Domino Internetwork Analyzer

Operating Guide

BN 9314/96.01

WAVETEK
WANDEL
GOLTERMANN

Communications Test Solutions

Microsoft® and Windows® are registered trademarks of Microsoft Corporation.

2000.Net_Check, DominoFastEthernet, DominoHSSI, DominoPLUS, DominoREMOTE, DominoServer, Examine, LinkView, LinkView PRO, Mentor, NetForce, NetForce Ranger, and Wizard are trademarks of Wavetek Wandel Goltermann.

ATMSim, DA-30C, Domino, DominoATM, DominoFDDI, DominoGigabit, DominoLAN, DominoWAN, DominoWIZARD, Internetworking, RTBench, and STBench are registered trademarks of Wavetek Wandel Goltermann.

All other trademarks and/or registered trademarks mentioned in this document are the property of their respective owners.

"The parallel port technology within this product is licensed under U.S. Patent 5,299,314."

Notice
Specifications and functions described in this document are subject to change without notice.

Revision History

January 1997	Revision 5
November 1997	Revision 6
February 1998	Revision 7
November 1998	Revision 8
December 1999	Revision 9, PN 9314-8496.017
September 2000	Revision 10

Printed in the USA on recycled paper.

Contents

2. Setting Up

3. Capturing Network Traffic

4. Monitoring Network Traffic

5. Examining Captured Traffic

6. Transmitting Traffic to the Network

A. Toolbar Reference

Preface

About This Book

This book contains background information, procedures, and examples for using the basic and advanced features of the Domino Internetwork Analyzer software.

This book assumes that you are familiar with the basic terminology and procedures for using Microsoft Windows. It also assumes that you have a basic understanding of personal computers, computer networks, and network protocols.

How This Book is Organized

This book is organized to follow the order of the Domino major tasks and the structure of the Domino software. A brief description of each chapter is provided below.

Chapter 1, Domino Basics	Provides introductory information about the Domino software, interface menus, and results windows.
Chapter 2, Setting Up	Provides instructions for installing and configuring the Domino software.
Chapter 3, Capturing Network Traffic	Explains how to capture and filter network traffic.
Chapter 4, Monitoring Network Traffic	Describes how to monitor traffic and display statistics and graphs in real time.
Chapter 5, Examining Network Traffic	Explains how to display, search for, filter, and print frames captured from your network.
Chapter 6, Transmitting Traffic to the Network	Describes how to play back and transmit capture files and how to build and transmit single frames.
Appendix A, Toolbar Reference	Provides a quick reference for the toolbar icons that appear on Domino screens.

Related Documentation

In addition to this manual, the following printed and online materials are included in the Domino package.

Domino Getting Started — Introduces the Domino Network Analyzer. Describes both software installation and hardware setup (including pin assignments for all interface cables) and provides a brief tour of the user interface.

On Line Help — Provides detailed information about Domino features and instructions about performing specific tasks. The on line help also provides network interface and protocol-specific reference information.

README.HLP — Contains information available only after the books in the package were published.

Document Conventions

The Domino documentation uses conventions for:

- key names, combinations, and sequences
- text instructions
- special information such as tips and notes

Keyboard Conventions

Convention	Description
Keys	All key names are shown as they typically appear on a personal computer, for example, Ctrl and Esc.
Key Combinations and Sequences	Keystroke combinations and sequences are used to invoke commands or perform operations. Key combinations are shown as **Key+Key**, for example, **Shift+F1**, which means to hold down the Shift key while pressing F1. Key sequences are shown as a comma-separated series, for example, Alt, F, A, which means to press and release each of these keys in order: first Alt, then F, then A.
Arrow Keys	The term arrow keys is the collective name for the Up Arrow, Down Arrow, Left Arrow, and Right Arrow keys.

Text Conventions

Convention	Description
Text That You Type	Specific text that you are to type is shown in boldface. For example, if the book says to type **win** you type the lowercase letters "win." What you type is always shown in lowercase letters, unless it must be typed in uppercase letters to work properly.
Filenames and Directories	Filenames and directories are shown in uppercase letters. For example, AUTOEXEC.BAT.
Nodenames and Programming Examples	Nodenames and programming examples are shown in Courier, a monospaced font, to more closely resemble their on-screen appearance.

Special Information

Tip:

A tip conveys information on shortcuts or convenient procedures that are not required but make tasks easier.

Note:

A note conveys information, which, if overlooked will seriously inconvenience the user but cause no permanent or unrecoverable errors.

Caution:

A caution message alerts you to the possibility of damage to the instrument, and describes the nature of the potential damage and steps to avoid the problem.

Warning:

A warning alerts you to the possibility of injury to the user of the instrument, such as from electrocution. Steps to avoid injury are part of the warning text.

Customer Support Contacts

To report a problem with Domino hardware or software, contact your local sales office.

When reporting a problem:

Be at your computer with the Domino analyzer running, and be prepared to provide the following information:

1. The name and version number of the Domino software that you are using.
2. The type and serial number of the WG hardware that you are using.
3. The type of network hardware you are using.
4. The specifications of the computer that you are using, including:
   - Make and model number
   - Processor speed
   - Amount of installed RAM
   - Available hard drive space
   - Operating system (Windows NT, Windows 98, or Windows 2000)
5. The exact wording of any messages that appeared on your screen.
6. What happened and what you were doing when the problem occurred.

Visit our Web site

For information on products, service, support, training, and how to contact your local sales office, visit WG's Web site at:

www.wwgsolutions.com

1. Domino Basics

1.1 The Domino Analyzer

The Domino Internetwork Analyzer is a small, portable network analysis instrument that you connect to a network and use to:

- monitor network activity
- capture and examine network traffic
- transmit test data onto the network
- measure and analyze network activity and performance

A personal computer serves as the instrument controller. The Domino user interface is a Microsoft Windows application that provides access to analyzer functions through easy-to-use menus, toolbars, and dialog boxes.

Each analyzer supports one network interface connection at a time. Up to eight analyzers can be linked in a daisy-chain configuration and connected to the controlling computer through the standard parallel interface port. This configuration enables you to perform concurrent data capture and analysis over multiple network interfaces.

Users of the WG DA-3x Protocol Analyzer will find that the Domino analyzer's data capture format and application software are DA-3x-compatible. Network data captured on a Domino analyzer can be transferred to a DA-3x for additional analysis.

NOTE:

The assumption is that, in the typical field service application, the Domino analyzer will be used with a notebook computer. References to a notebook computer in this document simply reflect that assumption. You can also use Domino with a standard size personal computer.

1.2 Software

The Domino Internetwork Analyzer supports four major areas of activity, each of which is reflected the structure of the software system. See Table 1-1.

Analysis activity	Software component
Basic analyzer applications and user support functions	Core software
Interface connectivity	Network interface software
Protocol decoding and analysis	Protocol software
Specialized test and measurement	Toolbox applications

Table 1-1. Domino software structure

The Domino analyzer software runs one or more analyzers that are connected to your computer through its parallel port. You can run as many as eight Domino analyzers through a direct connection.

1.2.1 Core Software

The Domino Core software consists of four primary applications: Capture, Monitor, Transmit, and Examine. Each of these applications can be accessed from the Workbench screen (The Workbench screen is shown in Figure 1-1.).

Capture, Monitor, and Transmit are the Real Time analysis applications of the Domino software. You use the Real Time applications to work with live network traffic or to simulate live network conditions. In contrast, you use the Examine application to work with captured traffic, either off-line or from a RAM capture buffer.

Application	Allows you to...
Capture	Capture and store network traffic in the capture buffer; filter network traffic to limit what is stored in the capture buffer.
Monitor	Monitor network events and display the results in graphs and charts.
Transmit	Play back a capture file onto the network and to the Domino analyzer simultaneously; build a test frame by editing a frame from a capture file, and transmit that frame onto the network for a specified duration.
Examine	Examine captured frames, display frame information, search for specific frames and filter captured frames.

Table 1-2. Domino Core Software Applications

Each of the Core software applications is explained in detail in separate chapters of this guide.

1.2.2 Network Interface Software

For each network interface that is supported by the Domino analyzer, the Domino software includes network interface software. You use the network interface software to set up the parameters for the network connection and to interact with the network interface.

1.2.3 Protocol Software

The Domino analyzer uses protocol software to decode the protocol information that is contained in the frames that are captured from the network traffic.

For the analyzer to be able to decode a protocol, the software for that protocol must be installed and the protocol must be identifiable by the protocol at the preceding layer. If a protocol is not identifiable by the preceding protocol, you can use the Advanced Setup functions of the Domino software to load that protocol and the one that precedes it at the appropriate layers on the protocol stack. Then the analyzer will be able to perform the decode.

1.3 The Domino Workbench

The Workbench screen provides access to all of the features of the Domino software. During installation, the Setup program automatically creates the Domino program group and the Domino icon. When you double-click the Domino icon to start the Domino software, the Workbench is the first screen that you see.

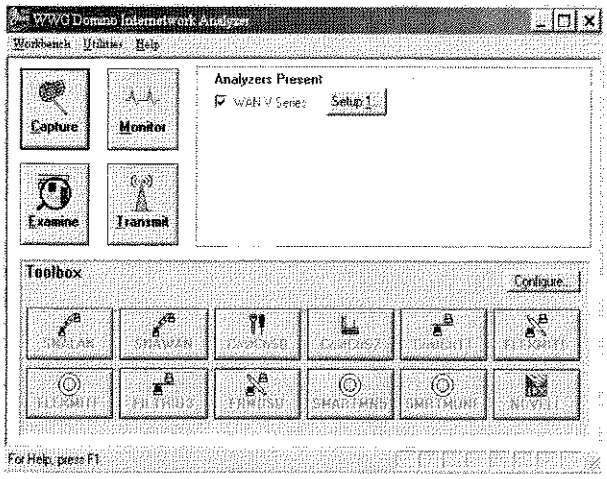


Figure 1-1. Workbench screen

The following table describes the main areas of the Workbench screen and their functions:

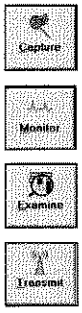
Screen area	Function
Four task buttons 	Enable selection of four main Domino applications: **Capture.** Starts the process of capturing network traffic. **Monitor.** Provides a comprehensive view of the activity on your network. **Examine.** Provides options for real time and post-capture processing of network traffic. **Transmit.** Plays back captured files onto the network, and builds and transmits single frames. Each of these applications is explained in detail in separate chapters of this guide.
Analyzers Present box	Lists and allows selection of the Domino analyzers currently connected through the computer's parallel port.
Toolbox	Allows assignment of optional applications to buttons for quick application starts.

Table 1-3. Workbench screen areas

To start an application:

1. Connect the Domino analyzer to the network. To learn how to connect an analyzer to the network, refer to *Domino Getting Started*.
2. In the **Analyzers Present** box, select the check box next to the analyzer on which you want to run the application.

   When the check box is selected, the analyzer is enabled.
3. In the Analyzers Present box, click **Setup** for the analyzer on which you want to run the application.

   In Setup, you specify the parameters for the network connection. To learn how to use Setup, see Chapter 2, "Setting Up."

   When the setup is complete, you return to the Workbench screen.
4. To start one of the Core applications (Monitor, Capture, Transmit, or Examine), click the corresponding task button.

1.4 Application Screens

When you start an application, the screen for that application appears. Figure 1-2. illustrates one of the application screens.

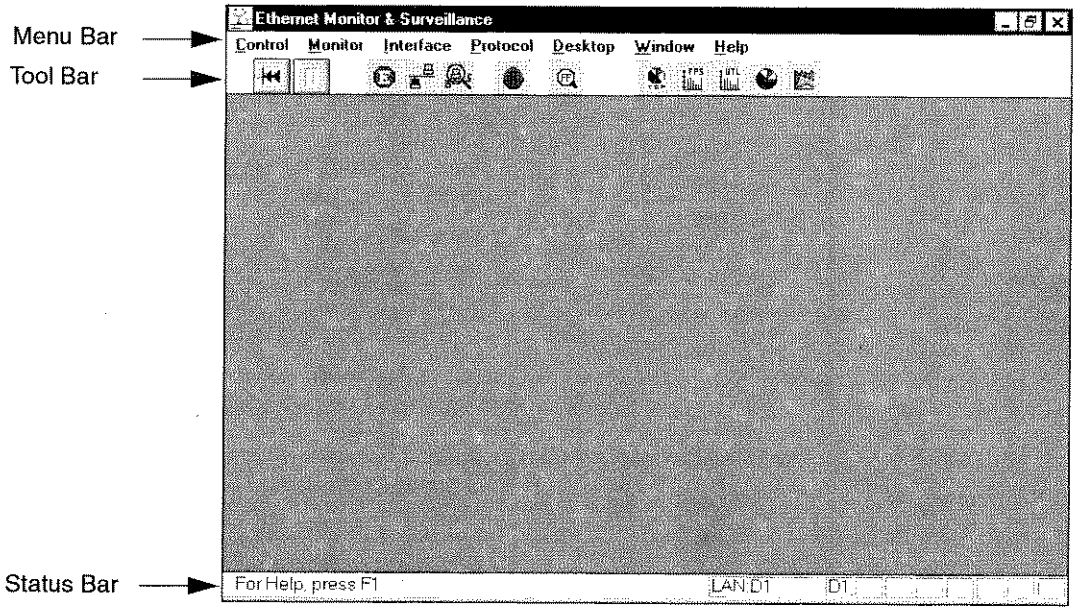


Figure 1-2. The Monitor screen, one of the Domino application screens

1.4.1 Menus and Menu Commands

Each Domino application screen has a menu bar at the top of the screen. The menu bar contains the names of the menus accessed from the screen; each menu includes commands that invoke actions or display results windows or dialog boxes on the screen.

1.4.2 Toolbars

Toolbars consist of a set of buttons that are displayed across the top of most Domino application screens. Toolbar buttons provide you with quick mouse access to the screen's most often used features. When the mouse pointer comes to rest on the button, a yellow flag identifies a button's function. Appendix A provides a reference to toolbar buttons and their functions.

1.4.3 Status Bar

The status bar is displayed at the bottom of each of the Domino application screens. It provides status information such as the current status of each Domino analyzer, prompts for currently highlighted menu commands, or prompts for accessing on-line help. The type of information displayed varies, depending on the screen that is displayed.

1.5 Domino Results Windows

The network information that the Domino analyzer collects is displayed in a variety of results windows. Examples of results windows include Network Status, Network Errors, Frame Summary, Protocol Detail, and Protocol Summary. The results windows that you can view vary, depending on the application that you are using. In every application you can display the available results windows by using commands on the screen menus and buttons on the toolbars.

To display a results window:

- From the Examine **Display** menu or from the **Interface** menu in any of the Real Time screens (Monitor, Capture, or Transmit), choose the results window that you want to display.

  The selected results window is displayed.

1.5.1 Moving Between Results Windows

You can have an unlimited number of results windows displayed on the screen at the same time. However, you can only interact with one window at a time—to move it, resize it, or close it. The title bar of the currently active window is highlighted.

To move to any open window:

- From the **Window** menu, choose the results window that you want to make active.

  The windows are listed at the bottom of the Window menu in the order in which they were opened.

To move to the next open window:

- From the **Control** menu, choose **Next** to move to the next window for the current capture buffer.

- Press **Ctrl+Tab** until the desired window is displayed.
- Use the mouse to click on a visible portion of the window.

1.5.2 Saving Results Statistics to an Export File

The Domino menus provide options that enable you to save the content of the current results window to either a CSV file or a text file for export to spreadsheet or word processing applications.

To save statistics to an export file:

1. From the **Control** menu in any of the Real Time screens (Monitor, Capture, or Transmit), or from the **File** menu in Examine, choose **Save to Export File**, then choose either **Export to CSV** or **Export to Text**.

   The Save Export File dialog box is displayed.

2. Type the name of the file in which you want to store the content of the results window in the filename box and click OK.

   The data in the current results window is stored in the file you specified with the extension .TXT or .CSV, depending on the type of export file you selected. You return to the screen in which you were working.

1.6 Interacting with Multiple Domino Analyzers

You can connect and run up to eight Domino analyzers with a single computer. To learn how to physically connect multiple analyzers to a computer, refer to *Domino Getting Started*.

When you start the Domino software, each instrument that is detected during startup is listed in the Analyzers Present box of the Workbench screen.

NOTE:

Before you begin, make sure that you set up each Domino analyzer appropriately for the application you want to run. To initiate the setup process for a specific analyzer, click **Setup** next to the listing for that analyzer in the **Analyzers Present** box. Chapter 2 provides detailed information about the setup process.

1.6.1 Starting a Core Application on Multiple Domino Analyzers

The check boxes in the **Analyzers Present** box on the Workbench are the switches that specify which analyzers will be active when you run the primary Real Time applications (Capture, Monitor, or Transmit). When the check box is selected, the corresponding analyzer is enabled. Then, when you choose the Capture, Monitor, or Transmit button from the Workbench, the application automatically starts on the enabled instrument.

To start Capture, Monitor, or Transmit on multiple analyzers:

1. Enable the analyzers on which you want to run the application by selecting the corresponding check boxes.

2. Click the **Capture**, **Monitor**, or **Transmit** button.

   The application is started on the enabled instruments.

1.6.2 Starting a Toolbox Application on Multiple Domino Analyzers

The startup dialog box that is displayed when you start one of the optional Domino Toolbox applications serves the same purpose as the check boxes in the **Analyzers Present** box of the Workbench. If you have only one Domino analyzer connected, this dialog box appears for you to confirm that you want to start the application in the currently selected test mode, with the specified setup, on the connected instrument. If you have multiple analyzers connected, the startup dialog box includes check boxes that you use to select the instruments on which you want to start the application.

To start an optional Toolbox application on multiple analyzers:

1. Click the application button in the Toolbox.

   The Start Toolbox Application dialog box is displayed.

2. Select the check boxes that correspond to the Domino analyzers on which you want to run the application.

   The application is started on each analyzer that you select.

1.6.3 Stopping an Application

To stop an application when you are running a single analyzer:

- From the menu bar, choose **Control/Exit**.

  The Stop Realtime Analysis dialog box appears, offering options for exiting without saving any captured frames or for saving captured traffic to a capture file before you exit.

To stop an application when you are running multiple analyzers:

1. From the menu bar for the application that you want to stop, choose **Control/ Stop Domino**.

   The Stop Realtime Analysis dialog box appears. The dialog box lists the Domino analyzers that are running the active application.

2. Select the analyzer on which you want to stop the application.

1.6.4 Shifting the Focus from One Domino Analyzer to Another

If you are running multiple Domino analyzers, the **Control menu** lists all the active analyzers, and allows you to shift your focus from one analyzer to another.

When you are running an application on multiple analyzers, the results windows that show the application's activity on each instrument are displayed in a "stack" on the screen. The selections on the Control menu enable you to change the focus, bringing the windows for the selected analyzer to the top of the stack so that you can see the statistics for the interface being monitored.

If you are running Domino analyzers of different types and you change focus from one interface type to another, the options on the toolbar change to match the interface of the analyzer that is "in focus."

To focus on a particular Domino analyzer:

- From the **Control** menu (shown in Figure 1-3.), choose the analyzer that you want to focus on.

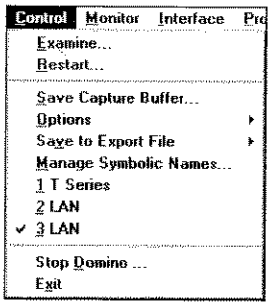


Figure 1-3. Control menu

The results windows for the selected analyzer come to the top of the stack.

Clicking on any part of a window brings that window to the top of the stack and changes the focus to the analyzer with which the window is associated.

1.6.5 Performing Tasks on Multiple Domino Analyzers

If you are running multiple Domino analyzers, certain options on the Control menu present a task dialog like the one shown in Figure 1-4.. Use it to specify which instrument's operation you want to address.

