on the screen	1. Check the power cable and power source. 2. Check the power switch. 3. Make sure the monitor's controls for brightness and contrast are set so the display is visible. 4. If you have a screen-saver program, press any key to redisplay the screen.

If	The Sniffer analyzer program does not start. (It should present in the main selection menu.)	Make sure there is no diskette in the floppy drive when you start the Sniffer analyzer. (This may produce the message **Non-system disk** or **disk error**.)

If	You cannot capture data from the network	1. Make sure that the capture submenu says **<from Ethernet>** (or **Token Ring**, as the case may be) instead of **<from *filename*>** 2. Check and disable any capture filters.
	...and you are using Ethernet	1. Check the connection from the DB-15 or BNC connector on the Sniffer analyzer's Ethernet adapter to the Ethernet cable. 2. Check the connection from the Ethernet cable to the transceiver. 3. Check the transceiver, using the instructions provided by its manufacturer. The transceiver may include a light indicating when it is receiving a signal (from the station to which it is connected; in this case the Sniffer analyzer). Try connecting a different station to the same transceiver or the Sniffer analyzer to a different transceiver. 4. On an IBM PS2 Model/70, check the **Internal transceiver** (BNC)/**External transceiver** (AUI) options. 5. Restart the Sniffer analyzer.
	...and you are using token ring	The message "lobe media test failed" probably means that the token ring cable is not attached. Make sure it is plugged into the DB-9 connector for token ring and not the DB-9 connector for video.
	...and you are using ARCNET	1. Check the connection from the BNC connector on the ARCNET adapter to the RG-62 cable from the ARCNET hub unit. 2. Check the network hub unit, using the instructions provided by its manufacturer. The hub may include a light indicating when it is receiving a signal (from the station to which it is connected, in this case the Sniffer analyzer). Try generating traffic from the Sniffer analyzer to see if the hub indicator light illuminates. 3. Check the DIP switch for the correct address (i.e, other than ARCNET stations on the net).
	...and you are using FDDI	If you are filtering on DLC addresses, check that your address options settings are set appropriately: Show LLC addresses or Show SMT addresses.

If	There is no output on the external color monitor	Check that the monitor is powered on and adjusted properly.
	...and you have a Model 30 or 50 Sniffer analyzer	Make sure you select **external color monitor** in the selection menu when you start the Sniffer analyzer.
	... and your Model 20 or 55 Sniffer analyzer has a token ring interface card	Make sure your monitor is attached to the DB-9 connector marked "Video" and not to the DB-9 connector marked "token ring."
	...and you have a Model 70 Sniffer analyzer	The analyzer detects the monitor automatically provided that the monitor is already connected when you turn the analyzer on. (On the series 700, there isn't a menu item for an external monitor.) When you attach a monitor: (a) Turn off the analyzer. (b) Connect the monitor to the analyzer's VGA port. (c) Turn the analyzer back on.

If	You don't see traffic that you expect	1. Check the station, protocol, and pattern-match capture filters to see whether traffic is being discarded. If the "frames seen" count is larger than the "frames accepted" count, then frames are being discarded.
	...and you are using token ring	1. Check that the ring speed is set correctly on the token ring NIC (16 or 4 Mbits/s). See the *Installation Guide* for more information. 2. Check that you are not the only station inserted on the ring. 3. If there are multiple MAUs, check that they are cabled together properly.
	..and you are using a WAN/Synchronous link	1. Check that the **Frame type** is set correctly in the **Options** menu. 2. Is **Frame type** set to **Router/Bridge**? If so, make sure that **Screen format** is set to **Skylines**. Otherwise, you will only see the DTE/DCE counters at the bottom of the screen. See page 3–13 for more information. 3. Check that **Encoding** is set correctly in the **Options** menu.

If	A pattern-match filter or trigger doesn't seem to work	1. Check the protocol and station-address filters; they may be causing the frames of interest to be discarded. 2. Double check the offset; detection of a pattern depends on telling the Sniffer network analyzer both what to look for and where to look. 3. Check to make sure the **AND/OR** options are set correctly.
	...and you are looking at frames sent on token ring	Check the offset origin: is it *frame-relative* (starting with the first frame byte) or *data-relative* (starting with the first LLC byte)?

If	You get the message "No frames eligible for display"	1. Check the address level display filter, or 2. Check the destination class display filter, or 3. Check the station address display filter, or 4. Check the protocol display filter, or 5. Check the pattern-match display filter. 6. Make sure that the display and capture filters are not mutually exclusive. 7. Use the **Use defaults** option and then redisplay the captured data.

If	You do not see frames that you expect	1. Check the display filters. 2. Check the capture filters, since they may have caused the frames to be discarded

If	Traffic counts during capture show implausible numbers	1. Check that you have selected the appropriate units (frames or kilobytes) in the Capture menu.

If	A "from" or "to" filter isn't working	1. Check the setting of the **Reverse direction** option in the filter menu. 2. Check the settings of other filters involved in capture or display; what you see displayed is what passes through all the filters. 3. Check that an earlier address filter doesn't already accept or discard the frames in question. Recall that filters are examined in sequence.

If	Network utilization seems too low	1. Check the display filters. Remember that only displayed frames are used in the network utilization calculation. Sometimes lower-level protocols that are not displayed carry much of the actual data. 2. Determine whether the frame sizes seem reasonable. The utilization might indeed be correct!

If	You are not seeing symbolic station names	1. Check the **Address level** filters to include addressing at the level you want. 2. Use **Manage names** to examine and add to the names list. 3. Remember to use the **Save names** option to make a permanent change to the name table. 4. Make sure the file STARTUP.*xx*D is in the analyzer's current directory (normally, \CAPTURE). 5. On FDDI networks, check **Options** for proper address selection: Show SMT addresses or Show LLC addresses.

If	HELP information is not available	1. Make sure the file *xx*SNIFF.HLP index file is in the *xx*SNIFF directory. 2. Make sure the various help files are in a subdirectory called HELP within *xx*SNIFF.HLP.

If	You are not getting any print output	1. Check the printer (power, switch settings, and so on). 2. Check that you have selected **LPT1** or **LPT2** (as appropriate) rather than **file** for the printer destination. 3. For serial printers, make sure that the transmit and receive pins are wired correctly. For some printers you may need a **null modem** cable. 4. For serial printers, make sure that you have issued the appropriate MODE command to set the baud rate, word size, parity, and so on. 5. Check the cable to the printer. For serial printers, make sure you are connecting to the appropriate port. The printer cable needs a DB-9 female connector for the Model 20, 30, 50, and 55. The Model 30 has two serial ports, so be sure you have made the appropriate connections.

If	You are not getting all the print output you expect	1. Check the **From frame** and **To frame** options in the **Print** menu. Do you have **Frame *nnn*** selected instead of **First frame** or **Last frame**? 2. Check the display filters; they affect what is printed. Remember that to print the entire detail report you must select all protocol levels and enable the **All layers** option.

If	You cannot save the capture buffer to a file because your hard disk is full	1. In the **Save data** dialog box, rewrite the path of the target file so that it starts with the drive A:\ or B:\, and write the file to a floppy disk. 2. Move to **Delete files** and delete an unwanted file. Then return to **Save data** and repeat your request.