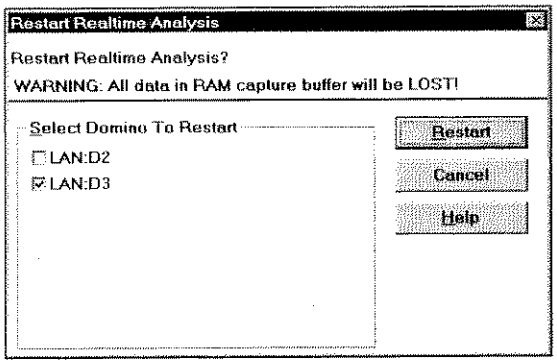


Figure 1-4. Restart Realtime Analysis dialog box

Similar dialogs are presented to enable you to perform such Control menu tasks as:

- stopping or restarting Real Time analysis
- saving data in the capture buffer to a file
- starting Examine from Real Time (Monitor, Capture, or Transmit).

To change the operation on a specific Domino analyzer:

1. From the **Control** menu, choose the task that you want to perform.

   The appropriate task dialog is displayed.
2. Select the check box for the analyzer on which you want to perform the task.
3. Click the button on the dialog box that starts the task.

1.6.6 Running Multiple Applications on Multiple Domino Analyzers

The Domino system provides multi-analyzer capability that enables you to operate several Domino analyzers concurrently, with different applications running on each instrument. For example, if you had two Ethernet segments and one Token Ring connected through a router, you could set up a test configuration using three DominoLAN analyzers with the following applications:

- Transmit running on Domino 1 connected to the first Ethernet segment
- Monitor running on Domino 2 connected to the second Ethernet segment
- Monitor running on Domino 3 connected to the Token Ring

Hints for running different applications on different instruments:

- Make sure you set up each Domino analyzer appropriately for the application you want to run. Chapter 2, "Setting Up" provides detailed information about the setup process.
- Remember that Capture, Monitor, or Transmit will start on all enabled instruments. If you want to run only one of these applications on a single analyzer, enable only that analyzer, then start the application.
- When your first application is running, you need to return to the Workbench to start the next one. Display the Windows taskbar and double-click the Domino button to display the Workbench screen.
- When you click one of the Toolbox buttons for an optional application, the Start Toolbox Application dialog box is displayed. If you have more than one Domino analyzer connected that would be compatible with the selected Toolbox application, the Start Toolbox Application dialog box includes a checklist in which you can choose the instrument on which you want to start the application.
- When all of the applications are running, you can use the commands on the Real Time **Control** menu to switch focus from one analyzer to another.

1.7 Working with Desktops and Desktop Files

The Domino applications provide a variety of results windows, statistical tables, charts, and graphs that you can display on the screen concurrently.

You may find that you frequently use the same combinations of windows and charts when, for example, you are monitoring network errors or tracking a particular type of network problem. Desktops and desktop files offer a convenient way to reproduce frequently-used window combinations and screen layouts without having to re-select all of the windows and rearrange them on the screen.

1.7.1 What Are Desktops and Desktop Files?

A **desktop** is a retrievable screen configuration that you define. It contains a set of results windows that you can recall to the screen with a single menu command. When you define a desktop you give it a name, which is added to the numbered selection list on the Desktop menu in the Real Time screens (Monitor, Capture, or Transmit). You can have up to 10 desktops defined (listed on the Desktop menu) at one time. To display a desktop, you select it from the Desktop menu.

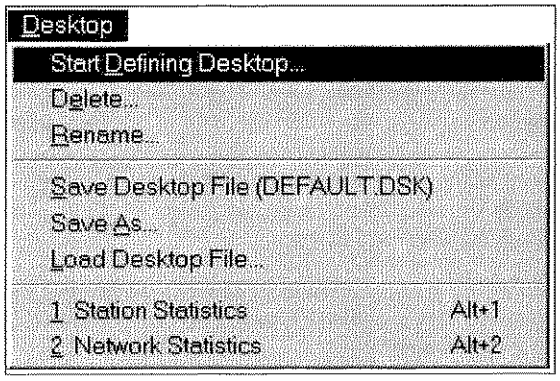


Figure 1-5. The Desktop menu

You can save the set of currently-defined desktops in a **desktop file**. When you load the desktop file, the desktops that it contains are listed on the Desktop menu.

- Desktops are **interface-specific**: For example, th e Token Ring Map window cannot be displayed (and therefore couldn't be part of a desktop) if you are running a DominoLAN analyzer with an Ethernet interface.
- Desktops are **application specific:** For example, the results windows available from Monitor are not available when you are running Transmit.
- Desktops are **analyzer-specific**: For example, If you create a desktop for a DominoLAN analyzer (Ethernet) connected as Domino 1 while you are running Monitor, that desktop does not appear on the Desktop menu for the DominoLAN analyzer (Ethernet) that is running Monitor and connected as Domino 2.

By contrast, **desktop files** are interface-specific and application-specific, but **not** analyzer-specific. If you save a desktop file on a DominoLAN analyzer (Ethernet) while you are running Monitor, you can load that desktop file on **any** connected DominoLAN analyzer (Ethernet) while you are running Monitor. As a result, by loading the same desktop file on several DominoLAN analyzers (all Ethernet) you could run Monitor and access the same set of desktops on all of the analyzers.

1.7.2 Using Desktops and Desktop Files

Table 1-4 summarizes the differences in using desktops and desktop files.

Desktops	Desktop files
Created or modified by choosing **Start Defining Desktop/Stop Defining Desktop** from the **Desktop** menu.	Created or modified by using the **Save Desktop** or **Save As** command on the **Desktop** menu.
Stored with the application from which you created it as a numbered selection on the Desktop menu.	Stored as a .DSK file in the \DOMINO\VIEWS directory.
Accessible only from a Domino analyzer of the same interface type, connected in the same position, and running the same application as the analyzer on which the desktop was created.	Accessible by all linked Domino analyzers of the same interface type that are running the application from which the desktop file was created.
Displayed by choosing the desktop from the numbered list of defined desktops on the **Desktop** menu.	Displayed by choosing the **Load Desktop** command on the **Desktop** menu. The content of the desktop file is represented by the desktops listed on the Desktop menu.
Deleted by choosing **Delete Desktop** from the **Desktop** menu.	Deleted using DOS or Windows file management functions.

Table 1-4. Desktops and Desktop Files

1.7.3 Defining a Desktop

Defining a desktop is like recording a macro for displaying a specific set of results or application windows. The basic procedure is to:

- name the desktop and start the desktop recorder
- open a set of results windows that are recorded as the content of the desktop
- stop the desktop recorder

The defined desktop consists of the windows that are displayed when you invoke the command to stop defining the desktop.

If you start defining a desktop when windows are already displayed on the screen, those windows are part of the desktop. All subsequent changes to the screen layout are added to the desktop definition until you choose the **Stop Defining Desktop** command.

To define a desktop:

1. From the menu bar in any of the Real Time applications (Monitor, Capture, or Transmit), choose **Desktop/Start Defining Desktop**.

   The Define a Desktop dialog box is displayed. (Figure 1-6.).

2. In the **Desktop to Define** box, type the name of the desktop you are going to create.

   The desktop name can be up to 30 characters long.

3. To start defining the desktop from a clear screen, select **Close All Open Windows First**.

4. Click **OK**.

   The desktop recorder is started and you return to the screen in which you were working.

5. Open the windows that you want to include in the desktop, and arrange them in whatever way seems best to you.

6. From the menu bar, choose **Desktop/Stop Defining Desktops.**

   The desktop is added as a numbered selection at the bottom of the Desktop menu.

NOTE:
If you start defining a desktop and then exit the application without invoking the **Stop Defining Desktop** command, the content of the screen when you exit is saved as the desktop you started to define.

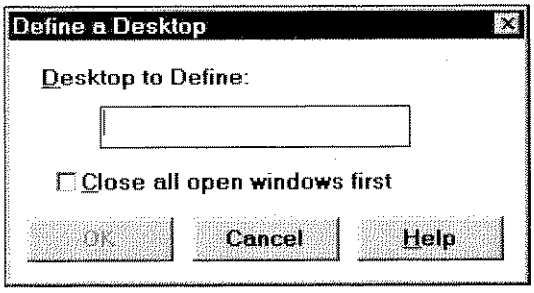


Figure 1-6. The Define a Desktop dialog box

1.7.4 Defining the Existing Screen Layout as a Desktop

If you realize that the current set of windows on the screen is a useful combination that you would like to be able to reuse, defining the desktop is simply a matter of starting the desktop recorder, specifying a name for the desktop, and immediately stopping the desktop recorder. The trick is to remember to stop the recorder before you make any changes to the screen.

To save the existing screen layout as a desktop:

1. From the menu bar, choose **Desktop/Start Defining Desktop**.

   The Define a Desktop dialog box is displayed.

2. In the **Desktop to Define** field, type the name that you want to assign to the existing combination of windows on the screen.

   The desktop name can be up to 30 characters long.

3. Click **OK**.

   The desktop recorder starts and you return to the screen in which you were working.

4. Immediately, from the menu bar, choose **Desktop/Stop Defining Desktop**.

   The existing screen layout is defined as a desktop.

1.7.5 Working with Desktops on Multiple Domino Analyzers

When you are running multiple Domino analyzers, only one analyzer is in focus at a time, and you can only interact with the analyzer that is in focus. The following are points to be aware of when you are working with desktops on multiple analyzers.

- Desktops are analyzer-specific. If you are running multiple analyzers and you define a desktop, the desktop includes only the windows that pertain to the analyzer that is in focus, regardless of what other windows (relating to other analyzers) are on the screen at the time.
- If you invoke the **Save Desktop File** command while you are displaying desktops for multiple analyzers, the only desktop that is saved to a desktop file is the one that pertains to the analyzer that is in focus.

1.7.6 Modifying a Desktop

You may find that a desktop would be more useful if it included other results windows, or if the existing windows were arranged differently.

To make changes to an existing desktop:

1. From the menu bar, choose **Desktop/Start Defining Desktop**.

   The Define a Desktop dialog box is displayed.

2. In **Desktop to Define**, type the name of the existing desktop that you want to change.

3. Click **OK**.

   The Desktop Modification confirmation box is displayed to tell you that you are about to overwrite an existing desktop.

4. Click **OK**.

   You are returned to the screen in which you were working.

5. Open or close windows or rearrange the windows on the screen.
6. From the menu bar, choose **Desktop/Stop Defining**.

   The original desktop is redefined to include the changes you have just made.

1.7.7 Deleting a Desktop

You can define up to ten desktops at one time. Periodically, you may need to delete old desktops to make space for new ones.

If you delete a currently selected desktop, all of the windows pertaining to that desktop are closed.

To delete a desktop:

1. From the menu bar, choose **Desktop/Delete Desktop**.

   The Delete a Desktop dialog box is displayed (Figure 1-7.).

2. From the list of defined desktops, select the desktops that you want to delete.
3. Click **OK**.

   The Delete a Desktop confirmation box is displayed.

4. Click OK to proceed with the deletion of the desktops.

   The desktop is deleted and you are returned to the screen in which you were working.

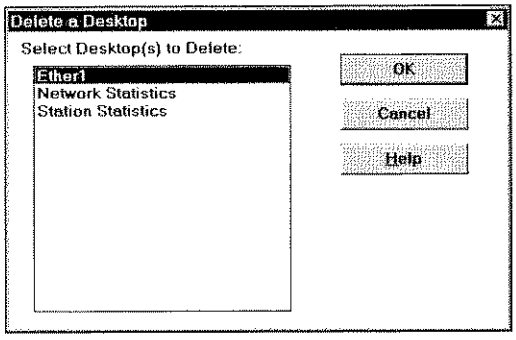


Figure 1-7. The Delete a Desktop dialog box

1.7.8 Renaming a Desktop

You may find it useful to be able to change the name of an existing desktop.

To rename a desktop:

1. From the menu bar, choose **Desktop/Rename Desktop**.

   The Rename a Desktop dialog box is displayed.

2. From the list of currently defined desktops, select the desktop that you want to rename.
3. In **Rename As**, type the new name for the desktop.
4. Click **OK**.

The desktop is renamed and you return to the screen in which you were working. The next time that you display the Desktop menu, the new desktop name appears in the numbered selection list.

1.7.9 Saving a Desktop File

Desktop files allow you to store desktops in a form that makes them portable from one Domino analyzer to another. For example, if you are running the same application on multiple analyzers of the same interface type, you can load the same desktop file on all of the analyzers and display the same configuration of results windows for all of the instruments.

To save the currently defined desktops to a new desktop file:

1. From the menu bar, choose **Desktop/Save As**.

   The Save Desktop File dialog box is displayed.

2. In **Filename**, type the name of the desktop file.
3. Click **OK**.

   The currently-defined desktops are saved into the desktop file that you specified.

NOTES:

- If you load a desktop file and make changes to the current desktop or desktops, you can save those changes to the desktop file by choosing **Save Desktop File** from the **Desktop** menu.
- If you load a desktop file and make changes to the defined desktops, when you exit the application you are prompted to save the changes to the current desktop file.
- The name of the currently loaded desktop file is displayed in parentheses next to the Save Desktop File command on the Desktop menu. The label "untitled" appears in the parentheses when no desktop file is currently loaded.

1.7.10 Loading a Desktop File

Once you have created a desktop file, you can load that file on any Domino analyzer of the same interface type that is running the application from which the desktop file was created.

To load a desktop file:

1. From the menu bar, choose **Desktop/Load Desktop File**.

   The Open Desktop File dialog box is displayed.

2. From the list of desktop files, select the desktop file that you want to load.
3. Click **OK**.

   You return to the screen in which you were working. The desktops stored in the desktop file are listed as numbered selections on the Desktop menu, replacing whatever desktops were on the menu before you loaded the desktop file.

NOTES:

- If you load a desktop file and make changes to the desktops, you can save those changes to the desktop file by choosing **Save Desktop File** from the **Desktop** menu.
- If you attempt to load a desktop file and have not saved the desktops you are currently working on, you are prompted to save the current desktops to a desktop file.

2. Setting Up

2.1 Getting Started

To start the Domino software:

- In the DominoNAS Components folder or the Domino Core folder, double-click the Domino Core icon.

  The Parallel Port Driver Test window is displayed while all the attached Domino analyzers are tested and initialized; then the Workbench screen appears (Figure 2-1.). The Workbench screen provides access to all of the features of the Domino Internetwork Analyzer.

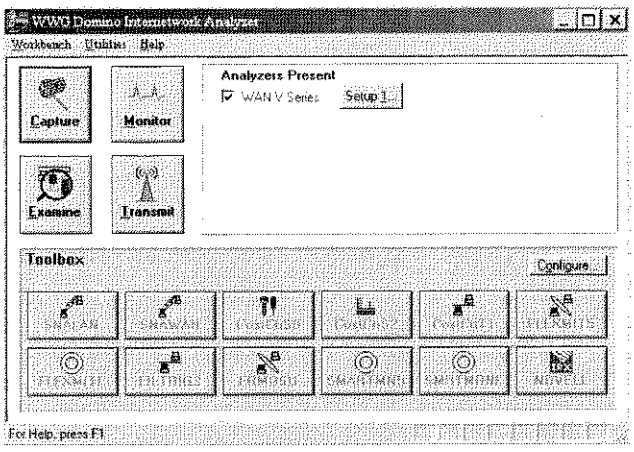


Figure 2-1. Workbench screen

2.1.1 Enabling a Domino Analyzer

The Analyzers Present box of the Workbench screen lists the Domino analyzers that are powered on and connected to the controlling computer. When you enable a Domino analyzer, you specify that you want that analyzer to be active when you run Capture, Monitor, or Transmit.

To enable a Domino analyzer:

- Choose the check box next to the analyzer that you want to enable.

  A check mark appears in the selected check box to indicate that the analyzer has been enabled.

You can enable multiple analyzers concurrently.

2.1.2 Reinitializing a Domino Analyzer

If no analyzers are listed in the Analyzers Present box on the Workbench screen, it means that the instruments were not connected or powered on when you started the software. To correct this without exiting the Domino software, you can reinitialize the analyzers.

To reinitialize a locally-connected analyzer:

1. Make sure that all the instruments you want to work with are connected and powered on.
2. From the menu bar on the Workbench screen, choose **Tools/Reinitialize Dominos**.

   The Parallel Port Driver Test window is displayed, all connected Domino analyzers are tested and initialized, and the Analyzers Present list is updated.

2.2 Setting up a Domino Analyzer

A Setup button appears beside each Domino analyzer listed in the Analyzers Present box of the Workbench screen. Choose this button to set up the corresponding analyzer. You can set up an analyzer whether it is enabled or not. The options that you can set vary depending on the interface type of the Domino analyzer chosen. You can learn about the options for your interface by reading the online Help for that interface.

To set up a network interface:

1. From the Workbench screen, click **Setup** for the analyzer that you want.

   The appropriate Setup dialog box appears. Figure 2-2. and Figure 2-3. are examples of Setup dialog boxes.

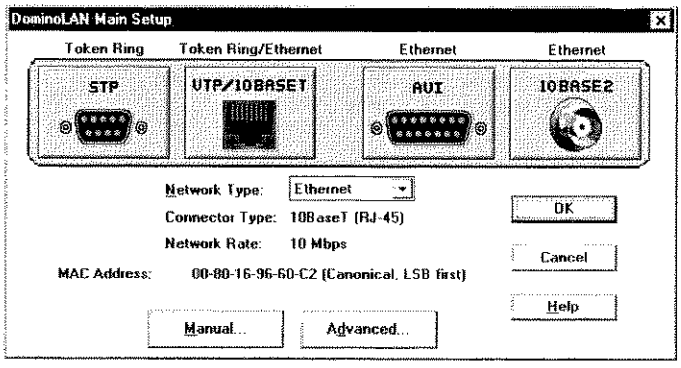


Figure 2-2. Sample DominoLAN Interface Setup dialog box

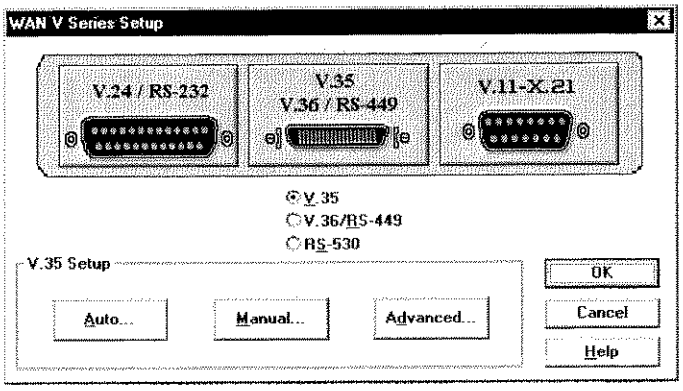


Figure 2-3. Sample DominoWAN Interface Setup dialog box

2. Select the connector type by choosing one of the illustrated connectors and one of the option buttons, if appropriate.
3. Choose one of the following configuration options:

Auto *DominoWAN V-series only*	Provides automatic interface configuration
Manual *All interfaces*	Enables you to configure all interface-specific parameters
Advanced *All interfaces*	Provides options such as setting up the protocol stack, RAM and disk capturing, frame slicing, and character code

4. Make any desired changes to the interface setup information and click **OK**.

2.3 Using DominoWAN Auto Configuration

When you select the auto configuration option, the DominoWAN analyzer tests samples of the line data, displays the configuration of the network, and configures the analyzer with the discovered parameters. This option is useful if you are not certain of the line characteristics. The DominoLAN analyzer does not support auto configuration.

To select auto configuration:

1. Click **Auto** on the interface-specific setup dialog box.

   The appropriate Auto Configuration dialog box (Figure 2-4.) is displayed with the automatic configuration settings. To have the DominoWAN analyzer retest the network, click **Re-sample**.

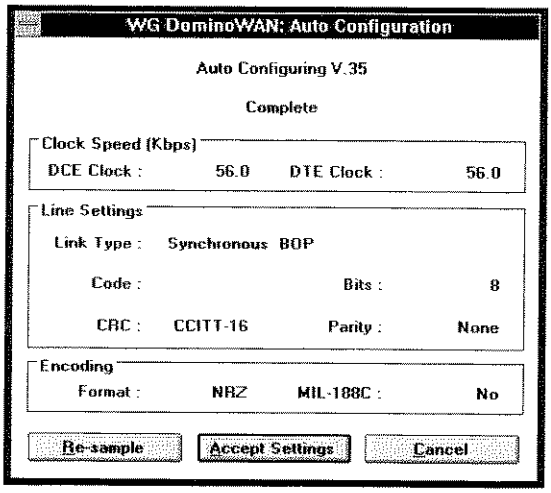


Figure 2-4. DominoWAN Auto Configuration dialog box

2. Click **Accept Settings**.

   The selected analyzer is automatically configured and you return to the Workbench screen.

2.4 Using Manual Configuration

Manual configuration enables you to specify configuration parameters such as test mode and hardware filters.

NOTE:

You cannot change the link type during Real Time analysis.

To select manual configuration:

1. Click **Manual** on the interface-specific Setup dialog box. (Figure 2-2. and Figure 2-3. are examples.)

   The appropriate manual setup dialog box appears. Figure 2-5. and Figure 2-6. are examples of manual setup dialog boxes.

2. Make the desired changes to the setup information.
3. Click **OK**.

   The selected Domino analyzer is configured and you return to the initial Setup dialog box.

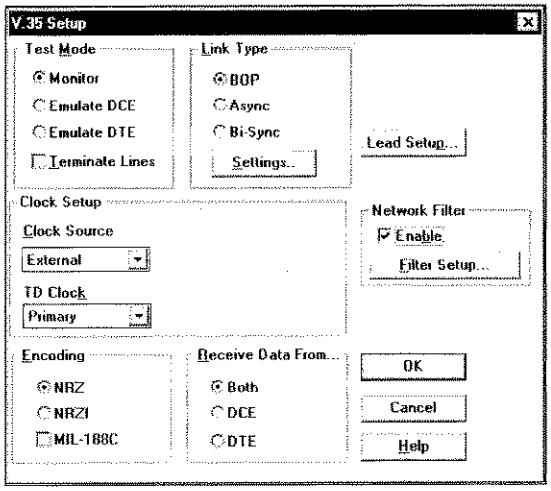


Figure 2-5. Sample WAN manual interface setup dialog box

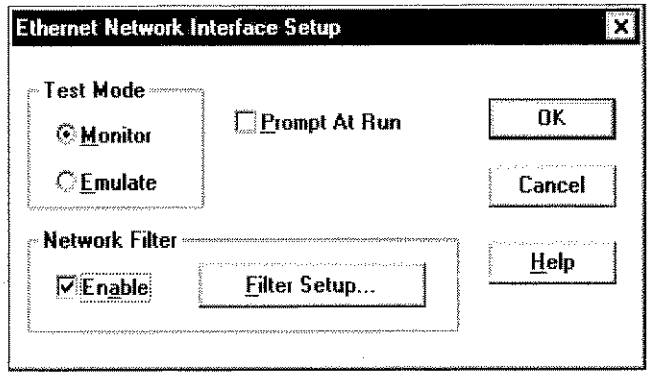


Figure 2-6. Sample LAN manual interface setup dialog box

2.5 Using Advanced Configuration

Advanced configuration includes setup for the following configuration items:

- Protocol Stack
- RAM/Disk Capture
- Internal Playback
- Frame Slicing
- Character Code

To select advanced configuration:

1. Click **Advanced** on the interface-specific Setup dialog box.

   The Advanced Setup dialog box appears (Figure 2-7.)

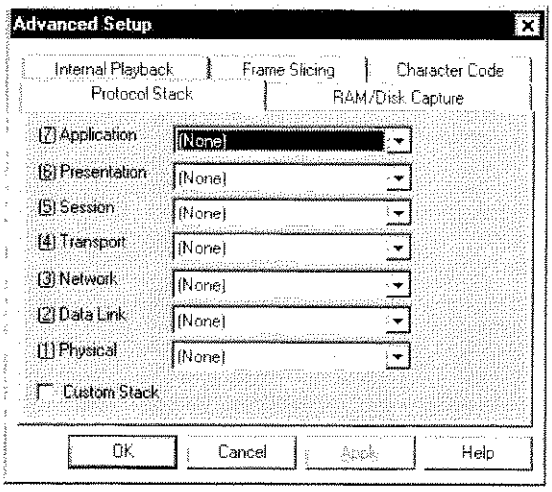


Figure 2-7. Advanced Setup dialog box with the Protocol Stack tab selected

2. Click one of the tabs and set up the desired parameters.
3. Click **OK**.

   You return to the Setup dialog box.

2.5.1 Setting Up the Protocol Stack

The Protocol Stack setup options enable you to load protocols on the protocol stack at their default layer or at any layer that you choose. This is controlled by the Custom Stack feature as follows:

- When Custom Stack is disabled, you can only select protocols to load at their default layer.
- When Custom Stack is enabled, you can load any protocol at any layer.

NOTE:

For the Domino analyzer to be able to decode a protocol, the software for that protocol must be installed and the protocol must be identifiable by the protocol at the preceding layer. A protocol that cannot be identified by the preceding protocol can be decoded only if you load that protocol and the one that precedes it at the appropriate layers on the protocol stack.

When analyzing WAN traffic, you must load the first protocol on the protocol stack, for example, Frame Relay, HDLC, or SDLC. Also, because WAN protocols typically lack the ability to detect the next layer protocol, it is advisable to load the upper layer protocols that you want to decode on the stack as well. The physical layer is automatically set to the interface you selected on the previous screen (e.g., V.24).

2.5.1.1 Loading a Protocol on the Stack

To load a protocol on the protocol stack:

1. In the Advanced Setup dialog box, click the **Protocol Stack** tab.

   The Protocol Stack setup appears (Figure 2-7.).

2. To load a protocol at any layer, select the **Custom Stack** check box to enable the custom stack feature.

   To load at the default layer, clear the **Custom Stack** check box to disable the custom stack feature.

3. Move the cursor to the layer where you want to load the protocol.

4. Use the Up Arrow or Down Arrow to scroll through the list of available protocols and select the protocol that you want to load.

   If a Setup button appears for the selected protocol, then click **Setup** and make any necessary changes to the protocol setup.

2.5.1.2 Decoding Proprietary Protocols

The Domino analyzer's ability to decode all traffic correctly is limited if the traffic includes proprietary protocol encapsulations that the instrument's protocol software does not decode.

The Glue protocol software lets you obtain accurate protocol decodes at all layers, even when proprietary protocol information is present, by enabling you to define fields that account for the bytes occupied by the proprietary protocol. When loaded at the appropriate layer and customized in this way, the Glue protocol software enables the Domino software to perform a rudimentary decode on the intervening protocol encapsulation, and protocols loaded at succeeding layers can then be decoded accurately. The Glue protocol software can be loaded at any layer on the protocol stack and at as many layers as needed. However, all protocols loaded on the protocol stack must be loaded in the order in which they occur in the frame, from lowest to highest layer.

When the protocol software is configured and loaded on the protocol stack, the Glue protocol software displays decode information in the Protocol Summary and Protocol Detail windows for the fields you have defined. These windows are results windows in the Examine application.

You can configure the Glue protocol software by defining protocol fields on the Glue Protocol Definition dialog box. You can access the Glue Protocol Definition dialog box from the Protocol Stack tab of the Advanced Setup dialog box.

To define protocol fields:

1. In the Protocol Stack setup, at the layer that carries the proprietary protocol, select the Glue protocol.

   A **Setup** button appears next to the box for the layer at which you loaded Glue.

2. Click **Setup**.

   The Glue Protocol Definition dialog box is displayed (Figure 2-8.).

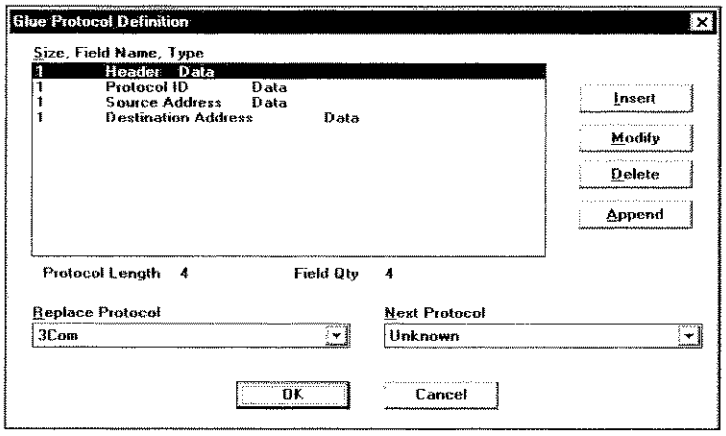


Figure 2-8. Glue Protocol Definition dialog box

3. For each field in the proprietary protocol that you are defining, perform the following steps:

   a. Click **Append**.

      The Field Definition dialog box is displayed (Figure 2-9.).

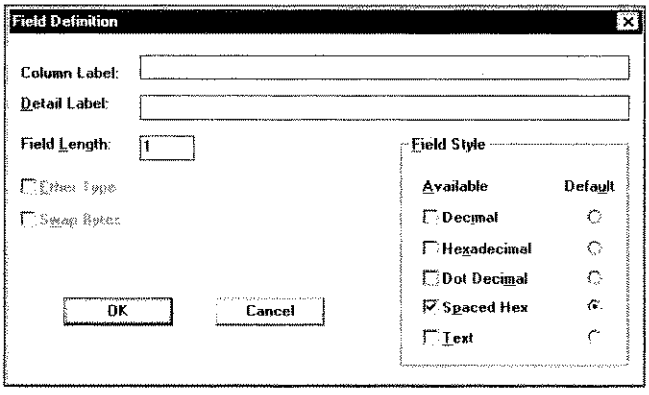


Figure 2-9. Field Definition dialog box

b. Define the field.

You can specify the length of the field and the format used for displaying the field contents. If an **Ether Type** field is in the proprietary protocol, you can specify whether or not the next protocol is detected based on its Ether Type value. In the **Swap Bytes** box you can specify whether the bytes of the field are swapped for decoding.

c. Click **OK**.

You return to the Glue Protocol Definition dialog box, where the size, field name, and type are shown.

4. Repeat steps a through c for each field that you are defining.
5. In the Glue Protocol Definition dialog box, specify the protocol that is being replaced and the protocol to be decoded at the next layer.

   An alternative way to indicate which protocol follows Glue in the Glue Protocol Definition dialog box is to enable the **Ether Type** check box when you define a protocol field. Decoding occurs as indicated below:

When the Ether Type check box is	And the Next Protocol field is	Decoding of data at the layer following Glue is
Enabled	Specified	As specified in the Next Protocol field.
Enabled	Unknown	As specified in Ether Type field.
Disabled	Unknown	According to stack specification.

6. Click **OK** when you have finished defining all of the proprietary protocol fields.

   You return to the Protocol Stack setup.

When you run your application and access the GLUE decode screen (Figure 2-10.), the Domino software will display decodes for the proprietary protocol with the headers and lengths that you have defined.

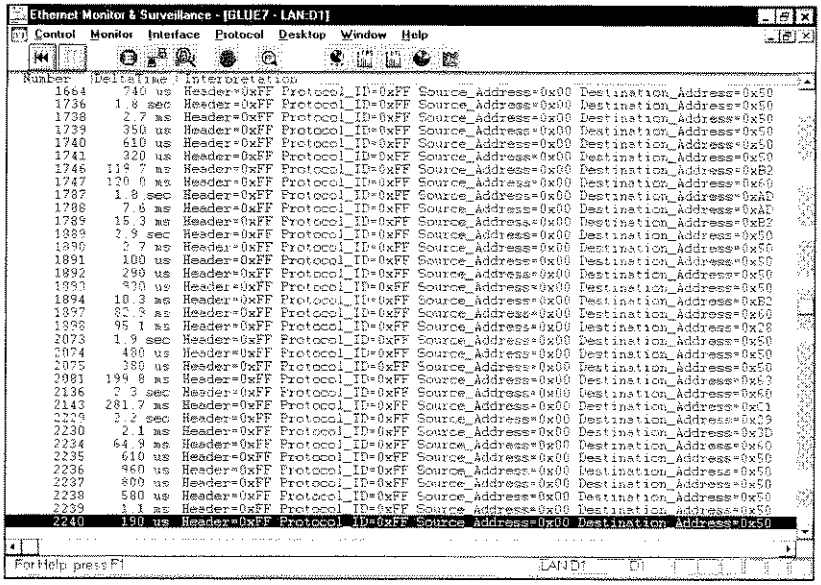


Figure 2-10. Glue Decode screen

2.5.1.3 Setting Up a Protocol

For a few selected protocols, such as Glue, HDLC, and SDLC, a Protocol Setup dialog box is available that you can use to specify how Domino interacts with the protocol software.

To set up a protocol:

1. In the Advanced Setup dialog box, click the **Protocol Stack** tab.

   The Protocol Stack setup appears (Figure 2-7.).

2. Load the desired protocol on the protocol stack.

   If a **Setup** button is available, it appears next to the layer protocol box.

3. Click **Setup**.

   The appropriate protocol setup dialog box appears. Figure 2-11. is an example.

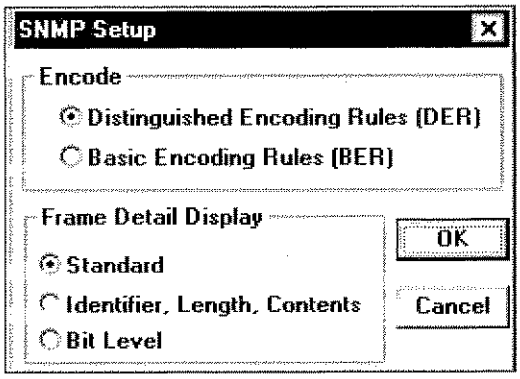


Figure 2-11. Sample protocol setup dialog box

4. Make any necessary changes to the protocol setup.
5. Click **OK**.

   You return to the Protocol Stack setup.

2.5.2 Setting Up the RAM Capture Buffer

The Domino analyzer captures network traffic during Real Time operation and stores the frames in a RAM buffer for analysis. This process of capture and analysis occurs not only when you are using the Capture application, but also when you use Monitor or Transmit. RAM/Disk Capture setup provides options for the following:

- Limiting the size of the analyzer's RAM capture buffer
- Specifying what happens when the buffer becomes full
- Automatically saving the contents of the buffer to your computer's disk.

2.5.2.1 Selecting the Maximum Size for RAM Capture Buffer

The actual size of the available memory (for options other than MIN) is determined by the amount of RAM installed on the analyzer. The analyzer RAM is shared by the capture buffer and the Domino operating software, which requires at least 500 KB to perform analysis tasks. This leaves the remaining RAM for capture buffer use. For example, if your Domino analyzer has 4 MB of analyzer RAM and you select 100% as the RAM Capture Size, then the size of the capture buffer is 3.5 MB.

To select the maximum size for the RAM capture buffer:

1. In the Advanced Setup dialog box, click the **RAM/Disk Capture** tab.

   The RAM/Disk Capture setup appears(Figure 2-12.).

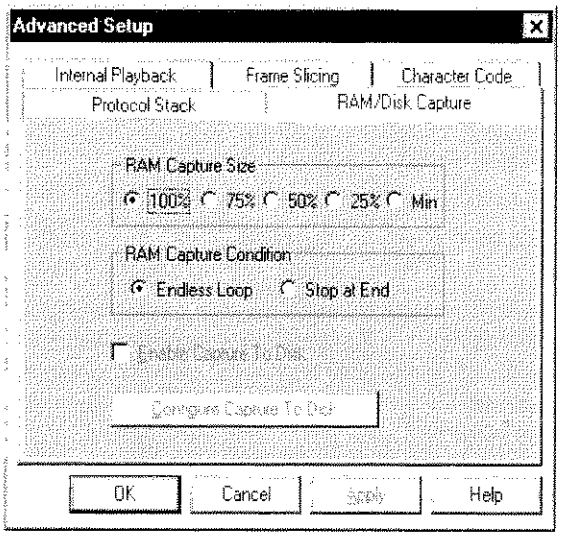


Figure 2-12. Advanced Setup dialog box with the RAM/Disk Capture tab selected

2. Choose one of the RAM Capture Size options:
   - 100%
   - 75%
   - 50%
   - 25%
   - Minimum (64 KB)

   The default RAM Capture Size is 100%.

2.5.2.2 Selecting the Stop Condition for RAM Capturing

The stop condition controls how the Domino analyzer responds when it has filled the buffer with captured traffic. The options are to stop capturing network traffic to the capture buffer or to overwrite the existing capture buffer starting at the beginning of the buffer.

To select the stop condition for RAM capturing:

1. In the Advanced Setup dialog box, click the **RAM/Disk Capture** tab.

   The RAMDisk Capture setup appears (Figure 2-7.).

2. Choose one of the Stop Condition options:
   - Endless Loop
   - Stop At End

   The default stop condition is Endless Loop.

NOTE:

The Domino analyzer always captures and analyzes traffic in the RAM capture buffer during Real Time operation and the stop condition parameter governs how the buffer is managed. However, when you choose Capture from the Workbench, the stop condition defaults to Stop At End. The Endless Loop option applies only to the Monitor and Transmit applications (except for FastEthernet interfaces). It does not apply when you run the Capture application.

2.5.2.3 Capturing Traffic to Your Computer's Disk

When you want to capture an amount of traffic that you expect will exceed the capacity of the RAM buffer, you can set up the system so that it automatically performs a capture, saves the captured traffic to your computer's disk, and repeats the process. You can specify how and when you want the process to start and to repeat. The cycle of automatic capturing, saving, and repeating can begin:

- Each time the Domino capture buffer is filled to a specified level.
- At a specified time, repeating at specified intervals.
- Each time a specified trigger occurs during a specified interval.

NOTE:

Capture to Disk is not available for LAN and FDDI network interfaces.

To repeat captures to your disk automatically:

1. In the Advanced Setup dialog box, click the **RAM/Disk Capture** tab. (Figure 2-13.).

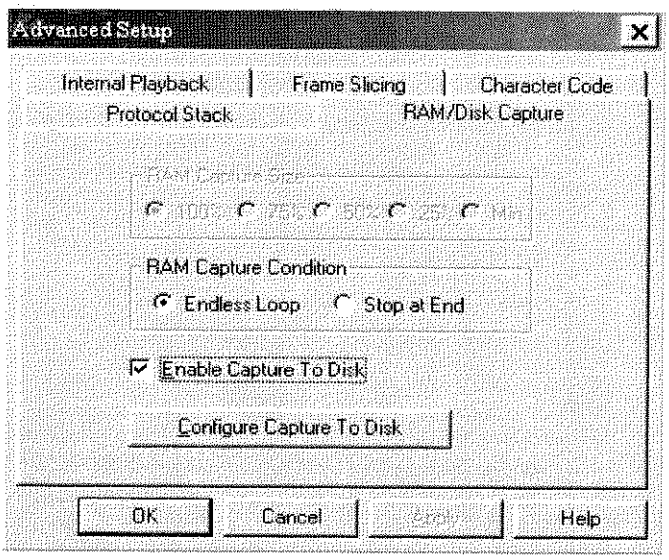


Figure 2-13. Advanced Setup dialog box with the RAM/Disk Capture tab selected

2. Select **Enable Capture to Disk**; then click **Configure Capture to Disk**.

   The Configure Capture to Disk dialog box appears (Figure 2-14.).