If	You have found a problem with the Sniffer Network Analyzer software	1. After saving a trace file and the setups to a floppy diskette, try to recreate the problem. Then: • Start the Sniffer analyzer. • Load the trace file. • Load the setups. • Recreate the problem. If it is a display error, "print" the relevant part of the display to a diskette file. If you can reconstruct the problem in this manner, please send the diskette to the Network General Corporation Technical Support Department. Be sure to include your system serial number and the software version number (displayed in the initialization screen).

If	You have found a problem with the FDDI Sniffer Network Analyzer	1. Check the LED status indicator light on the FDDI adapter board. The LED indicators are: Green: an active connection. Amber: the adapter board is attempting a connection. The adapter board at the other end of the cable is not active, or the cabling is not correct. Red: the board has been enabled and is not attempting a connection.

APPENDIX C: GLOSSARY OF TERMS

C

Appendix C. Glossary of Terms

1BASE5
The implementation of the IEEE 802.3 (StarLAN) standard using 1 megabit per second transmission on a baseband medium whose maximum segment length is 500 meters.

10BASE2
The implementation of the IEEE 802.3 (Ethernet) standard using 10 megabit per second transmission on a baseband medium whose maximum segment length is 185 meters.

10BASE5
The implementation of the IEEE 802.3 (Ethernet) standard using 10 megabit per second transmission on a baseband medium whose maximum segment length is 500 meters.

10BASE-T
The implementation of the IEEE 802.3 (Ethernet) standard using 10 megabit per second transmission on a baseband medium. The standard provides a means for attaching AUI-compatible devices to 24 gauge, unshielded twisted pair cable, instead of the usual coaxial media.

3Com 3+
A networking system from 3Com Corporation using parts of the XNS and Microsoft/IBM PC LAN program protocols.

3Plus
3Com's implementation of XNS. Interpreted by the XNS PI suite.

802.2
The IEEE standards designation for the LLC sublayer protocol that provides both datagram and reliable connection transmission.

802.3
The IEEE standards designation for the CSMA/CD network access method. Similar to (and often used interchangeably with) Ethernet.

802.4
The IEEE standards designation for token bus networks. Used primarily with MAP protocols.

802.5
The IEEE standards designation for the token ring network access method.

AARP
AppleTalk Address Resolution Protocol. For outgoing packets, supplies the hardware destination address corresponding to a higher-level protocol address, and filters incoming packets to pass only those that are broadcast or specifically addressed to it. Interpreted in the AppleTalk PI suite.

AC
Access control. A DLC byte on IEEE 802.5 token ring networks that contains the token indicator and frame priority information.

ACSE
Association Control Service Element. An ISO application-level protocol interpreted in the ISO PI suite.

ACTPU
Activate Physical Unit. An SNA message sent to start a session.

ACK
Acknowledge. A network packet acknowledging the receipt of data.

active monitor
A computer on a token ring that acts as the controller for the ring, regulating the token and other performance aspects.

ACT
Absolute Congestion Threshold. Frame Relay term.

ADSP
AppleTalk Data Stream Protocol. A connection-oriented protocol providing a reliable, full-duplex, byte-stream service between any two sockets on an AppleTalk internet. Interpreted in the AppleTalk PI suite.

advertising
The process by which a service makes its presence known on the network. Typically provided through some sort of LAN-based multicast.

AEP
AppleTalk Echo Protocol. See Echo.

AFP
AppleTalk Filing Protocol. A presentation-level protocol for access to remote files. Interpreted in the AppleTalk PI suite.

ALAP
AppleTalk Link Access Protocol. See LAP.

alarm
Network statistics sent from a DSS Server to a connected Console over a LAN or WAN. Triggered by the monitor or analyzer application on the Server when network statistics exceed certain thresholds. Consists of the name of an offender, a timestamp, and an alarm priority threshold.

alert
Notification of an alarm condition. Sent from a DSS Server to non-connected unit such as a pager or a Console. Consists of a numeric identifier and a numeric value of the alarm threshold.

API
Application Program Interface. The specification of functions and data used by one program module to access another; the programming interface that corresponds to the boundary between protocol layers.

APPC
Advanced Program-to-Program Communications. A communications system used to communicate between transaction programs on IBM computers; APPC uses the LU 6.2 subset of SNA.

architecture
The architecture of a system refers to how the system is designed and how the components of the system are connected to, and operate with each other.

ARCNET
A baseband token-passing network originally designed by the Datapoint Corporation that communicates among up to 255 stations at 2.5 Mbps.

ARP
Address Resolution Protocol.
(1) A protocol within TCP/IP for finding a node's DLC addresses from its IP address. Interpreted in the TCP/IP PI suite.
(2) Interpreted in the Banyan VINES PI suite.

ASCII
American Standard Code for Information Interchange. A mapping between numeric codes and graphical characters used almost universally for all personal computer and non-IBM mainframe applications.

ASN.1
Abstract Syntax Notation One. A set of conventions governing the ISO presentation layer. Interpreted in the ISO PI suite.

ASP

AppleTalk Session Protocol. A general protocol, built upon ATP, providing session establishment, maintenance, and tear-down, along with request sequencing. Interpreted in the AppleTalk PI suite.

asynchronous

A method of data transmission which allows characters to be sent at irregular intervals by preceding each character with a start bit and following it with a stop bit. Commonly used to communicate with modems and printers.

ATP

AppleTalk Transaction Protocol. Provides a loss-free transaction service between sockets, allowing exchanges between two socket clients in which one client requests the other to perform a particular task and report the result. Interpreted in the AppleTalk PI suite.

AUI

Attachment Unit Interface. Drop cable for Ethernet between station and transceiver.

backbone

The backbone is the part of the communications network which carries the heaviest traffic. It is one basis for design of the overall network service.

background services

A protocol transmitted by a Matchmaker frame in Banyan VINES.

background task

A secondary job performed while the user is performing a primary task. For example, many network servers will carry out the duties of the network (controlling communications) in the background while at the same time the users are running their own applications (such as word processors).

bandwidth

The amount of data that can be moved through a particular communications link. For example, Ethernet has a bandwidth of 10Mbits/s.

baseband

A transmission technique that sends data bits without using a much higher carrier frequency (contrast with broadband). The entire bandwidth of the transmission medium is used by one signal.

baud rate

A measure of signaling speed in data communications. Specifies the number of signal elements that can be transmitted each second. For most purposes, at slow speeds, a baud rate is the same as the speed in bits per second.

BCC

Block Check Character. Another word for Frame Check Sequence.

beacon

A token ring packet that signals a serious failure on the ring.

BECN

Backward Explicit Congestion Notification. The sixth bit in the second octet of the frame relay header. Used to inform a subscriber device of congestion in the backward direction.

BER

Bit error rate. The percentage of received bits in error compared to the total amount of bits received. Usually expressed exponentially.

BERT

Bit error rate test. Test used to ascertain the bit error rate on a given wide-area link.

BIND

An SNA message sent to activate a session between LUs.

bipolar
The predominant signaling method used for digital transmission services, such as DDS and T1.

BIS
Bracket Initiation Stopped. An SNA message sent to indicate that the sending station will not attempt to initiate any more brackets.

BNC
A standardized coaxial cable connector; used for Thin Ethernet ("Cheapernet") cables and ARCNET networks.

BOOTP
Boot Protocol. A protocol within TCP/IP that is used for downloading initial programs into networked stations. Interpreted in the TCP/IP PI suite.

breakout box
A test device used to view the signals in an RS-232, V.35, or other interface. The breakout box is used to diagnose problems with the interface.

bridge
A device used to connect two separate networks into one extended network. Bridges only forward packets between networks that are destined for the other network.

broadband
A transmission technique that sends data bits encoded within a much higher radio-frequency carrier signal. The transmission medium may be shared by many simultaneous signals since each one only uses part of the available bandwidth.

broadcast
(1) A message directed to all stations on a network or collection of networks.
(2) A destination address that designates all stations.

buffer
A software program, storage space in RAM, or a separate device used to store data. For example, the Sniffer Network Analyzer's capture buffer serves as a temporary storage space for captured network data until it can be saved to disk.

bursty traffic
Data communications term referring to an uneven pattern of data transmission.

capture
The process in which the Sniffer analyzer records network traffic for interpretation. Generally speaking, this interpretation takes place during **display**. However, the Expert Sniffer analyzer simultaneously captures and interprets network traffic.

CCITT
International Consultative Committee for Telephony and Telegraphy. CCITT is a member of the International Telecommunications Union (ITU) that is, in turn, a specialized body within the United Nations. It sponsors a number of standards dealing with data communications networks, telephone switching standards, digital systems, and terminals.

CGA
Color Graphics Adapter. The interface between a personal computer and a medium-resolution color monitor.

chat script
A group of three chat strings (Setup, Listen, and Disconnect) that control communication parameters for an asynchronous device.

chat string
A UNIX-style command/response sequence of characters which are downloaded to a serial device in order to control the device.

CIR

Committed Information Rate. The largest number of bits per second that a frame relay network agrees to carry for a PVC. CIR is assigned at the time of subscription to the frame relay service.

client

1. A module that uses the services of another module. The session layer is a client of the transport layer, for example.

2. A PC or workstation that accesses services or applications from another "server" PC or workstation.

CLLM

Consolidated Link Layer Management. An access signaling protocol specified by ANSI for frame relay links.

CLNS

Connectionless Network Service Protocol (also called ISO IP). Interpreted in the ISO PI suite.

CMIP

Common Management Information and Services Protocol. When used with TCP/IP, it is also known as CMOT.

CMOT

Common Management Information and Services Protocol Over TCP. A management protocol for networks; it uses ASN.1 encoding. Interpreted in the TCP/IP and ISO PIs.

compression

Reducing the bandwidth or bits necessary to encode information.

concentrator

A central point for connecting many individual stations to a network ring. Found most often on FDDI networks.

Courier

A presentation-level protocol in XNS (similar to RPC in the Sun protocol family); it delivers data to such application-level protocols as XNS Printing, XNS Filing, or XNS Clearinghouse.

CRC

Cyclic Redundancy Check. A check-word, typically two or four bytes at the end of a frame, used to detect errors in the data portion of the frame.

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance. A *random access* or *contention-based* control technique; the algorithm used in LocalTalk networks to control transmission.

CSMA/CD

Carrier Sense Multiple Access with Collision Detection. A *random access* or *contention-based* control technique; the algorithm used by IEEE 802.3 and Ethernet networks to control transmission.

CTERM

Command Terminal. A protocol within DECnet for communicating with generic intelligent terminals, that is, a virtual terminal protocol. Interpreted in the DECnet PI suite.

DAC

Dual Attachment Concentrator. A concentrator that offers two connections to the FDDI network capable of accommodating the FDDI dual ring, and additional ports for connection of other concentrators or FDDI stations.

DAP

Data Access Protocol. The DECnet protocol that provides remote file access. Interpreted in the DECnet PI suite.

DAS

Dual Attachment Station. An FDDI station that offers two connections to the FDDI dual counter-rotating ring.

DB-9

A 9-pin standardized connector used in personal computers for a token ring network connection (female), serial I/O port (male), and RGBI output. Also used for LocalTalk.

DB-15

A 15-pin standardized connector used at the transceiver, the drop cable, and the station of IEEE 802.3 or Ethernet network components.

DB-25

A 25-pin standardized connector used in personal computers for parallel output ports (female connector on IBM PC chassis) or for serial I/O ports (male connector on IBM PC chassis).

DCE

Data Circuit-terminating Equipment (also called Data Communications Equipment). On a serial communications link, the device that connects the DTEs into the communication line or channel.

DDP

Datagram Delivery Protocol. Extends the services of the underlying LAP protocol to include an internet of interconnected AppleTalk networks, with provision to address packets to sockets within a node. Interpreted in the AppleTalk PI suite.

DE Bit

Discard Eligibility Bit. The seventh bit of the second octet of the frame relay header. A value of 1 in the DE bit indicates that the frame is eligible for discard by a congested network.

destination address

That part of a message which indicates for whom the message is intended. Usually a collection of characters or bits. Just like putting a destination address on an envelope.

DFC

Data Flow Control. An SNA subprocess for reliable message transfer.

diagnosis

A problem on the network detected by the Expert Sniffer analyzer. The Expert Sniffer analyzer detects and alerts users to diagnoses as it discovers them on the network to which it is attached.

DIP switch

Dual In-Line Package. A small switch usually attached to a printed circuit board. Usually requires a small screwdriver to change. There are only two settings– on or off. Printed circuit boards usually have "banks" of multiple DIP switches used to configure the board in a semi-permanent way.

DIS

Draft International Standard. One of the stages in defining ISO protocols. Final stage is IS.

DISC

Disconnect. An LLC non-data frame indicating that the connection established by an earlier SABM or SABME is to be broken.

display

The process in which the Sniffer analyzer interprets the traffic recorded during capture. During display, the analyzer decodes the various layers of protocol in the recorded frames and displays them as English abbreviations or summaries.

DIX

DEC/Intel/Xerox. Used to refer to an early version of Ethernet.

DLC

Data Link Control. The lowest protocol level within the transmitted network frame; fields typically include the Destination address, and Source address, and perhaps other control information.

DLCI

Data Link Connection Identifier. 10-bit number used by the Frame Relay protocol to identify a virtual circuit.

DLL

1. Downline load. A protocol within the Datapoint RMS family used for downloading initial programs into networked stations.

2. Dynamic Link Library. A type of program library used in MS-Windows.

DM

Disconnected Mode. An LLC message acknowledging that a previously established connection has been broken.

DNS

Domain Name Service. A protocol within TCP/IP for finding out information about resources using a database distributed among different name servers. Interpreted in the TCP/IP PI suite.

DOS

Disk Operating System. The most common operating system for IBM-compatible personal computers.

DRP

DECnet Routing Protocol. The lowest-level DECnet protocol, concerned with moving packets from endnodes through routers to other endnodes. ("Routing" in DNA terminology corresponds to the ISO model's "Network" layer).

DSAP

Destination Service Access Point. The LLC SAP for the protocol expected to be used by the destination station in decoding the frame data.