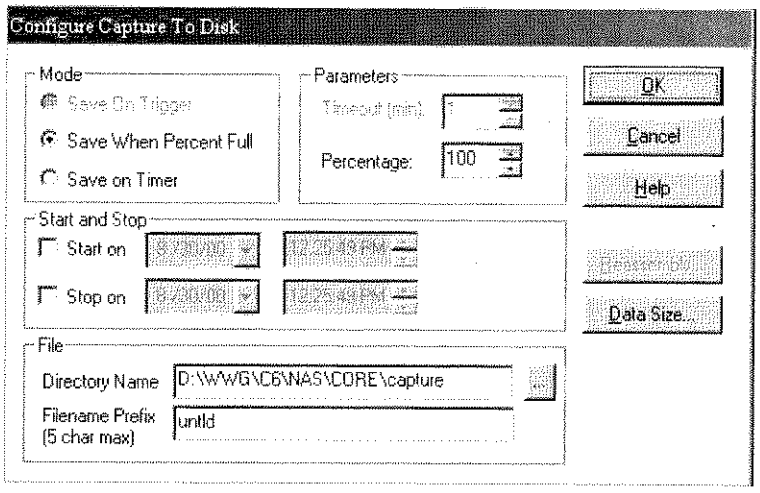


Figure 2-14. Configure Capture to Disk dialog box

3. Under **Mode**, take one of the following actions:

   - To save captured data and clear the Domino capture buffer each time that a trigger condition is met, click **Save on Trigger**. (This option is available for FastEthernet, HSSI, and Gigabit interfaces only.)

     To learn how to set up a trigger, see Section 3.2.3, "Setting Up Triggers."

   - To save captured data each time the Domino capture buffer is filled to a certain limit, click **Save When Percent Full**. Under **Parameters**, specify the point at which you want to initiate the save action (in terms of the percent of the buffer to be filled.)

   - To save a specified percentage of the RAM buffer at regular intervals, click **Save on Timer**. Under **Parameters**, use **Timeout** to specify how often you want to save the captured data (in minutes). Use **Percentage** to specify how much of the traffic in the buffer to save each time.

     To limit the interval in which the capturing and saving process occurs, specify the dates and times under **Start** and **Stop**.

4. Under **File**, type a name in the **Filename Prefix** box. (Click the button to browse to the directory that you want.)

   With each successive data capture, a new number is appended to the filename prefix.

5. Click **OK**.

   You return to the Advanced Setup dialog box. The process that you have set up will be activated when you start or reinitialize the analyzer.

Limiting the Amount of Capture Data that is Saved to Disk

When you set up the Domino system to save captured data to your disk repeatedly, the amount of data that is saved can grow very large. To preserve space on your disk, you can set limits on the total amount of capture data that is saved.

To limit the total amount of capture data:

1. In the Configure Capture to Disk dialog box (Figure 2-14.), click **Data Size**.

   The Data Size dialog box appears (Figure 2-15.), which displays the amount of disk space that is available on your disk.

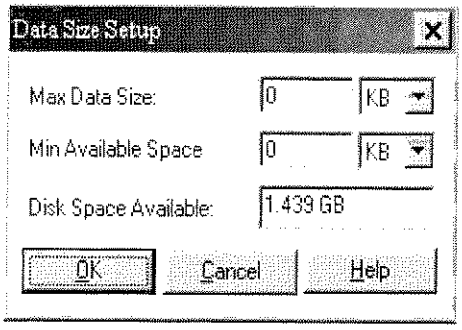


Figure 2-15. Data Size Setup dialog box

2. Take one or both of the following actions:
   - To limit the amount of data to be saved to your disk, specify a maximum amount in **Max Data Size**.
   - To limit the amount of disk space to be used, specify a minimum amount of space to keep available in **Min Available Disk Space**.
3. Click **OK** to return to the Configure Capture to Disk dialog box.

2.5.3 Setting Up the Playback of a Capture File

Use the Internal Playback feature to play back network traffic from a capture file to the Domino analyzer as if it were traffic on a live network. It does not play back traffic onto the network.

Internal Playback is useful when you have captured network traffic and you want to view the same traffic using an application. To use Internal Playback, you set it up in Advanced Setup, where you enable the feature and specify the capture file that you want to use. After you set up the feature, the file that you specified plays back when you start any of the Real Time applications.

NOTE:

The Domino system's Transmit feature enables you to play back a capture file onto the network. See Section Section 6.2, "Playing Back a Capture File."

2.5.3.1 Selecting a Capture File to Play Back

To select a capture file to play back onto the analyzer:

1. In the Advanced Setup dialog box, click the **Internal Playback** tab.

   The Internal Playback setup appears (Figure 2-16.).

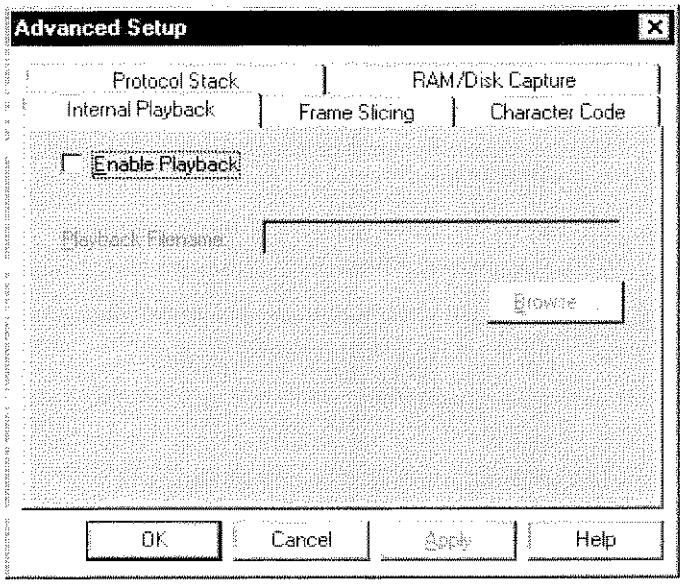


Figure 2-16. Advanced Setup dialog box with the Internal Playback tab selected

2. Select **Enable Playback**.
3. Click **Browse** to specify the path and name of the file that you want.

   The Open Playback File dialog box appears (Figure 2-17.).

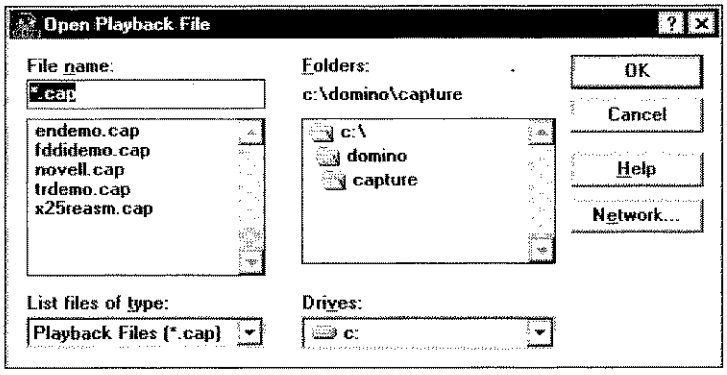


Figure 2-17. Open Playback File

4. Select the capture file that you want to use.
5. Click **OK** to close the Advanced Setup dialog box.

   Playback is enabled. When you start an application, the file you have selected will be played back to the Domino analyzer.

2.5.3.2 Enabling or Disabling the Internal Playback of a Capture File

When you have specified the name of the capture file and enabled the internal playback feature, you may find that you need to disable the playback of the capture file. From the Internal Playback setup, you can disable playback without losing the specified capture file. Then you can enable playback if you want to use it at a later time.

To disable the internal playback of a capture file:

1. In the Advanced Setup dialog box, click the **Internal Playback** tab.

   The Internal Playback setup is displayed (Figure 2-7.).

2. Clear the **Enable Playback** check box.

   The Enable Playback check box and the Playback Filename box are now empty.

To enable the internal playback of a capture file:

1. In the Advanced Setup dialog box, click the **Internal Playback** tab.

   The Internal Playback setup is displayed.

2. Select the **Enable Playback** check box.

   A check mark appears in the Enable Playback check box. The specified capture file and the Browse button are displayed.

2.5.4 Setting Up Frame Slicing

Use frame slicing to shorten the data frame before it is passed to the analyzer for processing. You might want to adjust the frame in this way if you are interested in the frame header and you have no use for the user data contained within the frame.

Frame slicing starts at the beginning of the frame. For example, if you select the 128-byte frame slicing option, all data after the first 128 bytes is discarded before the frame reaches the analyzer.

To set up frame slicing:

1. In the Advanced Setup dialog box, click the **Frame Slicing** tab.

   The Frame Slicing setup appears (Figure 2-18.).

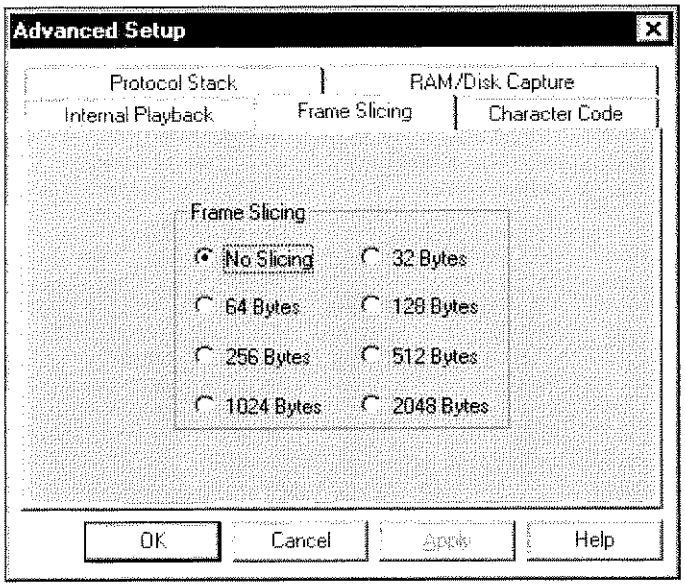


Figure 2-18. Advanced Setup dialog box with the Frame Slicing tab selected

2. Choose one of the frame slicing options.

NOTE:

If you inadvertently slice a frame in the middle of a protocol, that protocol becomes invalid for decoding.

2.5.5 Selecting the Character Code

Advanced Setup provides the option to select the data transmission character code, which controls the way the Domino analyzer interprets the data that it captures from the network.

The character code selection affects the display of the Hexadecimal and Character Trace results windows.

To select the character code:

1. In the Advanced Setup dialog box, click the **Character Code** tab.

   The Character Code setup appears (Figure 2-19.).

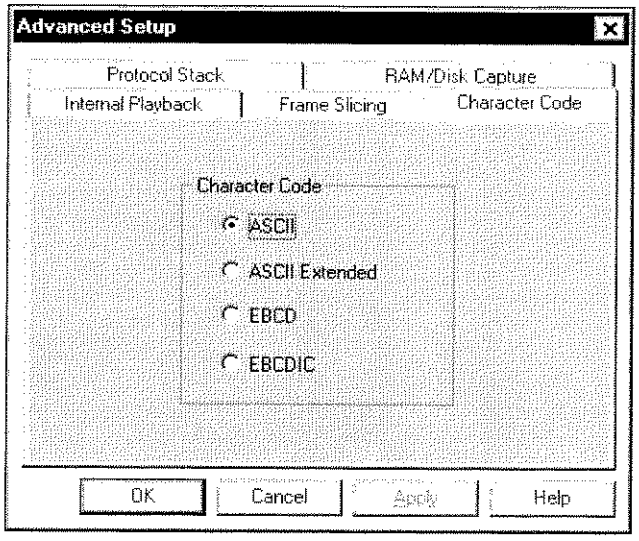


Figure 2-19. Character Code setup

2. Choose one of the Character Code options:
   - ASCII
   - ASCII Extended
   - EBCD
   - EBCDIC

2.6 Setting up the Toolbox

In the Toolbox (Figure 2-20.) at the bottom of the Workbench screen, you can assign buttons to optional Domino applications.

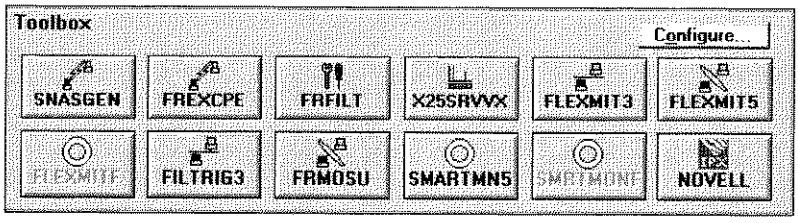


Figure 2-20. Toolbox on the Workbench screen

To configure the Toolbox application buttons:

1. In the Toolbox on the Workbench screen, click **Configure**.

   The Configure Assignable Buttons dialog box appears (Figure 2-21.).

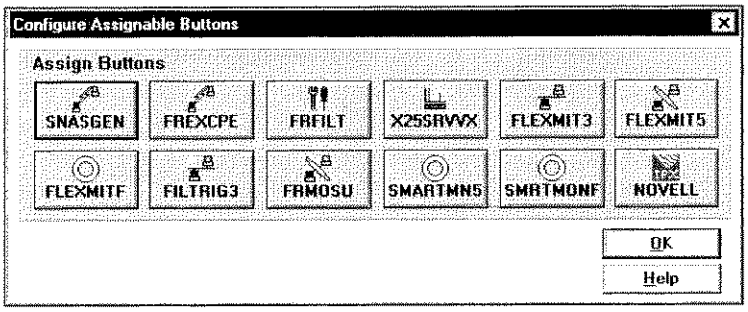


Figure 2-21. Configure Assignable Buttons dialog box

2. Click the button to which you want to assign the application.

   The Configure Single Button dialog box appears (Figure 2-22.).

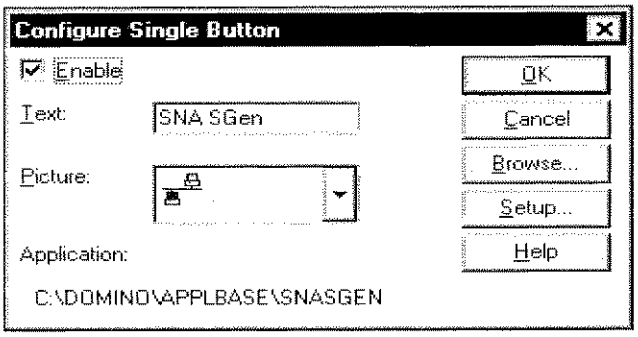


Figure 2-22. Configure Single Button dialog box

3. Select the **Enable** check box; then click **Browse**.

   The Select Application dialog box appears (Figure 2-23.).

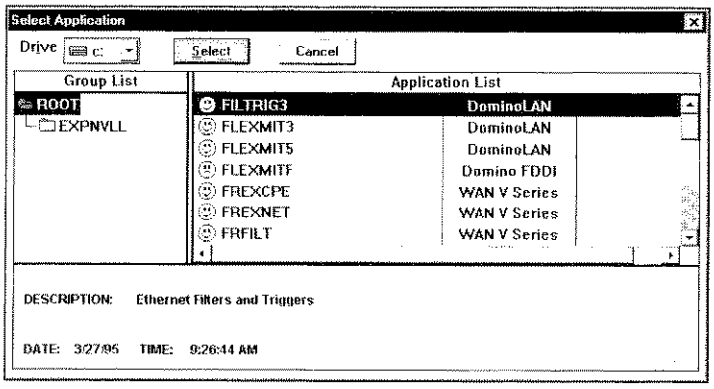


Figure 2-23. Select Application dialog box

4. Select an application from the **Application List** and click **Select**.

   If the application is not listed, locate it by doing one of the following:

   - select a new application group from the **Group List**
   - select a new drive.

   When you click **Select**, the dialog box closes and you return to the Configure Single Button dialog box. The name of the application that you selected appears in the **Text** box and **Application** displays the path.

5. In the **Picture** box, select the picture that you want to display on the button; then click **OK**.

   You return to the Configure Assignable Buttons dialog box.

6. Repeat steps 2 through 5 for each button to which you want to assign an application.

7. When you finish assigning buttons, click **OK**.

   You return to the Workbench screen. The buttons in the Toolbox reflect the application assignments that you configured.

2.6.1 Enabling or Disabling an Application Button

Occasionally, you might find that it is useful to disable a configured Toolbox button. You can disable a button without losing its assigned application, text, or icon. Then you can enable the application button when you want it to be visible again.

To disable or enable a configured application button:

1. In the Toolbox on the Workbench screen, click **Configure**.

   The Configure Assignable Buttons dialog box appears (Figure 2-21.).

2. Click the button that you want to disable or enable.

   The Configure Single Button dialog box appears (Figure 2-22.).

3. Clear or select **Enable**; then click **OK**.

   You return to the Configure Assignable Buttons dialog box.

4. Click **OK** to return to the Workbench screen.

2.6.2 Changing a Picture on an Application Button

You can change the picture or icon that is assigned to a Toolbox application button.

To change a picture on a button:

1. In the Toolbox on the Workbench screen, click **Configure**.

   The Configure Assignable Buttons dialog box appears (Figure 2-21.).

2. Click the button that you want to change.

   The Configure Single Button dialog box appears (Figure 2-22.).

3. In the **Picture** box, scroll through to select the picture that you want to use; then click **OK**.

   You return to the Configure Assignable Buttons dialog box.

4. Click **OK** to return to the Workbench screen.

2.6.3 Changing the Application Assigned to a Button

You can change the application that is assigned to a Toolbox button.

To change the application that is assigned to a button:

1. In the Toolbox on the Workbench screen, click **Configure**.

   The Configure Assignable Buttons dialog box appears (Figure 2-21.).

2. Click the button that you want to change.

   The Configure Single Button dialog box appears (Figure 2-22.).

3. Click **Browse**.

   The Select Application dialog box appears (Figure 2-23.).

4. Select the application that you want to assign and click **Select**.

   If the application that you want to assign is not listed in the **Application List**, locate it by doing one or more of the following:

   - In the **Group List**, select a new application group
   - Select a new drive

   When you click **Select**, the disalog box closes and you return to the Configure Single Button dialog box.

5. Change the text and picture that are specified in the boxes of the Configure Single Button dialog box. This is necessary because the **Text** box and **Picture** box will still contain the values that were previously assigned to the button.
6. Click **OK**.

   You return to the configure Assignable Buttons dialog box.

7. Click **OK** to return to the Workbench screen.

2.6.4 Changing the Text on a Button

When you assign an optional Domino application to a button, the system automatically uses the application's filename as the text that appears on the button. If you like, you can change the text that appears on a button.

To change a button's text:

1. In the Toolbox on the Workbench screen, click **Configure**.

   The Configure Assignable Buttons dialog box appears (Figure 2-21.).

2. Click the button that you want to change.

   The Configure Single Button dialog box appears (Figure 2-22.).

3. In the **Text** box, type the text that you want to appear on the button; click **OK**.

   You return to the configure Assignable Buttons dialog box.

4. Click **OK** to return to the Workbench screen.

Because a proportional-spaced font is used, the length of the text on a button varies depending on the width of the characters that you use. Typically, an application button can accommodate text that is up to 7 characters long.

You can assign an Alt+combination to an application button by inserting the ampersand symbol (&) in front of the character that you want to use in the application's text. For example, to assign the Alt+35 combination to the BERT_V35 application button, type BERT_V&35 in the text box.

2.7 Enabling the Display of Symbolic Names

You can enable and disable the feature that displays names instead of addresses in windows that provide station information.

To enable or disable the display of symbolic names:

1. From the menu bar on the Workbench screen, choose **Utilities/Manage Symbolic Names**.

   The Symbolic Name Setup dialog box appears (Figure 2-24.).