DTE

Data Terminal Equipment. On a serial communications link, a generic term used to describe the host or end-user machine.

duplex

Characteristic of data transmission. Either full or half duplex. Full permits simultaneous two-way communication. Half means only one side can talk at a time.

E1

A digital transmission link with a capacity of 2.048 Mbps (CCITT version of T1).

EBCDIC

Extended Binary-Coded-Decimal Interchange Code. A mapping between numeric codes and graphical characters used for IBM mainframe computers and communications protocols defined by IBM.

Echo

(1) A request/response protocol within XNS used to verify the existence of a host.
(2) A protocol within AppleTalk that allows any node to send a datagram to any other node and to receive an echoed copy of that packet in return to verify the existence of that node or to make round trip delay measurements. Interpreted in the AppleTalk PI suite.
(3) A protocol transmitted by a Matchmaker frame in Banyan VINES.

EGP

Exterior Gateway Protocol. A protocol within TCP/IP used to exchange routing information among gateways belonging to the same or different systems. A generalization of GGP.

EIA

Electronic Industries Association. A standard organization specializing in the electrical and functional characteristics of interface equipment.

ELAP
See LAP.

EPROM
Erasable Programmable Read Only Memory. A read-only memory device which can be erased and reprogrammed. EPROMs do not lose their memory when power is shut off.

Error
A protocol within XNS by which a station reports that it has received (and is discarding) a defective packet. Interpreted in the XNS PI suite.

error rate
In data transmission, the ratio of the number of incorrect elements transmitted to the total number of elements transmitted.

ES-IS Routing
End-System to Intermediate-System Routing. A protocol within the ISO family used to exchange routing information between gateways and hosts. Interpreted in the ISO PI suite.

Ethernet
A CSMA/CD network standard originally developed by Xerox; similar to (and often used interchangeably with) the IEEE 802.3 standard.

Ethertype
A 2-byte protocol-type code in Ethernet frames used by several manufacturers but independent of the IEEE 802.3 standard.

FC
Frame control. On a token ring network, the DLC byte that contains the frame's type.

FCS
Frame check sequence. A redundant check field used to increase the probability of error-free transmission on the network.

FDDI
Fiber Distributed Data Interface. ANSI/ISO standards that defines a 100Mb/s LAN over a fiber-optic media using a timed token over a dual ring of trees.

FECN
Forward Explicit Congestion Notification. The fifth bit in the second octet of the frame relay header. Used to inform a subscriber device of congestion in the forward direction.

FEP
Front-End Processor. The "traffic cop" of the data communications world. Typically sits in front of a computer and is designed to handle the telecommunications burden so the computer can concentrate on handling the processing burden.

FID
Format Identification. A field in the SNA Transmission header indicating the type of nodes participating in the conversation. LU 6.2 nodes are type 2.

filter
The Sniffer analyzer uses several varieties of filters, including the following. (1) **Capture filters**. These filters determine which arriving frames the analyzer discards and which it retains. (2) **Display filters**. These filters determine which frames in the capture buffer will be displayed. Eliminating a frame from display with a display filter does not remove the frame from memory. Rather, it simply removes the frame from display.

flow control
Hardware or software mechanisms used in data communications to turn off transmission when the receiving workstation is unable to store the data it is receiving. Various methods of regulating the flow of data during a conversation. Buffers are an example of flow control.

FMD
Function Management Data. A class of data embedded at the start of SNA RUs.

FMH
Function Management Header. The header part of SNA FMD containing addressing and transmission control information.

FOUND
Foundation Services. A protocol within DECnet used for primitive terminal-handling services. Interpreted in the DECnet PI suite.

frame
The multi-byte unit of data transmitted at one time by a station on the network; synonymous with Packet.

frame check sequence (FCS)
In bit-oriented protocols, a 16-bit field added to the end of a frame that contains transmission error-checking information.

Frame Relay
A streamlined access protocol commonly used for LAN interconnectivity.

FRMR
Frame Reject. An LLC command or response indicating that a previous frame had a bad format and is being rejected. The REJ frame contains five bytes of data explaining why and how the previous frame was bad.

Front-End Processor
See "FEP."

FRP
Fragmentation Protocol. Breaks up and reassembles network-layer packets so that they are acceptable to the data-link protocol and the underlying physical medium; used on networks whose physical medium is ARCNET. Interpreted in the Banyan VINES PI suites.

FS
Frame status. A byte appended to a token ring network frame following the CRC. It contains the Address Recognized and Frame Copied bits.

FTAM
File Transfer, Access and Management. An application-level protocol within the ISO suite, on top of ACSE.

FTP
File Transfer Protocol.
(1) A protocol based on TCP/IP for reliable file transfer. Interpreted in the TCP/IP PI suite.
(2) A protocol transmitted by a Matchmaker frame in Banyan VINES.

functional address
A limited broadcast destination address for IEEE 802.5 token ring networks. Individual bits in the address specify attributes that stations eligible to receive the frame should have. Similar to "multicast address."

gateway
In the general sense, a gateway is a computer that connects two different networks together. Usually, this means two different kinds of networks, such as SNA and DECnet. In TCP/IP terminology, however, a gateway connects two separately administered subnetworks, which may or may not be running the same networking protocols.

GGP

Gateway-to-gateway protocol. A protocol within TCP/IP used to exchange routing information between IP gateways and hosts. Interpreted in the TCP/IP PI suite. See also EGP.

GUI

Graphical User Interface, pronounced "gooey". An operating system or environment that displays options on the screen as icons, or picture symbols.

handshaking

The electrical exchange of predetermined signals when a connection is made between two devices carrying data. Just as people shake hands when they meet, computers must go through a procedure of "greeting" the opposite party and preparing for communications.

HDLC

High-level Data Link Control. A standard bit-oriented protocol developed by the International Standards Organization (ISO). In HDLC, control information is always placed in the same position. Specific bit patterns used for control differ dramatically from those used to represent data, minimizing errors. Many internetworking companies (such as Cisco and Vitalink) have developed proprietary versions of HDLC, which the Sniffer Internetwork Analyzer can decode.

header

The beginning portion of a message which contains destination address, source address, message-numbering, and other information. The header helps direct the message along its journey. Different protocols implement headers in different ways.

hop

A term used in routing. A hop is one data link. A path to the final destination on a net is a series of hops away from the origin. Each hop has a cost associated with it, allowing the calculation of a least cost path.

hub

A concentrator and repeater for the network. Generally speaking, a hub is a central point for wiring or computing in a network. For StarLAN, it is more properly known as a Network Hub Unit or as a Network Extension Unit.

I

Information. An LLC, HDLC, or SDLC frame type used to send sequenced data that must be acknowledged.

ICMP

Internet Control Message Protocol. A protocol within TCP/IP used principally to report errors in datagram transmission. Interpreted in the TCP/IP PI suite.

ICP

Internet Control Protocol. Used to broadcast notification of errors and to note changes in network topology in Banyan VINES. Interpreted in XNS PI suite.

IDP

Internet Datagram Protocol. Delivers to an internet address a single frame as an independent entity, without regard to other packets or to the addressee's response.

IEEE

Institute of Electrical and Electronics Engineers, Inc. Standards documents are available from them at 345 East 47th Street, New York, NY 10017.

IGRP

Interior Gateway Routing Protocol. Cisco routing protocol designed for campus-wide use, as opposed to wide-area use.

IONET

Input/Output Network. A device message protocol used by Datapoint.

IP

Internet Protocol. The lowest-level protocol under TCP/IP that is responsible for end-to-end forwarding and long packet fragmentation control. Interpreted in the TCP/IP PI suite. A similar protocol is interpreted in the Banyan VINES PI. See also the IPX and ISO IP protocols.

IPC

Interprocess Communication Protocol. A transport-level protocol in Banyan VINES, providing reliable message service and unreliable datagram service. Interpreted in the Banyan VINES PI suite.

IPX

Internet Protocol. Novell's implementation of Xerox Internet Datagram Protocol. Interpreted in the Novell NetWare PI suite.

IS

1. International Standard. The final phase for an ISO protocol definition. At this point, the protocol is fully specified and guaranteed not to change.

2. Intermediate System. An OSI term for a system that originates and terminates traffic, and that also forwards traffic to other systems.

ISDN

Integrated Services Digital Network. A digital telephone technology that combines voice and data services on a single circuit. Source of many ideas for frame relay networking.

ISO

International Organization for Standardization (or International Standards Organization).
(1) A consortium that is establishing a suite of networking protocols;
(2) The protocols standardized by that group.

ISODE

ISO Development Environment. Protocol for transmitting higher-level ISO protocols over a network whose lower levels are handled by TCP/IP. Interpreted in the TCP/IP and ISO PI suites.

ISO IP

The ISO standard Internet Protocol. Interpreted in the ISO PI suite.

KSP

Kiewit Stream Protocol. A transport protocol resembling TCP developed at Dartmouth College for the support of terminal emulators connected to AppleTalk networks; interpreted in the AppleTalk PI suite.

LAN

Local Area Network. The hardware and software used to connect computers together in a limited geographical area.

LAP

Link Access Protocol. The logical level protocol for AppleTalk. It exists in two variants: ELAP (for Ethernet) and LLAP (for LocalTalk networks). Interpreted in the AppleTalk PI.

LAPB

Link Access Protocol, Balanced. A subset of HDLC.

LAST

Local Area System Transport. Protocol for remote booting in DECnet/DOS.

LAVC

Local Area Vax Cluster. An adaptation of the System Communication Architecture (SCA) to run over the Ethernet instead of a CI bus. Used to enable MicroVAXs to operate as diskless nodes.

LLAP

See LAP.

LAT

Local Area Transport. The DECnet protocol that handles multiplexed terminal (keyboard and screen) traffic to and from timesharing hosts. Interpreted in the DECnet PI suite.

leased line

Same as a leased circuit, dedicated circuit, or leased channel. A telephone line rented for exclusive continuous use. Commonly used to connect LANs remote from one another.

link protocol

The set of rules by which a logical data link is set up and by which data transfers across the link. Includes formatting of the data.

LLC

Logical Link Control. A protocol that provides connection control and multiplexing to subsequent embedded protocols; standardized as IEEE 802.2 and ISO/DIS 8802/2.

LMI

Local Management Interface. An access signaling protocol defined for Frame Relay circuits. LMI carries information on the status of PVCs between the network and a subscriber device. Optional additions to LMI include multicasting, global addressing, and flow control.

LOOP

Loopback protocol. A protocol under Ethernet for sending diagnostic probe messages.

LSA

Lost Subarea. An SNA error condition.

LU 6.2

Logical Unit 6.2. A subset of the SNA protocols used for peer-to-peer communications between computers.

LUSTAT

Logical Unit Status. An SNA message used to send status information.

MAC

Medium Access Control. The protocol level that describes network management frames sent on the 802.5 token ring. Most MAC frames are handled transparently by the network adapter.

Mail Service

Protocol used (in conjunction with StreetTalk) for the transmission of messages in the VINES distributed electronic mail system. Interpreted in the Banyan VINES PI suite.

Manchester encoding

A data encoding technique that uses a transition at the middle of each bit period that serves as a clock and also as data.

MAP

Manufacturing Automation Protocol. A multilayer networking protocol developed primarily by General Motors for manufacturing control applications.

Matchmaker

Protocol used by the VINES service that provides high-level program-to-program communication, including translation as necessary to match the conventions of sender's and receiver's formats. Matchmaker is descended from XNS Courier. Interpreted in the Banyan VINES PI suite.

MAU

Multiple Access Unit (also Medium Attachment Unit). The wiring concentrator or transceiver used for attaching stations connected to the network.

MIB

Management Information Data Base. The structured database of network statistical information used by the SNMP and CMIP protocols.

MIC

Media Interface Connector. An optical fiber connector pair that links the fiber media to the FDDI node or another cable.

modem

A contraction of modulate and demodulate; a conversion device installed in pairs at each end of an analog communications line. The modulator part of the modem codes digital information onto an analog signal by varying the frequency of the carrier signal. The demodulator part extracts digital information from a modulated carrier signal.

MOP

Maintenance Operations Protocol. A protocol under DECnet for remote testing and problem diagnosis. Interpreted in the DECnet PI suite.

MOUNT

A protocol developed by Sun Microsystems that provides request access checking and user validation. It is used in conjunction with NFS. Interpreted in the Sun PI suite.

multicast

(1) A message directed to a group of stations on a network or collection of networks (contrast with broadcast).
(2) A destination address that designates such a subset.

multiplexing

Sending several signals over a single line and separating them at the other end.

N(R)

Receive sequence number. An LLC or HDLC field for I frames that indicates the sequence number of the next frame expected; all frames before N(R) are thus implicitly acknowledged.

N(S)

Send sequence number. An LLC or HDLC field for I frames that indicates the sequence number of the current frame within the connection.

NBP

(1) Name-Binding Protocol. Used in AppleTalk networks to permit network users to use character names for network services and sockets. NBP translates a character-string name within a zone into the corresponding socket address. Interpreted in the AppleTalk PI suite.
(2) NetBIOS Protocol. Used in 3Com 3+ Open software. Interpreted in the XNS PI suite.

NC

Network Control. An SNA subprocess.

NCP

NetWare Core Protocol. Novell's application-level protocol for the exchange of commands and data between file servers and workstations. Interpreted in the Novell NetWare PI suite.

ND

Network Disk. A protocol within the Sun NFS family used to access virtual disks located remotely across the network. Interpreted in the TCP/IP PI suite.

NetBIOS

Network Basic I/O System.
(1) A protocol implemented by the PC LAN Program to support symbolically named stations and the exchange of arbitrary data.
(2) The programming interface (API) used to send and receive NetBIOS messages.
There exist several different and incompatible implementations of NetBIOS, and separate PIs for them, as, for example, in the IBM and the TCP/IP PI suites.

NETBLT

Network Block Transfer. A protocol within earlier versions of TCP/IP. Not interpreted in the TCP/IP PI suite.

NetWare

The networking system designed by Novell Inc. and the protocols used therein.