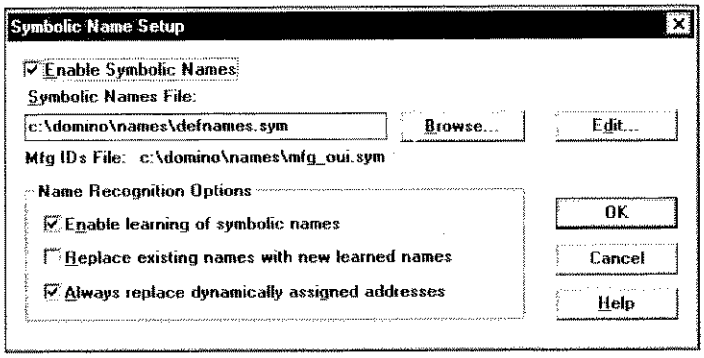


Figure 2-24. Symbolic Name Setup dialog box

2. Select or clear the **Enable Symbolic Names** check box.
3. If you are enabling the feature, verify that the file listed in **Symbolic Names File** is the one that you want to use and check any **Name Recognition Options** that you want. Then choose **OK**.

   The dialog box closes and you return to the Workbench screen. Stations are identified by names instead of addresses in windows that provide station information.

NOTE:

The Manage Symbolic Names command is also available from the Examine **Buffer** menu and the **Control** menu in Capture, Monitor, or Transmit. To learn more about managing symbolic names, refer to the Help for the Domino software.

2.7.1 Enabling the Analyzer to Learn Symbolic Names

The Domino analyzer is equipped to learn the names associated with the addresses of stations that it detects and to add those names and addresses to the symbolic names file.

The symbolic names feature offers options to replace existing names with new learned names and to replace dynamically assigned addresses.

To enable the analyzer to learn symbolic names:

1. From the menu bar on the Workbench screen, choose **Utilities/Manage Symbolic Names**.

   The Symbolic Name Setup dialog box appears (Figure 2-24.).

2. Select **Enable Symbolic Names** and verify that the file that you want is specified in **Symbolic Names File**.

3. Under **Name Recognition Options**, select **Enable learning of symbolic names**.

4. If you want to replace an existing name when the analyzer learns a new name for an address, select the corresponding check box.

   If you have edited the symbolic names file to provide station names that you recognize easily, clear the check box to ensure that your names remain as you want them.

5. If you want to replace dynamically assigned addresses, select the corresponding check box.

   In some networks, addresses are assigned dynamically each time a station logs on. If your network assigns addresses dynamically, be sure to select this option. If you do not, duplicate address entries are likely to be added to your symbolic names file.

6. Choose **OK**.

   The dialog box closes and you return to the Domino screen in which you were working. The analyzer learns the names associated with the stations that it detects and adds the station names and addresses to the symbolic names file.

NOTE:

The Manage Symbolic Names command is also available from the Examine **Buffer** menu and the **Control** menu in Capture, Monitor, or Transmit. To learn more about managing symbolic names, refer to the Help for the Domino software.

2.8 Displaying Software Version Number Information

Use the About Domino Internetwork Analyzer command to display the software version information for your Domino analyzer to determine whether you have the latest version of the Core software, network interface software, and protocol software.

The About Domino Internetwork Analyzer dialog box also displays:

- the copyright notice
- the analyzer board
- the interface board
- the interface module (WAN only)

To display software version information:

♦ From the menu bar on the Workbench screen, choose **Help/About Domino Internetwork Analyzer**.

Use the scroll bar to scroll through the software version number information.

3. Capturing Network Traffic

NOTE:
This chapter describes how to capture traffic and save it to a file. To learn how to set up the system for automatic captures to be saved in a series of files on your computer's disk, see Section 2.5.2.3, "Capturing Traffic to Your Computer's Disk."

The Capture application records live traffic off the network and stores it in a RAM capture buffer on the Domino analyzer. For the DominoFDDI, DominoLAN and DominoWAN (V-series, E1, and T1) analyzers, Capture provides filtering capability to enable you to limit the frames that are captured to those of particular interest. It also provides the ability to define as a trigger event the receipt of a frame that matches specified criteria. When you set up a trigger event and define an action to occur in response to the trigger, you can compare network behavior before and after the trigger event.

When you capture traffic, you can save the traffic that is stored in the capture buffer to a file. With a capture file, you can:

- Open the file in the Examine application to study the traffic in detail.
- Play back the traffic from the capture file as if it were live network traffic. Internal playback is useful when you want to review the traffic in the Monitor results windows or analyze it with the features available in one of the Toolbox applications.
- Play back the capture file while simultaneously transmitting its contents onto the network and back to the Domino for further analysis. To learn about external playback, see Section 6.2, "Playing Back a Capture File."

3.1 Starting the Capture Application

Capture is one of the four main Domino functions that are available from the Workbench screen, which is the first screen you see when you start the Domino software. To learn more about the Workbench screen and how to prepare to use an application, see Section 1.3, "The Domino Workbench."

To start the Capture application:

- Choose Capture from the Workbench menu or click the Capture button.

  Capture starts, opens a RAM capture buffer for each enabled Domino, and begins capturing traffic from the network. A default desktop is displayed that consists of interface-specific results windows. If you make changes to the desktop, your changes are saved and the modified desktop is restored the next time you start Capture.

If you are using a DominoLAN, DominoFDDI, or DominoWAN analyzer, the Filter/Trigger dialog box is automatically displayed. This enables you to set up filters and triggers while data is being captured, although you must stop and restart data capture to activate the filters or triggers that you set up.

3.2 Using Capture Filters and Triggers

When you use the Capture application to capture network data, all of the traffic that is received by the analyzer is placed in the capture buffer. This can result in a large accumulation of data, only a small portion of which may be relevant to an event that you are monitoring or a problem that you are troubleshooting. The Capture application for the DominoLAN, DominoFDDI, and DominoWAN analyzers provides filtering capability to enable you to limit the frames that are captured to those of particular interest.

Filters are conditions that you define to limit the amount of network traffic that is captured. When a filter is enabled, incoming frames are either captured or discarded according to whether they meet the filter conditions. Filtering network traffic allows you to isolate and save only those frames that are significant to a specific problem or event. The Capture Filter setup allows you to specify address, protocol, byte pattern, frame size, and error type as filter conditions that can be used singly or in combination.

A trigger is an event that you define that causes an action to occur. To set up a trigger, you specify one or more frame characteristics as trigger conditions. When a frame that matches the specified conditions is captured, it activates the trigger action that you select, such as stopping the capture buffer or running a Windows program.

When you use a trigger and a filter concurrently, the filter that you define must include (filter in) the type of frame that you define as your trigger. If the filter discards the trigger frame, the trigger condition can never be met because the triggered frame isn't captured.

3.2.1 Logical Combination of Filter Conditions

To ensure that the filter that you set up traps the network traffic that you are interested in, you need to understand how the Capture Filters interact with each other. The basic rule is:

- conditions on the same tab of the Filter Setup are logically ORed
- conditions on each tab are logically ANDed with conditions on the other tabs

For example:

- If you choose to filter IP traffic from the Protocol tab, and specify three addresses on the Address page, the filter will trap IP protocol frames that contain any one of the addresses that you selected (IP AND Address 1 OR Address 2 OR Address 3).
- If you choose IP and IPX protocols on the Protocol tab, and specify three addresses on the address tab, the filter will trap either IP protocol frames that contain one of the three addresses, OR IPX protocol frames that contain one of the three addresses.
- But, if you choose IPX on the Protocol tab AND specify an IP address on the Address tab, you have logically ANDed two mutually exclusive conditions, and no frames will be trapped by the filter.

3.2.2 Setting Up Capture Filters

Setting up a Capture filter consists of specifying global filter conditions, which apply to the entire filter setup, and one or more specific filter conditions. The specific filter conditions are:

Address	You specify the frame type (either DLC, IP, or IPX) and whether to filter on a specific source address, destination address, or both.
Protocol	You can select up to four protocols on which to filter.
Match	You can filter on three match options: Pattern, Size, and Error. You can specify as many as four filter conditions in one match filter.
WAN	Allows you to filter on Frame Relay or HDLC protocol frame characteristics.

To set up capture filters:

1. From the Capture menu bar, choose **Filters/New**.

   The Filter/Trigger dialog box appears (Figure 3-1.).

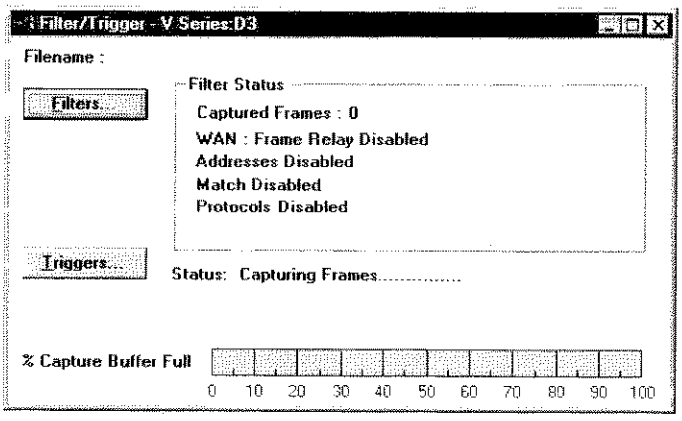


Figure 3-1. Filter/Trigger dialog box

2. Click **Filters**.

   The Filters Setup dialog box appears.

3. Set up the global filter parameters using the options on the General tab, shown in Figure 3-2., to specify:

   - Whether to include or exclude filtered frames from the capture buffer.
   - Which encapsulation method to specify as a filter condition. The options are: Ethertype, LLC SAP, or SNAP. Ethertype is not an encapsulation method for Token Ring or FDDI; the option is not available when you are setting up a Token Ring network filter or a FDDI network filter.

4. Set up the address, protocol, and match filters using the options on the Addresses, Protocol, and Match tabs.

   If you are using a DominoWAN analyzer, use the options on the WAN tab to filter HDLC or Frame Relay frame characteristics, and to ensure that the filter setup corresponds to the implementation of HDLC or Frame Relay on your network.

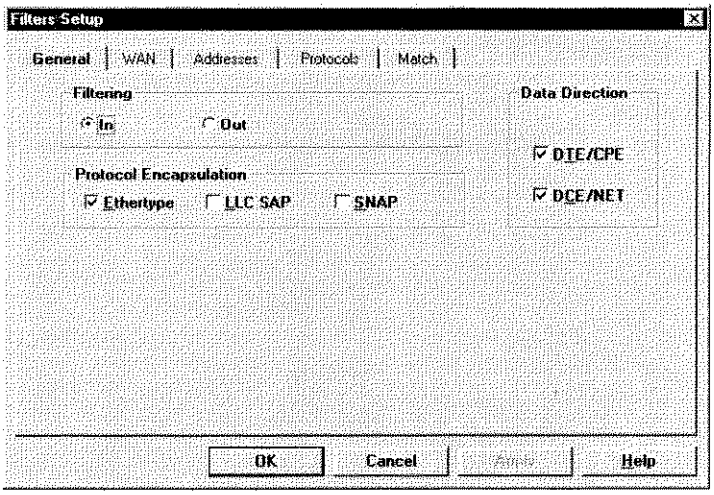


Figure 3-2. General tab, Filters Setup dialog box

5. When you have defined and enabled all of the filters that you want to use, choose **Filters/Start** from the Capture menu bar to begin capturing filtered traffic.

NOTE:

The options on the General tab of the Filters Setup dialog box specify conditions that work in conjunction with any filters in the current setup. Neither of the settings on the General tab have any effect unless an Address, Protocol, Match, or WAN filter is enabled.

3.2.2.1 Setting Up an Address Filter

The address filter enables you to filter network traffic according to the source and destination of the frames. If traffic flows in both directions between two addresses, you can specify either address as source or destination, and then use the bi-directional option to capture all traffic between the two.

To set up an address filter:

1. On the Filters Setup dialog box, shown in Figure 3-2., click the Addresses tab.
2. Click **Add**.

   The Address Information dialog box appears (Figure 3-3.).

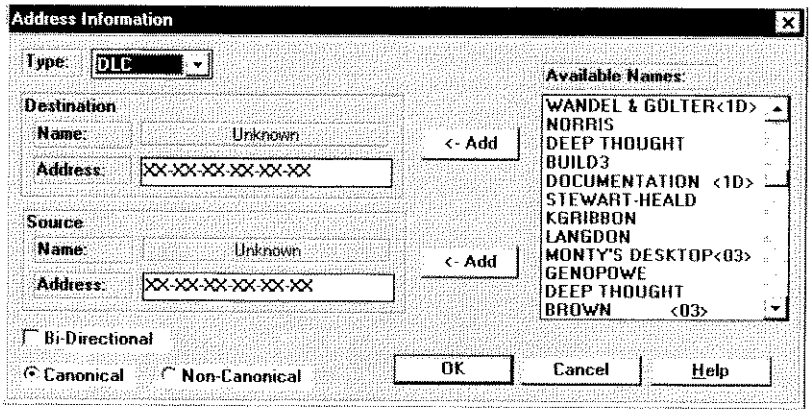


Figure 3-3. Address Information dialog box

3. In **Type**, select the address type: DLC, IP, or IPX.

   Notice that the address format changes depending on the address type that you select.
4. In **Source Address**, do one of the following:
   - Type the source address of the frames you want to filter.
   - Select a name from the **Available Names** list and click **Add**.
5. In **Destination Address**, do one of the following:
   - Type the destination address of the frames you want to filter.
   - Select a name from the **Available Names** list and click **Add**.
6. Select the format in which you would like the addresses to be displayed. The options are:

Canonical	The default address format for Ethernet. The canonical address format displays the address as six groups of two hexadecimal digits, separated by dashes.
Non-canonical	The default format for Token Ring and FDDI. The non-canonical address format displays the address as six groups of two hexadecimal digits, separated by colons.

7. To make this filter active when you start capturing frames, select the **Enable** check box.
8. Click **OK** to confirm your selections and return to the Filter/Trigger dialog box.

If the **Destination** and **Source** lists do not display the names that you want to see, be sure that the correct symbolic names file is selected in the Symbolic Name Setup dialog box. Even if you have disabled symbolic names, the selected file controls the entries that appear in this list. If the list grows too long and contains entries that you never use, delete the unnecessary entries. See the online Help topic, "Managing Symbolic Names".

3.2.2.2 Setting Up a Protocol Filter

The protocol filter enables you to filter network traffic for up to four protocols.

To set up a protocol filter:

1. On the Filters Setup dialog box shown in Figure 3-2., click the Protocols tab (Figure 3-4.).

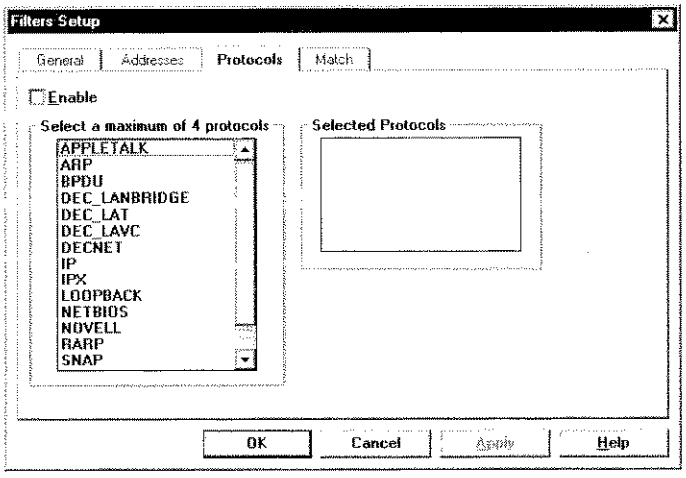


Figure 3-4. Protocols tab, Filters Setup dialog box

2. On the Protocols tab, select up to four protocols from the list of protocols.

   Each protocol that you select is listed in the **Selected Protocols** box.

3. Token Ring only: To specify that MAC frames are to be trapped by the filter, select the **Include MAC Frames** check box.

   FDDI only: To specify that SMT frames are to be trapped by the filter, select the **Include SMT frames** check box.

4. To make this filter active when you start capturing frames, click **Enable**.

5. Click **OK** to confirm your selections and return to the Filter/Trigger dialog box.

3.2.2.3 Setting Up a Match Filter

The match filter enables you to screen frames for three characteristics:

- For DominoLAN and DominoFDDI analyzers: a 6-byte pattern that occurs at a specific offset into the frame. For DominoWAN analyzers: a 64-byte pattern at a specific offset.
- The size of the frame
- An error condition

You can set up a match filter that consists of up to four logically combined filter conditions using one or all of the match options. For example, you could filter for frames that meet the following criteria:

Pattern 00-80-16-8E occurring at offset 2

OR	Pattern 00-C0-C0-D0 occurring at offset 15
AND	Bad CRC error condition
AND NOT	more than 2000 bytes long

The Match tab of the Filter Setup enables you to create filters to match almost any network analysis situation by allowing you to specify byte-level filter criteria.

For example, you can create a filter to identify Ethernet collisions on your network. On the Match tab, set a pattern match for AAAA and 5555 (the patterns formed by the Ethernet preamble, in hexadecimal) at various offsets, and OR the matches together. Filtering on the preamble pattern at larger offsets will trap collisions occurring later in the frame.

To set up a match filter:

1. On the Filters Setup dialog box, click the Match tab (Figure 3-5.).

   The options on the Match tab allow you to specify up to four filter conditions.

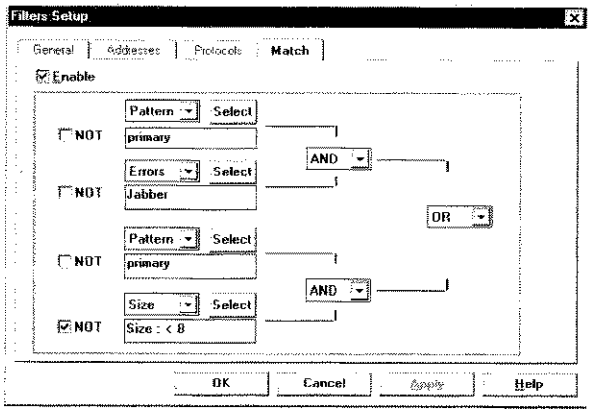


Figure 3-5. Match tab, Filters Setup dialog box

2. For the first filter condition, select the match option: **Pattern**, **Size**, or **Error**.
3. Click **Select** to display the setup dialog box for the match option that you selected.
4. Specify the pattern, frame size, or network error on which you want to filter, and click **OK** to return to the Match tab.
5. Repeat steps 2, 3, and 4, for each filter condition that you want to set up.
6. To make this filter active when you start capturing frames, click **Enable**.
7. Click **OK** to confirm your selections and return to the Filter/Trigger dialog box.

3.2.2.4 Setting Up a WAN Filter

The WAN filter options differ depending on whether you are filtering HDLC or Frame Relay traffic. Both the HDLC and the Frame Relay filter setups require that you specify protocol setup information in addition to the frame characteristics that you choose as filter conditions. The protocol setup parameters in the filter setup are the same as those that you specified when you set up either HDLC or Frame Relay on the protocol stack; the values you select most correspond to the implementation of HDLC or Frame Relay on your network.

To set up a WAN filter for HDLC frames:

1. From the Filter/Trigger dialog box, click **Filters**.

   The Filters Setup dialog box appears.
2. Click the WAN tab.
3. In the **Layer 2** box, choose **HDLC**.

   The options on the dialog box change to reflect your selection.
4. To filter HDLC frames according to frame type, select one or more of the frame type options from the list.
5. Set the address size, modulo, and encapsulation type to correspond to the implementation of HDLC on your network.
6. To specify that this filter will be active when you start capturing frames, click **Enable**.
7. Click **OK** to confirm your selections and return to the Filter/Trigger dialog box.

To set up a WAN filter for Frame Relay frames:

1. From the Filter/Trigger dialog box, click **Filters**.

   The Filters Setup dialog box appears.
2. Click the WAN tab.

3. In the **Layer 2** box, choose **Frame Relay**.

   The options on the dialog box change to reflect your selection.

4. Set the **Encapsulation Type** and **MAC Layer** options to correspond to the implementation of Frame Relay on your network.