Network Management

1. A general term describing the protocols and applications used to manage networks.

2. A protocol transmitted by a Matchmaker frame in Banyan VINES.

network object

The Expert Sniffer analyzer creates network objects by performing multilevel protocol analysis on the frames that pass through its real-time protocol interpreters. In this way, the Expert analyzer can distill a relatively small number of network objects from the huge body of information it processes. Network objects can be any of the following: a DLC station, a network station, a connection, an application, or a subnetwork.

network topology

The geography of a network. Examples of network geographies include ring, bus, and star.

NEU

Network Extension Unit. A concentrator and repeater for StarLAN networks.

NFS

Network File System. A protocol developed by Sun Microsystems for requests and responses to a networked file server. Interpreted in the Sun PI suite.

NGCP

Network General Control Protocol. Network General Corporation protocol used for communications between Distributed Sniffer System consoles and servers.

NHU

Network Hub Unit. A concentrator and repeater for StarLAN networks.

NICE

Network Information and Control Exchange. The DECnet protocol for network management. Interpreted in the DECnet PI suite.

NIF

Neighbor Information Frame. Used by stations on an FDDI ring to announce their addresses to downstream neighbors.

NIS

Network Information Services. Previously known as "Yellow Pages." A set of services in the Network File System that propagate information from masters to recipients. Used for the maintenance of system files on complex networks.

nodes

Points in a network where service is provided, service is used, or communications channels are interconnected. "Node" is sometimes used interchangeably with "workstation."

NRZ

Non-return to Zero.

NRZI

Non-return to Zero Inverted. A binary encoding scheme that inverts the signal on a "one" and leaves the signal unchanged for a "zero." The Sniffer Internetwork Analyzer can interpret both NRZ and NRZI, but you must set the correct option in the **Options** menu.

NSP

Network Services Protocol. The DECnet protocol that provides reliable message transmission over virtual circuits. Interpreted in the DECnet PI suite.

null modem

A cross-pinned cable used for DTE to DTE communications. Sometimes called a modem eliminator.

octet

A string of eight bits. Synonymous with Byte.

OpenNET

A networking system from the Intel Corporation that uses parts of the OSI standards and components of the Microsoft/IBM PC LAN program. Interpreted in the ISO PI suite.

OSI

Open Systems Interconnection. A generalized model of a layered architecture for the interconnection of systems.

overhead

In data communications, all information found on the network at a given time. Includes control, routing, and error-checking characters, in addition to user-transmitted data.

packet

The multi-byte unit of data transmitted at one time by a station on the network. Synonymous with Frame.

packet switching

A method for sending data in packets through a network to some remote location. The data to be sent is subdivided into individual packets of data, each having a unique identification and carrying its destination address. This way, each packet can go by a different route, possibly arriving in a different order than it was shipped. The packet ID allows the data to be reassembled in proper sequence.

PAD

Packet Assembler Disassembler. Special purpose computer on an X.25 network that allows asynchronous terminals to use the synchronous X.25 network by packaging asynchronous traffic into a packet.

PAP

Printer Access Protocol. A protocol within AppleTalk that uses ATP XO commands to create a stream-like service for communication between user stations and the Apple LaserWriter or similar stream-based devices. Interpreted in the AppleTalk PI suite.

parallel interface An interface which permits parallel transmission, or simultaneous transmission of the bits making up a character or byte, either over separate channels or on different carrier frequencies of the same channel.

parity A process for detecting whether bits of data have been altered during transmission of that data.

parity bit A binary bit appended to an array of bits to make the sum of the bits always odd or always even. Used with a parity check for detecting errors in transmitted binary data.

patch panel A device in which temporary connections can be made between incoming and outgoing lines. Used for modifying or reconfiguring a communications system or for connecting test instruments (such as the Sniffer Network Analyzer) to specific lines.

PC*I Personal Computer Integration. Data General's nomenclature for their networking system. Protocols used include the ISO IP and TP4 levels and the Microsoft/IBM PC LAN program SMB protocols. Interpreted in the ISO PI suite.

PCF Physical Control Fields. The part of the token ring DLC header that includes the AC and FC fields.

PDU Protocol Data Unit. The data delivered as a single unit between peer processes on different computers.

PEP Packet Exchange Protocol. A protocol within the XNS family used to exchange datagrams. Interpreted in the XNS/MS-Net PI suite.

PI Protocol Interpreter. A program that knows the frame format and transaction rules of a communications protocol and can decode and display frame data.

PING A TCP/IP tool supplied with TCP/IP Distributed Sniffer System. PING is a diagnostic utility that sends ICMP Echo Request messages to a specific IP address on the network.

PMAP Port Mapper. A protocol developed by Sun Microsystems for mapping RPC program numbers to TCP/IP port numbers. Interpreted in the Sun PI suite.

port The physical access point to a computer, multiplexor, device, or network where signals may be sent or received.

preamble A fixed data pattern transmitted before each frame to allow receiver synchronization and recognition of the start of a frame.

protocol A specific set of rules, procedures, or conventions governing the format and timing of data transmission between two devices.

protocol interpreter The Sniffer analyzer uses its protocol interpreters to identify the protocols nested within each frame and interpret their contents.

PUP PARC Universal Packet. A type of Ethernet packet formerly used at the Xerox Corporation's Palo Alto Research Center. Interpreted in the XNS/MS-Net and the TCP/IP PIs but not included in their protocol diagrams since no longer in regular use.

PVC Permanent Virtual Circuit. A unique, predefined logical path between two endpoints of a network.

RAM Random Access Memory. A chip or collection of chips where data can be entered, read, and erased. RAM is the fastest memory device, but loses its memory when power is shut off.

RARP Reverse Address Resolution Protocol. A protocol within TCP/IP for finding a node's IP address given its DLC address. Interpreted in the TCP/IP PI suite.

RDP Reliable datagram protocol. A protocol within an earlier version of TCP/IP. Not interpreted in the TCP/IP PI suite.

REJ Reject. An LLC frame type that requests retransmission of previously sent frames.

REM Ring Error Monitor. A station on the 802.5 token ring network that collects MAC-level error messages from the other stations.

repeater A device inserted at intervals along a circuit to boost, amplify, and/or regenerate the signal being transmitted.

RFC Request For Comment. Designation used in DoD/TCP protocol research and development.

RG-58 The designation for 50-ohm coaxial cables used by Cheapernet (thin Ethernet).

RG-59 The designation for 75-ohm coaxial cables used by PC Network (broadband).

RG-62 The designation for 93-ohm coaxial cables used by ARCNET.

RGBI Red-Green-Blue-Intensity. An interface used for attaching a color monitor to a personal computer; DB-9 connectors are typically used.

RH Request/response header. An SNA control field prior to a Request Unit or Response unit.

RI Routing Information. A protocol at the logical link level for devices operating on the token ring. Interpreted by the token ring and Ethernet Distributed Sniffer™ System independent of other PIs.

RII Routing Information Indicator. If the first bit in the source address field of a token ring frame is 1, then the data field begins with Routing Information. Interpreted by the token ring and Ethernet Distributed Sniffer™ System independent of other PIs.

RIP Routing Information Protocol. A protocol within the XNS and TCP/IP families used to exchange routing information among gateways. Interpreted in the XNS PI suite and in the TCP/IP PI suite.

RJ-45

The designation for the 8-wire modular connectors used for StarLAN and 10BASE-T networks. It is similar to, but wider than, the standard (RJ-11) telephone modular connectors.

RMS

Resource Management System. A set of protocols used by Datapoint to communicate from client stations to servers.

RNR

Receive Not Ready. An LLC and HDLC command or response indicating that transmission is blocked.

router

(1) An internet linking device operating at network layer 3.
(2) A protocol transmitted by a Matchmaker frame in Banyan VINES.

RPC

Remote Procedure Call. A protocol for activating functions on a remote station and retrieving the result. Interpreted in the Sun PI suite. A similar protocol exists in Xerox XNS.

RPL

Remote Program Load. A protocol used by IBM on the IEEE 802.5 token ring network to download initial programs into networked stations. Interpreted in the IBM PI suite.

RPS

Ring Parameter Server. A station on a token ring network that maintains MAC-level information about the LAN configuration such as ring numbers and physical location identifiers.

RR

Receive ready. An LLC non-data frame indicating readiness to receive data from the other station.

RS-232C

Recommended Standard 232. EIA standard defining electrical characteristics of the signals in the cables that connect a DTE and a DCE.

RSTAT

Remote status. A protocol with the Sun NFS family used to exchange statistics on network activity. Interpreted in the Sun PI suite.

RTMP

Routing Maintenance Protocol. Used in AppleTalk networks to allow bridges or internet routers dynamically to discover routes to the various networks of an internet. A node that is not a bridge uses a subset of RTMP (the RTMP stub) to determine the number of the network to which it is connected and the node IDs of bridges on its network. Interpreted in the AppleTalk protocol interpreter.

RTP

Routing Update Protocol. Used to distribute network topology information. Interpreted in the Banyan VINES PI suite.

RU

Request Unit/Response unit. The part of an SNA frame after the RH that contains the details of a request or its response.

RUnix

Remote Unix. A protocol atop TCP/IP for issuing remote requests over the network to a UNIX host.

S

Supervisory. An LLC, HDLC, or SDLC frame type used for control functions.

SABM

Set Asynchronous Balanced Mode. An LLC non-data frame requesting the establishment of a connection over which numbered I frames may be sent.

SABME

Set Asynchronous Balanced Mode (Extended). SABM with two more bytes in the control field. Used in LAPB.

SAC

Single Attachment Concentrator. A concentrator that offers one S port for attachment to the FDDI network and M ports for the attachment of stations or other concentrators.

SAP

Service Access Point.
(1) A small number used by convention or established by a standards group, that defines the format of subsequent LLC data; a means of demultiplexing alternative protocols supported by LLC.
(2) Service Advertising Protocol. Used by NetWare servers to broadcast the names and locations of servers and to send a specific response to any station that queries it.

SAS

Single Attachment Station. An FDDI station that offers one S port for attachment to the FDDI ring.

SBI

Stop Bracket Initiation. An SNA message sent to request that the other station not initiate any more brackets.

SC

Session Control. An SNA subprocess for establishing and maintaining connections.

SCP

Session Control Protocol. The DECnet protocol concerned with the establishment of virtual circuits over which NSP transfers data; interpreted in the DECnet PI suite.

SCSI

Small Computer Standard Interface. Pronounced "scuzzy." A standard for connecting disk drives to disk controllers, used typically in small multiuser computers.

SDLC

Synchronous Data Link Control. An older serial communications protocol that was the model for LLC and with which it shares many features.

semaphore

A synchronization mechanism on an operating system.

serial interface

An interface which requires serial transmission, or the transfer of information in which the bits composing a character are sent sequentially. Implies only a single transmission channel.

SESSION

Name for the session-level protocol in the ISO series, interpreted in the ISO PI suite.

Sever

A protocol transmitted by a Matchmaker frame in Banyan VINES.

SIF

Status Information Frame. Used by stations on an FDDI ring to exchange information about station configuration and operating parameters.

SIG

Signal. A high-priority SNA message used to request permission to send.

SMB

Server Message Block. A message type used by the IBM PC LAN Program to make requests from a user station to a server and receive replies. Many of the functions are similar to those made by an application program to DOS or to OS/2 running on a single computer.

SMB is part of the protocol family that for DOS machines is called MS-NET and for OS/2 machines is called The LAN Manager. Under the IBM PC LAN Program, SMBs are sent as data within NetBIOS frames, but in other context may be transported differently. The OS/2 version of SMB contains extensions not present in the DOS version. Both versions are interpreted in the IBM, XNS, TCP/IP, ISO, DECnet, and Banyan VINES PI suites.

SMT

Station Management. Provides ring management, connection management, and SMT frame services for an FDDI ring.

SMTP

Simple Mail Transfer Protocol. A protocol within TCP/IP for reliable exchange of electronic mail messages. Interpreted in the TCP/IP PI suite.

SNA

Systems Network Architecture. A complex set of protocols used by IBM for network communications, particularly with mainframe computers. Interpreted in the IBM PI suite.

SNAP

Sub-Network Access Protocol (also sometimes called Sub-Network Access Convergence Protocol). An extension to IEEE 802.2 LLC that permits a station to have multiple network-layer protocols. The protocol specifies that DSAP and SSAP addresses must be AA hex. A field subsequent to SSAP identifies one specific protocol. Interpreted in the TCP/IP PI suite and the AppleTalk PI suite. (See RFC 1042 for further information on SNAP.)

SniffMaster Console

The Distributed Sniffer System™ (DSS) *client* that communicates with the DSS Sniffer Servers from any point on the network. The Console delivers instructions to the Server and reads the output of the Server's analysis. The Console is a computer that uses proprietary software and hardware. The proprietary hardware is a network interface card called a Transport Card for communicating over the network with Servers.

Sniffer Server

The Distributed Sniffer System (DSS) *server* that captures and analyzes packet level network data under instructions from the *client*, a DSS SniffMaster Console. The Server is a computer that uses proprietary software and hardware. The Sniffer Server's analysis applications are based on the Sniffer network analyzer and the Advanced Network Monitor. The Server uses two network interface cards: a Transport Card that supports communication with Consoles and a Monitor card that is used to capture frames and collect statistics from the network.

SNMP

Simple Network Management Protocol. Interpreted in the TCP/IP PI suite.

SNRM

Set Normal Response Mode. Place a secondary station in a mode that precludes it from sending unsolicited frames. The primary station controls all message flow. Used in SDLC.

SNRME

Set Normal Response Mode (Extended). SNRM with two more bytes in the control field. Used in SDLC.

socket

A logically addressable entity or service within a node, serving as a more precise identification of sender or recipient.

spanning tree

A method of creating a loop-free logical topology on an extended LAN. Formation of a spanning tree topology for transmission of messages across bridges is based on the industry-standard spanning tree algorithm defined in IEEE 802.1d.

SPP

Sequenced Packet Protocol. A virtual-circuit connection-oriented protocol in XNS.

SPP

Sequenced Packet Protocol.
(1) The XNS protocol that supports reliable connections using sequenced data; interpreted in the XNS PI suite. A variant called SPX is used in Novell NetWare.
(2) The transport-level protocol that provides virtual connection service in Banyan VINES, based upon the protocol of the same name in XNS. Interpreted in the Banyan VINES PI suite.