5. To filter frames addressed to one or more DLCIs, select the DLCI from the **DLCI List**.

   The **Add**, **Edit**, and **Delete** options on the dialog box enable you to make changes to the DLCI list.

6. To trap frames addressed to the selected DLCI that will provide information about congestion on the network, select one or more of the **Congestion** filter options: **FECN**, **BECN**, or **DE**.

7. To filter frames addressed to the selected DLCI according to the setting of control bytes, select one or more of the following options: **UI**, **XID**, **C/R bit**.

8. To specify that this filter will be active when you start capturing frames, click **Enable**.

9. Click **OK** to confirm your selections and return to the Filter/Trigger dialog box.

NOTES:

- The congestion and control byte options only function as filter conditions in relation to a DLCI address selection.
- In order for the analyzer to decode the filtered frames, you must have Frame Relay or HDLC loaded on the protocol stack. To learn how to load the protocol stack, see Section 2.5.1, "Setting Up the Protocol Stack."

3.2.3 Setting Up Triggers

A trigger is an event that you define that causes an action to occur. To set up a trigger, you specify one or more frame characteristics as trigger conditions. When a frame that matches the specified conditions is captured, the trigger action is activated.

When you use a trigger and a filter concurrently, the filter that you define must include (filter in) the type of frame that you define as your trigger. If the trigger is not filtered in, the filter discards the trigger frame and the trigger condition can never be met because the triggered frame isn't captured.

3.2.3.1 Setting Up a Trigger Condition

The trigger conditions that you can set up are the same as the match filter conditions. You set the trigger up in the same manner as you do the match filter--by specifying that an incoming frame must match certain frame characteristics (pattern, frame size, or error type).

To set up a trigger condition:

1. From the Filter/Trigger dialog box, click **Triggers**.

   The Triggers dialog box appears.

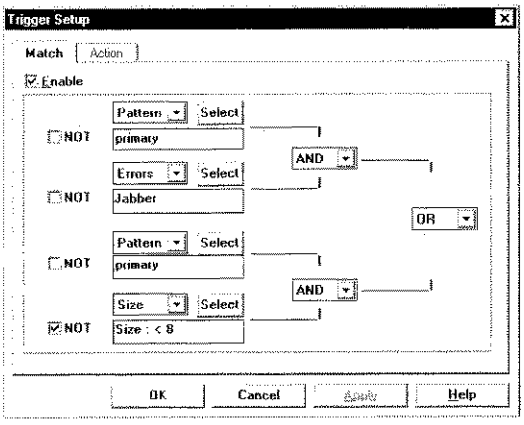


Figure 3-6. Match tab, Trigger Setup dialog box

2. Click the Match tab (Figure 3-6.).

   The options on the Match tab allow you to specify up to four trigger conditions.

3. For the first trigger condition, select the match option: **Pattern**, **Size**, or **Error**.
4. Click **Select** to display the setup dialog box for the match option that you selected.
5. Specify the pattern, frame size, or network error that you want to use as a trigger, and click **OK** to return to the Match tab.
6. Repeat steps 3, 4 and 5 for each trigger condition that you want to set up.
7. To make this trigger active when you start capturing frames, click **Enable**.
8. Click **OK** to confirm your selections and return to the Filter/Trigger dialog box.

3.2.3.2 Setting Up a Trigger Action

After you have set up a trigger, you select the action that you want to occur when the trigger frame is received.

Trigger actions often require some additional setup. The setup options appropriate to the action you select are displayed when you select the action. For example, when you select **Save Capture Buffer**, you can specify the percentage of the capture buffer that you want to fill with captured traffic after the trigger event occurs. Continuing to collect data in the capture buffer after the trigger event occurs provides the opportunity to examine and compare the quality of network traffic from before and after the event.

To set up a trigger action:

1. From the Filter/Trigger dialog box, click **Triggers**.

   The Triggers dialog box appears.

2. Click the Action tab (Figure 3-7.).

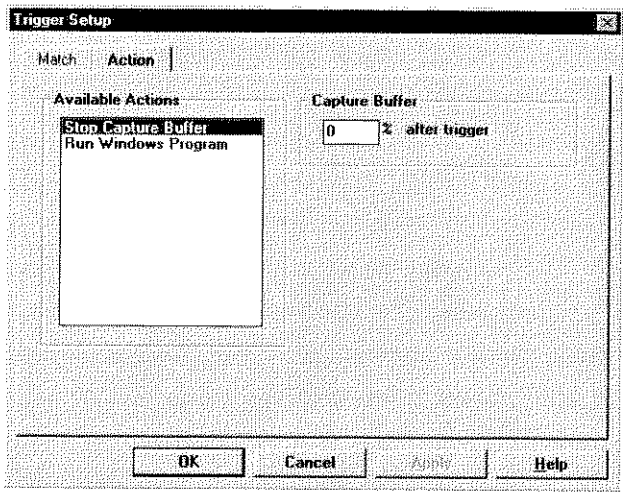


Figure 3-7. Action tab, Trigger Setup dialog box

3. From the **Available Actions** box, select the action. The options are:

   Stop Capture Buffer

   Run Windows Program

4. Do one of the following:

   - If you select **Stop Capture Buffer**, specify the percentage of the capture buffer that you want to fill with captured traffic after the trigger event occurs.

     Stop Capture Buffer enables you to obtain a snapshot of network traffic before and after the trigger even occurs. If you specify that you want to fill 50 percent of the capture buffer after the event, and before the event occurs

28 percent of the capture buffer is full, 78 percent of the capture buffer will be filled when data capture stops.

- If you select **Run Windows Program**, click **Browse** to open the Open Program File dialog box and choose an executable program that will run when the trigger event occurs.

5. Click **OK** to return to the Filter/Trigger dialog box.

3.2.4 Ending Filter Setup

When you have finished setting up the filters and triggers for a session, or if the Filter/Trigger dialog box is open and you do not want to set up any filters, you end filter setup by closing the Filter/Trigger dialog box.

To end filter setup:

♦ From the Capture menu bar, choose **Filters/Close**.

The Filter/Trigger dialog box closes.

3.2.5 Starting and Stopping the Capture of Network Traffic

When you have completed a filter setup, or if you have decided not to implement capture filters and simply want to begin capturing network traffic, you can start data capture from the Filters menu.

To start capturing traffic:

♦ From the Capture menu bar, choose **Filters/Start**.

When data capture begins, the **Filtered Frames** field on the Filter/Trigger dialog box reports the number of filtered frames that have been captured. If no filters are enabled, this field reports the number of frames that have been captured.

While the analyzer is capturing frames, a scale on the Filter/Trigger dialog box indicates the percentage of the capture buffer that has been filled. When the buffer is full, the content of the buffer is overwritten with newly captured frames. The overwritten portion of the buffer is indicated by a change in color on the percentage scale..

Shortcut:

You can also use the Start button  on the Capture toolbar to start data capture.

To stop capturing traffic:

- From the Capture menu bar, choose **Filters/Stop.**

> **Shortcut:**
>
> You can also use the Stop button  on the Capture toolbar to stop data capture.

3.2.6 Clearing the Capture Buffer

To clear the capture buffer:

- From the Capture menu bar, choose **Filters/Flush.**

> **Shortcut:**
>
> You can also use the Flush button  on the Capture toolbar.

3.3 Working with Filter/Trigger Setup Files

The Capture **Filters** menu provides file management options, so that you can save and reuse the filter and trigger setups that you create. The default file type of the setup file varies, depending on the network interface type. For example, the default file type for Ethernet filter/trigger setup files is .FT3. The default file type for Token Ring filter/trigger setup files is .FT5.

To open a filter setup file:

1. From the Capture menu bar, choose **Filters/Open.**

   The Open dialog box appears.

2. In **File Name**, select the name of the filter setup file that you want to use; then click **OK**.

   The Filter/Trigger dialog box appears. The status display field shows whether any filters are enabled in the newly loaded setup.

To save a filter setup to a new filter/trigger setup file:

1. From the Capture menu bar, choose **Filters/Save.**

   The Save As dialog box appears.

2. In **File Name**, type a file name to use for the new filter/trigger setup file.

3. To save the file to a different drive or directory, use the **Directory** and **Drive** options to specify where you want to store the file.
4. Click **OK**.

To save a filter setup to an existing filter/trigger setup file:

1. From the Capture menu bar, choose **Filters/Save As**.

   The Save As dialog box is displayed.
2. In **File Name**, select the name of an existing filter/trigger setup file from the list.
3. To save the file to a different drive or directory, use the **Directory** and **Drive** options to specify where you want to store the file.
4. Click **OK**.

4. Monitoring Network Traffic

The Monitor application provides a comprehensive view of the activity on your network. It helps you to track network performance and it discovers and reports the most common network anomalies. Monitor command options enable you to view both network-level and station-specific traffic analysis data.

4.1 Starting the Monitor Application

Monitor is one of the four main functions that are available from the Workbench screen, which is the first screen you see when you start the Domino software. To learn more about the Workbench screen and how to prepare to use an application, see Section 1.3, "The Domino Workbench."

To start the Monitor application:

- Choose Monitor from the Workbench menu or click the Monitor button.

  Monitor starts and begins monitoring the traffic on the network. A default desktop is displayed that consists of interface-specific results windows. If you make changes to the desktop, your changes are saved and the modified desktop is restored the next time you start Monitor.

Figure 4-1 illustrates the Monitor screen with two open results windows.

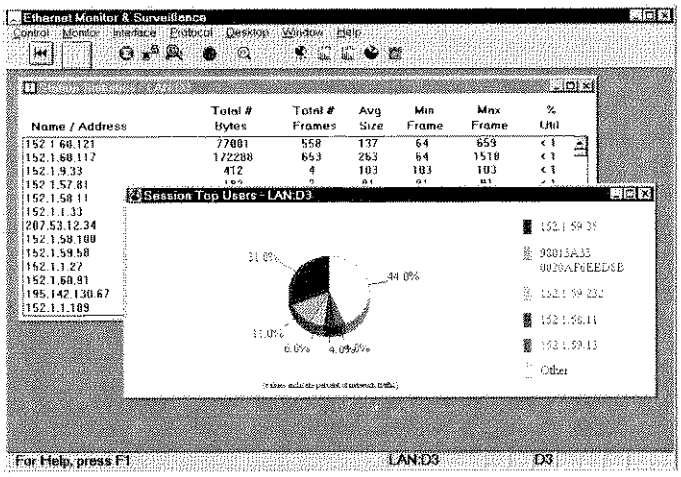


Figure 4-1. Sample Monitor results windows

4.2 Monitoring a Token Ring Network in Passive Mode

The DominoLAN analyzer provides a passive mode of operation that enables you to use the monitor application to unobtrusively monitor the traffic on a Token Ring network. In passive mode, the DominoLAN analyzer is physically connected to the network, but is not an active station and does not transmit any frames onto the ring.

Passive mode allows the analyzer to connect to a beaconing ring, thereby increasing your ability to quickly locate the cause of the beacon condition.

To set up the DominoLAN to operate in passive mode:

1. From the Workbench, click the **Setup** button for the DominoLAN connected to the Token Ring network you want to monitor.
2. From the DominoLAN Main Setup dialog box, select one of the Token Ring interface connector types. Verify that the Token Ring is specified as the network interface type; then click **Manual**.

   The Token Ring Network Interface Setup dialog box is displayed.
3. In **Test Mode**, select **Monitor** and click **OK**.

   You return to the DominoLAN Main Setup dialog box.
4. Click **OK** to save your interface setup selections and return to the Workbench.
5. From the Workbench, click **Monitor**.

   The Monitor application starts.

4.3 Viewing Station-Specific Statistics

Monitor provides the following options for obtaining statistics for individual stations on your network:

Display Station List	Lists the top network users identified by address with the following statistics for each user: • Total bumber of bytes • Total number of frames • Average frame size • Minimum frame size • Maximum frame size • Percent of network utilization
Sort by Lineside (DominoWAN analyzers only)	Sorts the station list according to whether the station is transmitting from the DTE or DCE side of the line
Sort by Usage	Sorts the station list by percentage of network use, in descending order
Top Users	Displays a pie chart showing the top network users and the percentage of network traffic associated with each, for one of the following time periods: • current (the last 30-second interval) • session (since monitoring started or statistics were reset)

To display the station-specific statistics:

1. From the menu bar on the Monitor screen, choose **Monitor/Station**.
2. From the Station sub-menu, choose how you want to view the station-level statistics:
   - **Display Station List** shows data in tabular format
   - **Top Users** presents the current or session station-level data in graphic format

3. If you are viewing the station list, you can choose one of the sorting options from the **Monitor/Station** menu to modify the display of the station list.
   - **Sort by Lineside** (DominoWAN analyzers only)
   - **Sort by Usage**

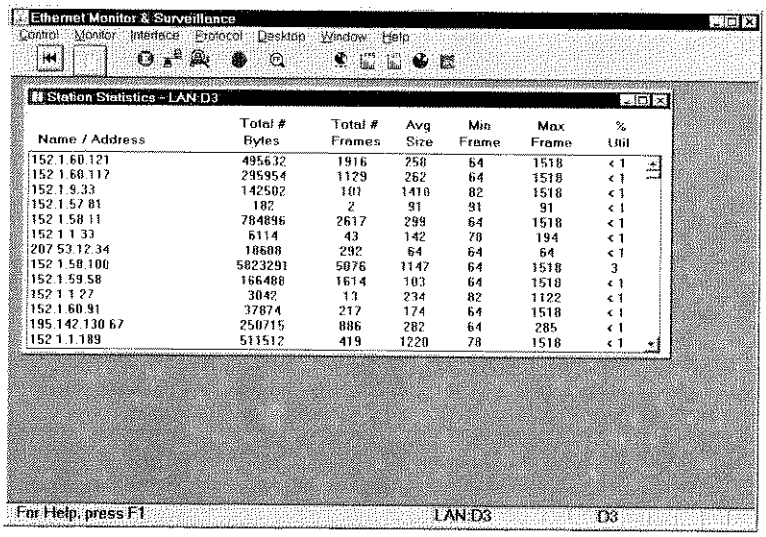


Figure 4-2. Sample station statistics window

4.4 Viewing Network Utilization Statistics

The Network Utilization graph displays network utilization statistics in bar graph format. It indicates the current utilization and displays the utilization for each interval during the monitoring period in the bar graph.

To learn how to scroll through the graph using the keyboard or the mouse, see Section 4.15, "Examining Captured Network Traffic." To learn how to change the time interval used for displaying the graph, see Section 4.16, "Scrolling Through Graphs."

4.4.1 Displaying a Network Utilization Graph

To display a Network Utilization graph:

♦ From the **Monitor** menu, choose **Network/Utilization Graph**.

The Network Utilization graph appears (Figure 4-3.).

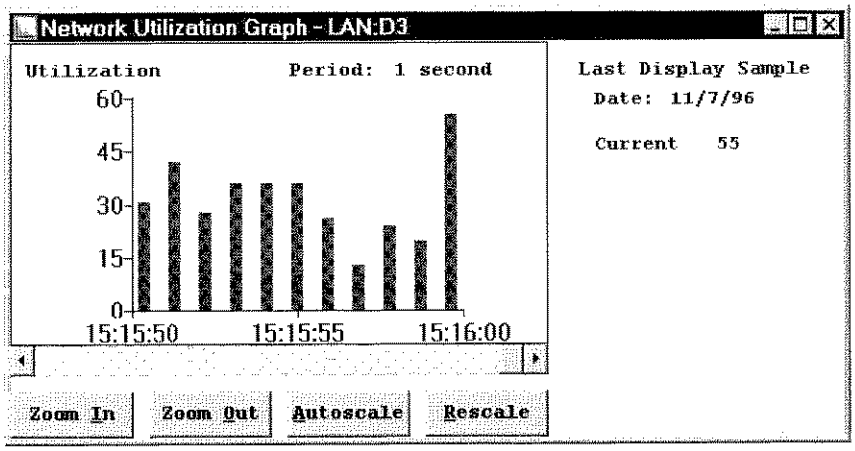


Figure 4-3. Sample Network Utilization Graph

Shortcut:
Use the Network Utilization button on the Monitor toolbar.

4.4.2 Changing the Network Utilization Scale

The utilization in the Network Utilization graph (Figure 4-3.) is displayed as a percentage. Monitor automatically adjusts the scale of the graph to fit the largest network utilization value that has been recorded during the monitoring period. However, if there are peaks of unusually high network utilization, this scale might be inappropriate for viewing the rest of the network utilization statistics. You can scale the graph based on the period that you are currently viewing.

To change the network utilization scale to fit the displayed period:

- Click **Rescale**.

  The network utilization scale adjusts to fit the network utilization statistics that are currently displayed in the Network Utilization graph.

To autoscale the network utilization scale:

- Click **Autoscale**.

  The network utilization scale adjusts to match the scope of all of the network utilization statistics gathered during the monitoring period.

4.5 Viewing Protocol Distribution Statistics

Use the Protocol Distribution window and pie chart to view a list of the current protocols, the percentage of the total traffic generated by each protocol, and a pie chart of those percentages.

4.5.1 Displaying the Protocol Distribution Window

The Protocol Distribution window displays a list of the protocols currently detected in the network traffic and shows the percentage of the total traffic that contains each of the detected protocols.

To display the Protocol Distribution window:

- From the **Monitor** menu, choose **Network/Protocol Distribution**.

  The Protocol Distribution window appears (Figure 4-4.).

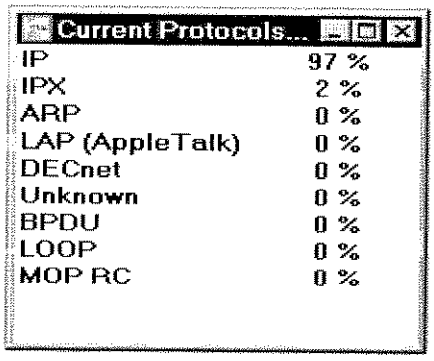


Figure 4-4. Sample Protocol Distribution window

4.5.2 Displaying the Protocol Distribution Pie Chart

The Protocol Distribution pie chart displays protocol distribution statistics in pie chart format. This pie chart indicates the percentage of the total network traffic that contains each of the protocols detected on the network.

To display the Protocol Distribution pie chart:

- From the **Monitor** menu, choose **Network/Protocol Pie Chart**.

  The Protocol Distribution pie chart appears (Figure 4-5.).

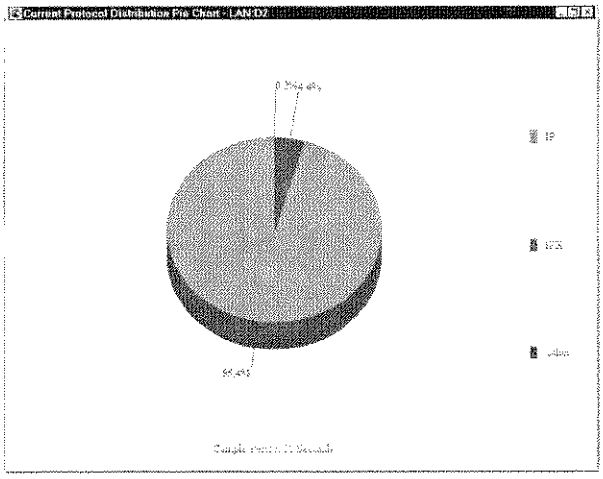


Figure 4-5. Sample Protocol Distribution pie chart

Shortcut:
Use the Protocol Distribution button on the Monitor toolbar.

4.6 Viewing Frame Size Distribution Statistics

Use the Frame Size Distribution window and area graph to view a list of frame size ranges, their percentage of the total frames, and the statistics in area graph format.

4.6.1 Displaying the Frame Size Distribution Window

The Frame Size Distribution window displays a list of frame size ranges appropriate for the type of network being monitored. It also indicates the percentage of the total frames that fall within each frame size range.

To display the Frame Size Distribution window:

- From the **Monitor** menu, choose **Network/Frame Size Distribution**.