SPX

Sequential Packet Exchange. Novell's version of the Xerox protocol called SPP. Interpreted in the Novell NetWare PI suite.

SQE

Signal Quality Error. The 802.3/Ethernet collision signal from the transceiver.

SQE TEST

The SQE signal generated by the transceiver at the end of a transmitted frame to check the SQE circuitry. Also known as *heartbeat* in Ethernet.

SS7

Signaling System 7. Protocol related to ISDN. Directs how the interior of an ISDN network is managed.

SSAP

Source Service Access Point. The LLC SAP for the protocol used by the originating station.

SSCP

System Services Control Point. An SNA identification of communications management functions.

StarLAN

A network developed by AT&T Bell Labs and based upon a derivative of the CSMA/CD (Ethernet) network standard originally developed by Xerox; similar to (and often used interchangeably with) the IEEE 802.3 standard.

StreetTalk

Protocol used in Banyan VINES to maintain a distributed directory of the names of network resources. In VINES names are global across the internet and independent of the network topology. Interpreted in the Banyan VINES PI suite.

SUA

Stored Upstream Address. The network address of a token ring station's nearest upstream neighbor. Texas Instruments calls this the UNA (see Upstream Neighbor Address).

subnet
A term used to denote any networking technology that makes all nodes connected to it appear to be one hop away. In other words, the user of the subnet can communicate directly to all other nodes on the subnet. A collection of subnets together with a routing or network layer combine to form a network.

SVC
Switched Virtual Circuit. A virtual circuit that is set up on demand, as in the case of a dial-up telephone line, or an X.25 call.

symptom
An abnormal or unusual network event which the Expert analyzer.

T1
A digital transmission link with a capacity of 1.544 Mbits/sec.

Talk
A protocol transmitted by a Matchmaker frame in Banyan VINES.

TC
Transmission Control. An SNA subprocess.

TCP
Transmission Control Protocol. The connection-oriented byte-stream protocol within TCP/IP that provides reliable end-to-end communication by using sequenced data sent by IP. Interpreted in the TCP/IP PI suite.

TCP/IP
Transmission Control Protocol/Internet Protocol. A suite of networking protocols developed originally by the US Government for Arpanet and now used by several LAN manufacturers. The individual TCP/IP protocols are listed separately in this Glossary.

Telnet
Protocol for transmitting character-oriented terminal (keyboard and screen) data. Interpreted in the TCP/IP PI suite.

terminator
A resistive connector used to terminate the end of a cable or an unused tap into its characteristic impedance. The terminator prevents interference-causing signal reflections from the ends of the cable.

TFTP
Trivial File Transfer Protocol. A protocol within TCP/IP used to exchange files between networked stations. Interpreted in the TCP/IP PI suite.

TH
Transmission header. The initial part of an SNA frame immediately following the LLC header.

THT
Token Holding Timer. The maximum length of time a station holding the token can initiate asynchronous transmissions. The THT is initialized with the value corresponding to the difference between the arrival of the token and the TTRT (FDDI).

token
A small message used in some networks to represent the permission to transmit; it is passed from station to station in a predefined sequence.

token bus
A type of LAN where all stations can hear what any station transmits and where permission to transmit is represented by a token sent from station to station.

token ring A type of LAN where stations are wired in a ring and each can directly hear transmissions only from its immediate neighbor. Permission to transmit is granted by a token that circulates around the ring.

TP Transport-level Protocol. It exists in alternate forms, depending on how the services it assumes are provided to it by the network level below it. TP 0 assumes that the connection is maintained at the lower level, while TP 4 assumes a connectionless network protocol, so that functionality for the establishment and maintenance of a connection are included in the transport protocol. Levels 0, 2, and 4 are interpreted in the ISO PI suite.

trigger A Sniffer analyzer feature that allows a user to define an event after which the analyzer will stop capture to ensure that frames preceding or following the event are retained in the capture buffer.

TRLR Trailer format. Variant of IP in which the protocol headers follow rather than precede the user data.

TRT Token Rotation Timer. A clock that times the period between the receipt of tokens (FDDI).

TS Transmission Services. An SNA subprocess.

TSR Terminate and Stay Resident. A DOS program that once loaded into RAM, remains there in the background until unloaded or power is shut off.

TTRT Target Token Rotation Timer. The value used by the MAC receiver to time the operations of the MAC layer. The TTRT value varies depending on whether or not the ring is operational (FDDI).

TVX Valid Transmission Timer. A timer that times the period between valid transmissions on the ring; used to detect excessive ring noise, token loss, and other faults (FDDI).

UA Unnumbered Acknowledgment. An LLC frame that acknowledges a previous SABME or DISC request.

UDP User Datagram Protocol. A protocol within TCP/IP for sending unsequenced data frames not otherwise interpreted by TCP/IP.

UI Unnumbered Information. An LLC, HDLC, or SDLC frame type used to send data without sequence numbers.

UNA Upstream Neighbor Address. The network address of a token ring station's nearest upstream neighbor. IBM calls this the SUA (see Stored Upstream Address).

UNIX A popular portable operating system written by AT&T.

VINES VIrtual NEtwork Software. The networking operating system developed by Banyan Systems Inc., and the protocols used therein. Notable components are StreetTalk and MatchMaker.

virtual circuit A communications link that appears to be a dedicated point-to-point circuit.

VMTP Versatile Message Transaction Protocol (proposed).

VTP Virtual Terminal Protocol.

V.35 A CCITT wideband interface recommendation for WANs.

WAN Wide Area Network. A collection of LANs, or stations and hosts, extending over a wide area that can be connected via common carrier or private lines. Typically, transmission speeds are lower on a WAN than on a LAN.

X.25 A CCITT recommendation that defines the standard communications interface for access to packet-switched networks.

X.400 ISO standard protocol for electronic mail. Interpreted in the ISO PI suite.

X.500 ISO standard protocol for directory services. Similar to DNS and NIS.

XID Exchange Identification. An LLC unnumbered frame type used to negotiate what LLC services will be used during a connection.

XNS Xerox Network Systems. A family of protocols standardized by Xerox; in particular the Internet Transport Protocols.

X Windows Protocol for the management of high-resolution color windows at workstations, originated by MIT, DEC, and IBM and subsequently transferred to a consortium of vendors and developers.

YP Yellow Pages. A protocol developed by Sun Microsystems for implementing a distributed resource look-up database; similar in function to DNS. Interpreted in the Sun PI suite. Now called "NIS."

ZIP Zone Information Protocol. Used in AppleTalk to maintain an internet-wide mapping of networks to zone names. ZIP is used by the Name-Binding Protocol (NBP) to determine which networks belong to a given zone. Interpreted in the AppleTalk PI suite.

Zone In AppleTalk networks, a set of one or more networks within an internet, such that no network is a member of more than one zone.

INDEX

Index

Network General

We simplify network complexity.™

Network General Corporation
4200 Bohannon Drive
Menlo Park, CA 94025 USA
+1 (415) 688-2700

Network General Europe
Belgicastraat 4
1930 Zaventem, Belgium
+32 (2) 725-6030

Network General Canada, Ltd.
9225 Leslie Street, Unit #7
Richmond Hill, Ontario L4B 3H6 Canada
+1 (416) 882-7905

P/N:20028-004