  The Frame Size Distribution window appears (Figure 4-6.).

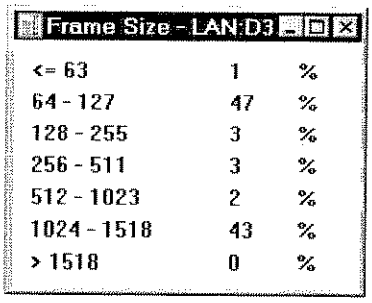


Figure 4-6. Sample Frame Size Distribution window

4.6.2 Displaying the Frame Size Distribution Area Graph

The Frame Size Distribution area graph displays frame size statistics in area graph format. This area graph indicates the percentage of the total frames that fall within specific frame size ranges.

To display the Frame Size Distribution area graph:

- From the **Monitor** menu, choose **Network/Frame Size Area Graph**.

  The Frame Size Distribution area graph appears (Figure 4-7.).

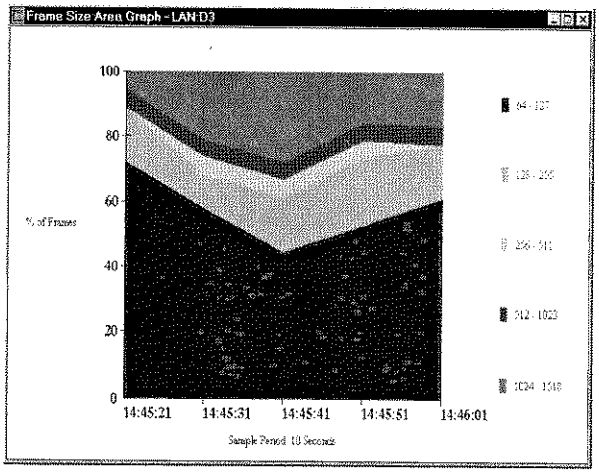


Figure 4-7. Sample Frame Size Distribution area graph

Shortcut:
Use the Frame Size button  on the Monitor toolbar.

4.7 Viewing Network Error Statistics

The Network Errors window displays error statistics that are specific to the type of network that you are monitoring.

To display the Errors window from the DominoWAN Monitor screen:

- From the **Monitor** menu, choose **Network/Errors**.

  The Network Errors window is displayed (Figure 4-8.).

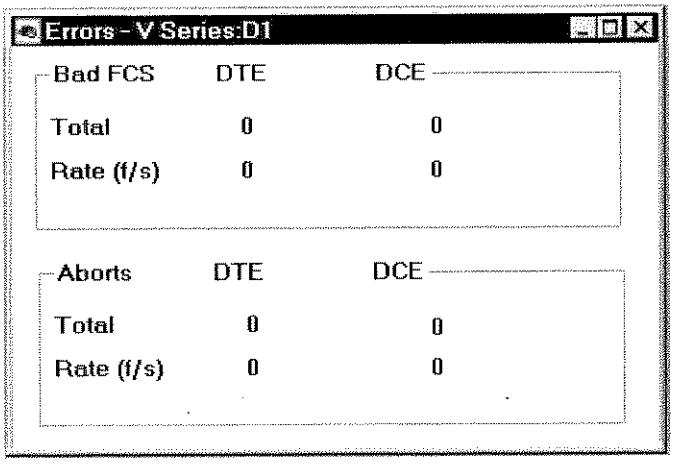


Figure 4-8. Errors window

Shortcut:
Use the Errors button  on the Monitor toolbar.

To display the Errors window from the DominoLAN Monitor screen:

- From the **Interface** menu, choose **Network Errors**.

The Network Errors window is displayed (Figure 4-9.).

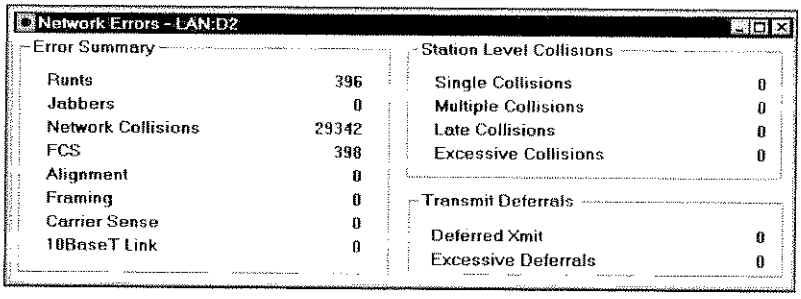


Figure 4-9. Network Errors window

Shortcut:
Use the Network Errors button on the Monitor toolbar.

4.8 Viewing Frame Rate Statistics

The Frame Rate graph displays frame rate statistics in bar graph format. It indicates the current frame rate and displays the frame rate for each interval during the monitoring period in the bar graph.

To learn how to scroll through the graph using the keyboard or the mouse, see Section 4.16, "Scrolling Through Graphs." To learn how to change the time interval used for displaying the graph, see Section 4.17, "Changing the Time Scale of Graphs."

4.8.1 Displaying the Frame Rate Graph

To display the Frame Rate graph:

- From the **Monitor** menu, choose **Network/Frame Rate Graph**.

The Network Frame Rate graph appears (Figure 4-10.).

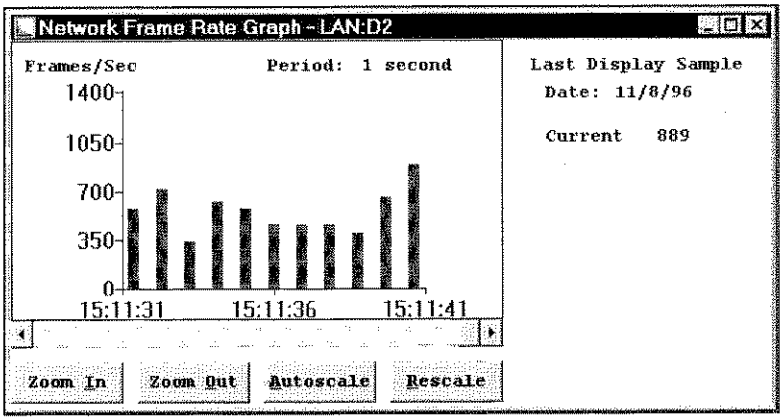


Figure 4-10. Sample Network Frame Rate Graph

Shortcut:
Use the Frame Rate button on the Monitor toolbar.

4.8.2 Changing the Frame Rate Scale of the Frame Rate Graph

The frame rate in the Frame Rate graph (Figure 4-10.) is displayed in frames per second. Monitor automatically adjusts the scale of the graph to fit the largest frame rate value that has occurred during the monitoring period. However, if there are peaks of unusually high traffic rates, this scale may be inappropriate for viewing the rest of the frame rate statistics. Monitor allows you to scale the graph based on the rates in the period that you are currently viewing.

To increase the frame rate scale of the Frame Rate graph:

- Click **Zoom Out**.

  The scale increases from seconds to minutes or from minutes to hours. If the current interval is hours, then the scale does not change.

To decrease the frame rate scale of the Frame Rate graph:

- Click **Zoom In**.

  The scale decreases from hours to minutes or minutes to seconds. If the current interval is seconds, then the scale does not change.

4.9 Displaying Frame Contents

When you are monitoring network traffic, results windows can display the contents of frames as they are being received from the analyzer.

- For LAN traffic, the Hex Trace window displays frame contents.
- For WAN traffic, your link type determines the window in which frame contents are displayed. When your link type is BOP (Bit-Oriented Protocol) or asynchronous (with a framing option), frame contents appear in the Hex Trace window. When your link is bisynchronous or asynchronous without framing, the contents appear in the Character Trace window.

4.9.1 Hexadecimal Trace

The Hex Trace window displays the contents of each frame in hexadecimal format and character code format. The Hex Trace window also displays the ID number, time, and length for each frame.

To display the Hex Trace window:

- From the menu bar, choose **Interface/Hex Trace**.

  The Hex Trace window appears (Figure 4-11.).

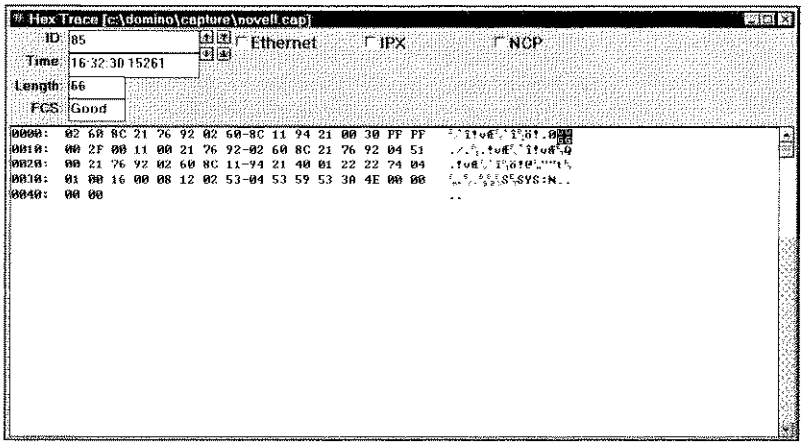


Figure 4-11. Hex Trace window

Shortcut:
Use the Hexidecimal Trace button on the Monitor toolbar.

4.9.2 Character Trace

For unframed asynchronous links, the Character Trace window displays the contents of each frame in the selected character code format along with the frame's timestamp.

For bisynchronous links, the Character Trace window displays the frame's timestamp, the contents of each frame, and an indicator showing whether the block check character (BCC) is bad or good. The data portion of the frame can be displayed in Data, Hex, or Decode format. The Data format uses the selected character code, the Hex format displays in hexadecimal, and the Decode format displays DATA or TRANSDATA for non-transparent and transparent data.

To display the Character Trace window:

1. From the menu bar, choose **Interface/Character Trace**.
2. On bisynchronous links, choose **Data**, **Decode** or **Hex Trace** from the **Character Trace** submenu.

   The Character Trace window appears (Figure 4-12.).

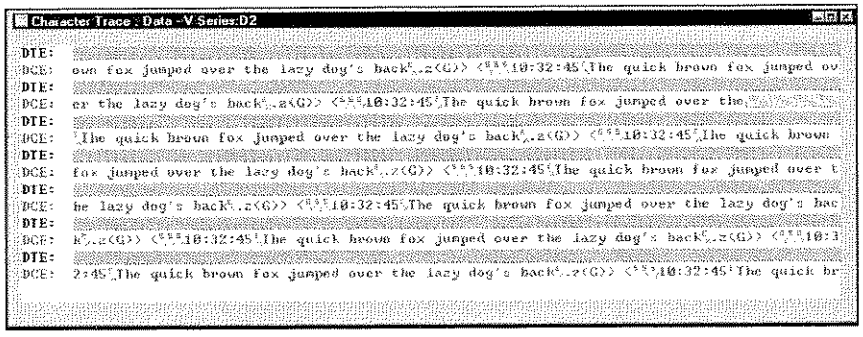


Figure 4-12. Character Trace window

Shortcut:
Use the Character Trace button on the Monitor toolbar.

4.9.3 Changing the Character Code Format

In both the Hex trace window and the Character Trace window, the default character code format is ASCII Extended. You can change the character code format using the Character Code commands on the Interface menu.

To change the character code format:

1. From the menu bar, choose **Interface/Character Code**.

2. Choose the format that you want from the Character Code submenu:
   - **ASCII**
   - **ASCII Extended**
   - **EBCD**
   - **EBCDIC**

4.10 Selecting the LAN Encapsulation Method

When you monitor WAN traffic, you must specify the method used for encapsulating LAN traffic to enable the Domino software to properly decode the received frames.

To select the LAN encapsulation method:

1. From the menu bar, choose **Monitor/Setup LAN Encapsulation**.

   The WAN Monitor Setup dialog box is displayed (Figure 4-13.).

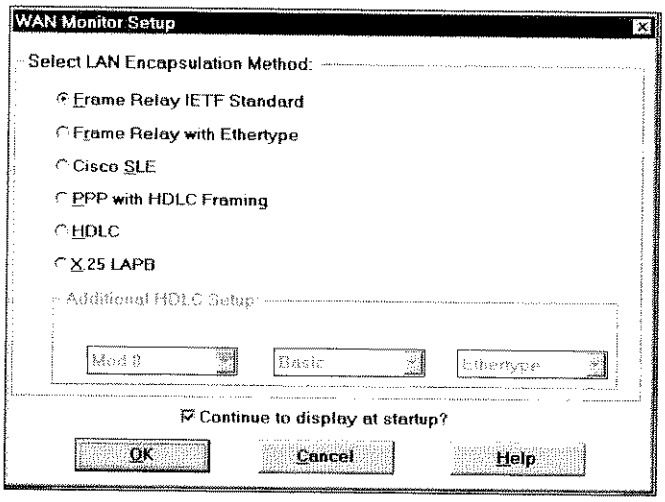


Figure 4-13. WAN Monitor Setup dialog box

2. Choose one of the LAN encapsulation methods.

   If you select **HDLC** as the encapsulation method, you must also specify the mode of operation (modulus), type of addressing, and encapsulation method used by HDLC.

   If you select **X.25 LAPB** as the encapsulation method, you must also specify the mode of operation (modulus), link type, and encapsulation method.

3. Click **OK**.

   Your selections are accepted and you return to the Monitor screen.

4.11 Modifying and Displaying the Network Interface

Use the Setup command on the Interface menu to change the setup for the network interface. The setup options vary, depending on the network interface.

To modify and display the network interface setup:

- From the menu bar, choose **Interface/Setup**.

  The appropriate network interface setup dialog box is displayed (Figure 4-14.). For detailed information, see Chapter 2 "Setting Up."

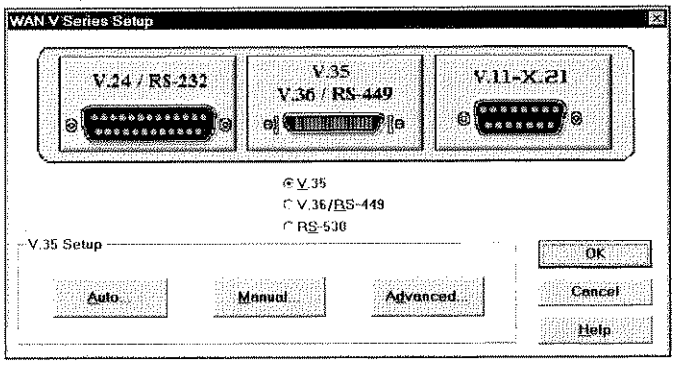


Figure 4-14. Sample Network Interface Setup dialog box

4.12 Modifying the Protocol Stack

While you are monitoring network traffic, you can use the Protocol Stack command on the Protocol menu to rearrange the protocols that are loaded on the stack. You can also remove protocols that are loaded, replace loaded protocols, or load additional protocols, as needed.

To modify the protocol stack:

- From the menu bar, choose **Protocol/Protocol Stack**.

The Protocol Stack dialog box appears (Figure 4-15).

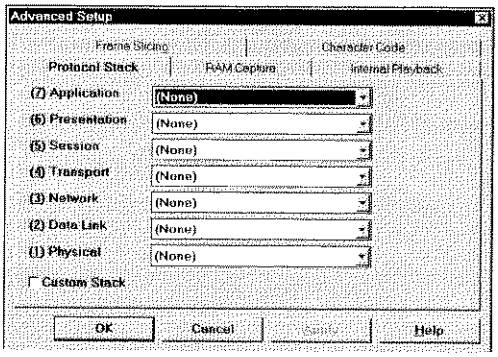


Figure 4-15. Protocol Stack dialog box

NOTE: For the Domino system to be able to decode a protocol, the software for that protocol must be installed and the protocol must be identifiable by the protocol at the preceding layer. A protocol that cannot be identified by the preceding protocol can be decoded only if you load that protocol and the one that precedes it at the appropriate layers on the protocol stack.

When analyzing WAN traffic, you must load the first protocol on the protocol stack, for example, Frame Relay, HDLC, or SDLC. Also, because WAN protocols typically lack the ability to detect the next layer protocol, it is advisable to load the upper layer protocols that you want to decode on the stack as well. The physical layer is automatically set to the interface you selected on the previous screen (for example, V.24).

4.12.1 Rearranging the Protocol Stack

You can load protocols on the protocol stack at their default layer or at any layer that you choose. This is controlled by the Custom Stack feature on the Protocol Stack dialog box (Figure 4-15).

To select protocols to load:

Task	Action
To load a protocol at any layer	Select the **Custom Stack** check box to enable the feature.
To load a protocol at its default layer	Select the **Custom Stack** to clear the check box and disable the feature.

Table 4-1. Protocol loading procedures

4.12.2 Changing Protocols

You can use the Protocol Stack dialog box (Figure 4-15) for the following protocol tasks:

- Add
- Replace
- Remove
- Set up

To change the protocol stack:

Task	Action
To add an additional protocol	1. Use the cursor to select the layer where you want to load the additional protocol. 2. Use the **Up Arrow** or **Down Arrow** to scroll through the list of available protocols and select the protocol that you want to load. 3. Click **OK** to re-analyze the capture network traffic.
To remove a protocol	1. From the Protocol Stack dialog box select the layer and the protocol to be deleted. 2. Select **(None)** and click **OK**.
To replace a protocol	1. From the Protocol Stack dialog box select the layer and the new protocol you want to load. 2. Click **OK**.
To set up a protocol	1. If the selected protocol has a Setup button, click **Setup**. 2. Make any necessary changes to the protocol setup.

Table 4-2. Procedures for modifying the protocol stack

The protocol stack options enable you to decode traffic at all layers of the OSI Reference Model. However, the analyzer's ability to decode all traffic correctly is limited if the traffic includes proprietary protocol encapsulations.

The Glue protocol software lets you obtain accurate protocol decodes at all layers, even when proprietary protocol information is present. With the Glue software, you can define fields that account for the bytes occupied by the proprietary protocol. When the software is loaded at the appropriate layer and customized in this way, the analyzer can decode the intervening protocol encapsulation. Then the protocols loaded at succeeding layers can be decoded accurately.

For information about loading and using the Glue protocol software, see 2.5.1.3, "Setting Up a Protocol."

4.13 Restarting Monitor

You can use the Restart command on the Control menu to restart the monitoring of traffic on the network and reset all of the network statistics.

To restart Monitor:

- From the menu bar, choose **Control/Restart**.

  The Domino software restarts Monitor, prompts you to verify the network interface setup (if the **Prompt at Run** option is enabled), resets all of the network statistics, and begins monitoring network traffic again.

Shortcut:
Use the Restart button  on the Monitor toolbar.

4.14 Pausing Monitor

Use the Pause command on the Window menu to pause the updating of the current results window and view traffic that you are interested in while continuing to monitor subsequent network traffic. When you are finished viewing the traffic, choose **Pause** again to resume the display of traffic.

Shortcut:
Use the Pause button  on the Monitor toolbar.

4.15 Examining Captured Network Traffic

Monitor provides you with access to results statistics that are pertinent to the network you are monitoring, as well as to Protocol Summary windows in which you can view protocol-specific information about the network traffic that has been stored in the capture buffer.

You can also switch to the Examine application from Monitor to review the network traffic that is being captured and stored in a RAM capture buffer while Monitor is running.

To examine captured network traffic:

- From the menu bar, choose **Control/Examine**.

  A dialog box is displayed which notes that switching to Examine will cause a gap in the RAM buffer, and asks you to confirm that you want to start Examine. If you are running Monitor on multiple Domino analyzers, this dialog box includes check boxes for each connected instrument, so that you can specify which traffic you want to examine. When you click **OK** on this dialog box, the Examine screen is displayed.

NOTE:

When you access the Examine screen from Monitor, the Domino analyzer continues to monitor network traffic and store captured network traffic in the RAM capture buffer.

4.16 Scrolling Through Graphs

The Network Utilization graph (Figure 4-3.) and Frame Rate graph (Figure 4-10.) contain scroll bars which you can use to scroll through the graphs to view information for different times during the monitoring period. You can scroll through the information using the keyboard or a mouse.

To scroll through the graphs using the keyboard:

Key	Action
Left Arrow	Scrolls backward one interval at a time
Right Arrow	Scrolls forward one interval at a time
Pg Up	Scrolls backward 11 intervals at a time
Pg Dn	Scrolls forward 11 intervals at a time
Ctrl-Home	Scrolls to the beginning of the monitoring period
Ctrl-End	Scrolls to the end of the monitoring period

To scroll through the graphs using the mouse:

Key	Action
Left Scroll Arrow	Click to scroll backward one interval at a time.
Right Scroll Arrow	Click to scroll forward one interval at a time.
Scroll Box	Drag it left or right in the scroll bar to move forward or backward through the graph.
Scroll Bar	Click to the left or right of the scroll box to move forward or backward one screen at a time.

4.17 Changing the Time Scale of Graphs

The information in the Network Utilization graph (Figure 4-3.) and the Frame Rate graph (Figure 4-10.) is displayed in either 1 second, 1 minute, or 1 hour intervals over the entire monitoring period. You can select the interval used for displaying the graph.

To increase the time scale of the graphs:

- Click **Zoom Out**.

  The scale increases from seconds to minutes or from minutes to hours. If the current interval is hours, then the scale does not change.

To decrease the time scale of the graphs:

- Click **Zoom In**.

  The scale decreases from hours to minutes or minutes to seconds. If the current interval is seconds, then the scale does not change.

5. Examining Captured Traffic

The Examine application is the Domino feature that enables you to review and analyze network traffic. Examine uses capture buffers in the RAM of the Domino analyzer to provide options for both real time and post-capture examination of network traffic. When Real-Time applications (Monitor, Transmit, Capture or the Toolbox applications) are running, the Domino system captures network traffic and stores it in a capture buffer. You can start Examine during real time operation and review the contents of that buffer, which can be continuously updated with newly captured data. To provide for post-capture examination of network traffic, the contents of a RAM capture buffer can be saved to a file. You can then use Examine to load the file into a capture buffer and review the data from the capture file.

With few exceptions, Examine works the same whether you're examining "live" buffered data during real time or captured data from a file. This chapter describes how to use Examine, including:

- working with capture files
- displaying frame information in a variety of results windows
- searching for specific frames
- jumping to specific frames
- filtering captured frames
- working with data from the capture buffer
- printing frame contents

5.1 Starting the Examine Application

Examine is one of the four main Domino functions that are available from the Workbench screen, which is the first screen that you see when you start the Domino software. To learn more about the Workbench screen and how to prepare to use an application, see Section 1.3, "The Domino Workbench."

To examine network traffic from a capture file:

♦ Choose **Examine** from the **Workbench** menu or click the Examine button.

Examine starts and displays the Open File dialog box, in which you select the capture file that contains the data that you want to examine.

To examine network traffic during real time operation:

♦ From the menu bar for the Real-Time screen in which you are working, choose **Control/Examine**.

Examine starts and displays the data from the RAM capture buffer in a set of default results windows.

Figure 5-1 illustrates the Examine screen with several open results windows.

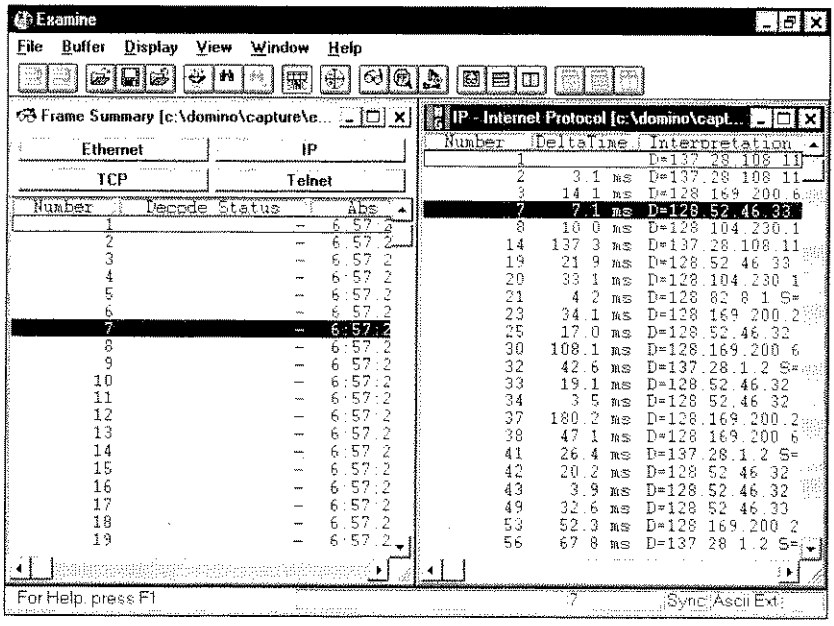


Figure 5-1. Examine screen

5.2 Capture Files vs. Capture Buffers

The Domino system stores network traffic in:

- capture buffers
- capture files

A capture buffer is an area in RAM where the system temporarily stores captured network traffic or the contents of a capture file that you want to examine. A capture file is a copy of the data in a capture buffer that is saved to disk for later use.

Table 5-1 summarizes the uses of capture buffers and capture files.

Type of capture storage	Functions
Capture buffers	• Store captured frames as they are captured from the network • Allow you to filter, search, and save to file the captured frames contained in the buffer • Store the contents of each capture file that you open, one buffer for each file • Allow you to open more than one capture file at a time, and switch from one buffer to another
Capture files	• Store captured network traffic permanently on disk • Can be played back onto the network to duplicate network test conditions

Table 5-1. Capture buffers and files

5.3 Working with Capture Files

You can examine captured network traffic in real time or you can open a capture file and load its contents into the capture buffer.

Within the Examine application, you can perform the following actions on capture files:

- open and close capture files
- save captured frames to a new capture file
- export captured frames to a CSV file or a text file

5.3.1 Saving Captured Frames to a New Capture File

You can save the contents of the capture buffer to a new capture file.

To save the captured frames to a new capture file:

1. From the menu bar, choose **File/Save As**.

   The Save Capture File dialog box appears (Figure 5-2).

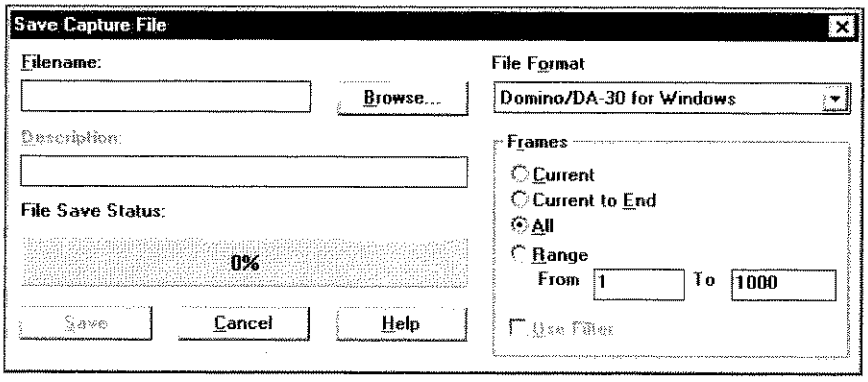


Figure 5-2. Save Capture File dialog box

2. Type a filename to use for the new capture file in the **File Name** box.
3. Click **Browse** to save the file to a different drive or directory.
4. In **Frames**, choose the range of frames that you want to save.

Current	Saves the frame that is highlighted in the Frame Summary window.
Current to End	Saves the frames from the highlighted frame to the end of the capture buffer.
All	Saves all of the frames in the capture buffer.
Range	Specifies the range that you want.

The **Use Filter** option is useful if you have examined and filtered the traffic in the capture buffer. Filtering is covered in Section Section 5.7, "Filtering Captured Frames."

Examine saves the contents of the capture buffer to the specified capture file. The **File Save Status** bar indicates the progress of the save. After Examine has saved the new capture file, you return to the Examine screen.

5.3.2 Opening an Existing Capture File

You can open an existing capture file from the **File** menu of the Examine screen and view frame and protocol information about the captured frames.

To open an existing capture file:

1. From the Examine screen menu bar, choose **File/Open**.

   The Open Capture File dialog box appears (Figure 5-3).

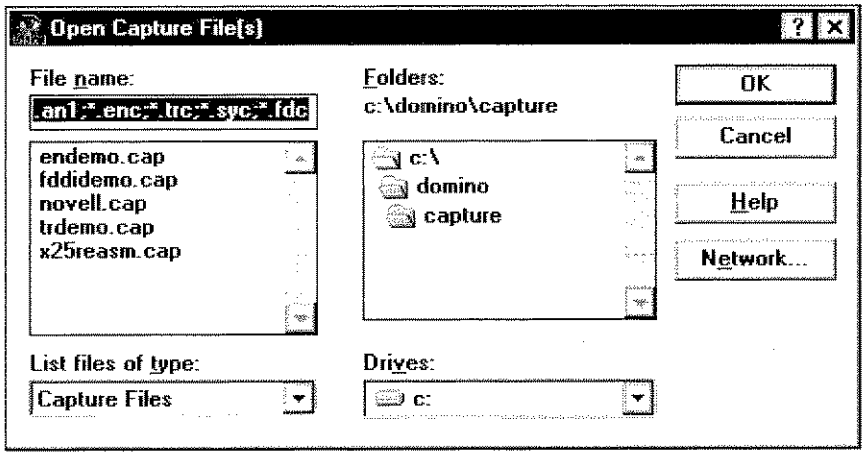


Figure 5-3. Open Capture File dialog box

2. Select or type the name of the capture file that you want to open in the **File name** box.
3. Click **OK**.

   The frames are loaded into the capture buffer and the Frame Summary window appears (Figure 5-5).

NOTE:

When you click the Examine button on the Workbench, the Open Capture File dialog box is automatically displayed.

Shortcut:

Click the Open button  on the Examine toolbar to gain quick access to the Open capture File dialog box from the within the Examine application.

5.3.2.1 Opening Character-Based Capture Files

If you have created capture files using the original WG DA-3x protocol analyzer, which is a character-based rather than Windows-based system, you can use those files with your Domino analyzer. The Domino system recognizes the DA-3x character-based capture files and automatically converts them to the format used by the Domino system's Windows interface.

To open a character-based capture file:

1. From the menu bar, choose **File/Open**.

   The Open Capture File dialog box appears (Figure 5-3).

2. Select **All Files** as the type of file to open in the **List Files of Type** box.

   All of the files in the current directory are listed in the **Filename** box.

3. Select the directory in the **Directories** box where the character-based capture file that you want to open is stored.

   All of the files in the selected directory are listed in the **Filename** box.

4. Select the name of the character-based capture file in the **Filename** box.

5. Click **OK**.

   The Convert Capture File confirmation box appears.

6. Click **Yes** to convert the format of the character-based capture file.

   The Save Converted Capture File dialog box appears (Figure 5-4).

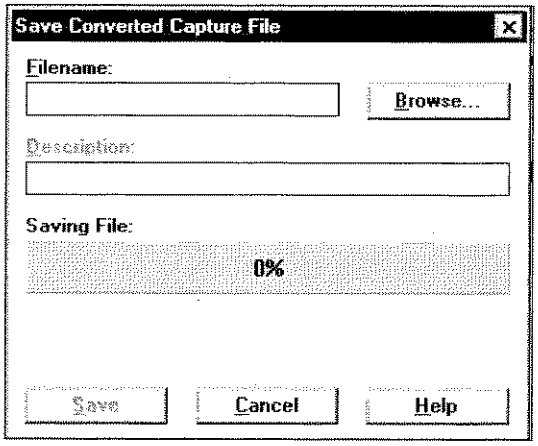


Figure 5-4. Save Converted Capture File dialog box

7. Type a filename to use for the converted capture file in the **Filename** box.

8. Type a brief description for the converted capture file in the **Description** box. The description can be up to 40 characters long and can contain spaces and punctuation.

9. Click **Save**.

   Examine converts the capture file and then loads the contents into a capture buffer. The Saving File bar indicates the progress of the conversion. After Examine has converted the capture file, you return to the Examine screen and the Frame Summary window appears (Figure 5-5).

5.3.3 Moving Between Capture Buffers

When you have more than one capture file open in Examine, you can move between the capture buffers that store the opened files.

To move to...	From the Buffer menu, choose...
The next capture buffer	**Next**
The previous capture buffer	**Previous**
A specific capture buffer	The capture buffer that you want to make active

Table 5-2. Commands for moving between capture buffers

Shortcut:
Click the Next Buffer button  or the Previous Buffer button  on the Examine toolbar.

5.3.4 Closing Capture Files

It is not necessary to exit Examine to close the current capture file. You can close one capture file and continue working on other open capture files or open an additional capture file.

You can also close all of the open capture files at the same time. This is helpful when you have been examining several capture files and you want to close all of them and open a different capture file.

To close the current capture file or all capture files:

- From the menu bar, choose **File/Close** or **File/Close All**.

  The capture file or files close along with the results windows.

If you close the only open capture file or all the capture files, the Open Capture File dialog box appears (Figure 5-3). This allows you to easily open another capture file.

Shortcut:
Click the Close button  on the Examine toolbar.

5.4 Displaying Frame Information

Results windows display information about the frames in the capture buffer. The results windows are accessed from the **Display** menu and include:

- Frame Summary
- Hexadecimal Trace
- Character Trace (DominoWAN only)
- Protocol Detail
- Protocol Summary

To display a results window:

♦ From the **Display** menu, choose the results window that you want to display.

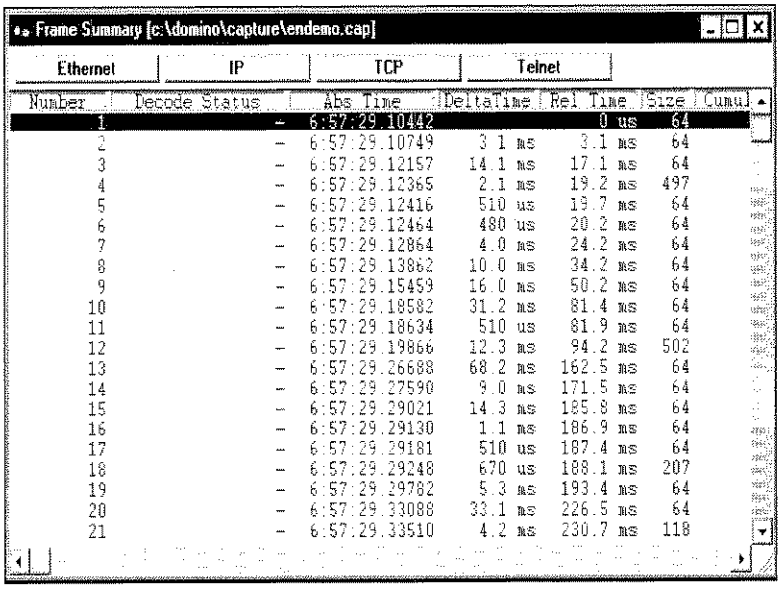
The selected results window appears.

5.4.1 Frame Summary

The Frame Summary window displays summary information about each frame in the current capture buffer. This window is automatically displayed when you open an existing capture file or access Examine from Capture, Monitor, or Transmit. If you close this window, an option on the **Display** menu allows you to display it again. In addition, you can choose to display only some of the fields in the Frame Summary. For information on selecting fields to display, see Section Section 5.8.8, "Displaying or Hiding Fields in Summary Windows." To display the Frame Summary window:

♦ From the menu bar, choose **Display/Frame Summary**.

The Frame Summary window appears (Figure 5-5).



Number	Decode Status	Abs Time	DeltaTime	Rel Time	Size	Cumu
1	–	6:57:29.10442		0 us	64	
2	–	6:57:29.10749	3.1 ms	3.1 ms	64	
3	–	6:57:29.12157	14.1 ms	17.1 ms	64	
4	–	6:57:29.12365	2.1 ms	19.2 ms	497	
5	–	6:57:29.12416	510 us	19.7 ms	64	
6	–	6:57:29.12464	480 us	20.2 ms	64	
7	–	6:57:29.12864	4.0 ms	24.2 ms	64	
8	–	6:57:29.13862	10.0 ms	34.2 ms	64	
9	–	6:57:29.15459	16.0 ms	50.2 ms	64	
10	–	6:57:29.18582	31.2 ms	81.4 ms	64	
11	–	6:57:29.18634	510 us	81.9 ms	64	
12	–	6:57:29.19866	12.3 ms	94.2 ms	502	
13	–	6:57:29.26688	68.2 ms	162.5 ms	64	
14	–	6:57:29.27590	9.0 ms	171.5 ms	64	
15	–	6:57:29.29021	14.3 ms	185.8 ms	64	
16	–	6:57:29.29130	1.1 ms	186.9 ms	64	
17	–	6:57:29.29181	510 us	187.4 ms	64	
18	–	6:57:29.29248	670 us	188.1 ms	207	
19	–	6:57:29.29782	5.3 ms	193.4 ms	64	
20	–	6:57:29.33088	33.1 ms	226.5 ms	64	
21	–	6:57:29.33510	4.2 ms	230.7 ms	118	

Figure 5-5. Frame Summary window

Shortcut:
Click the Frame Summary button on the Examine toolbar.

5.4.2 Frame Contents Windows

When you are monitoring network traffic, results windows can display the contents of frames as they are being received from the analyzer.

- For LAN traffic, the Hex Trace window displays frame contents.
- For WAN traffic, your link type determines the window in which frame contents are displayed.

When your link type is...	Frame contents appear in...
BOP (Bit-Oriented Protocol) or asynchronous (with a framing option)	the Hex Trace window.
bisynchronous or asynchronous without framing	the Character Trace window.

Table 5-3. WAN frame contents windows

5.4.2.1 Hexadecimal Trace

When your link type is BOP (Bit-Oriented Protocol) or asynchronous (with a framing option), the Hex Trace window displays the contents of each frame in hexadecimal format and character code format. The Hex Trace window also displays the ID number, time, and length for each frame.

To display the Hex Trace window:

- From the menu bar, choose **Display/Hex Trace**.

  The Hex Trace window appears (Figure 5-6).

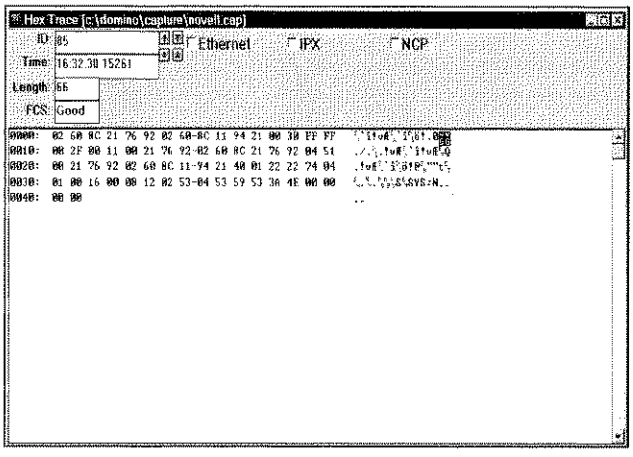


Figure 5-6. Hex Trace window

Shortcut:
Click the Hexadecimal Trace button on the Examine toolbar.

5.4.2.2 Character Trace

For bisynchronous links, the Character Trace window displays the frame's timestamp, the contents of each frame, and an indicator showing whether the block check character (BCC) is bad or good. The data portion of the frame can be displayed in Data, Hex, or Decode format. The Data format uses the selected character code, the Hex format displays in hexadecimal, and the Decode format displays DATA or TRANSDATA for non-transparent and transparent data.

For unframed asynchronous links, the Character Trace window displays the contents of each frame in the selected character code format along with the frame's timestamp.

To display the Character Trace window:

- From the menu bar, choose **Display/Character Trace**.

  The Character Trace window (Figure 5-7) appears.

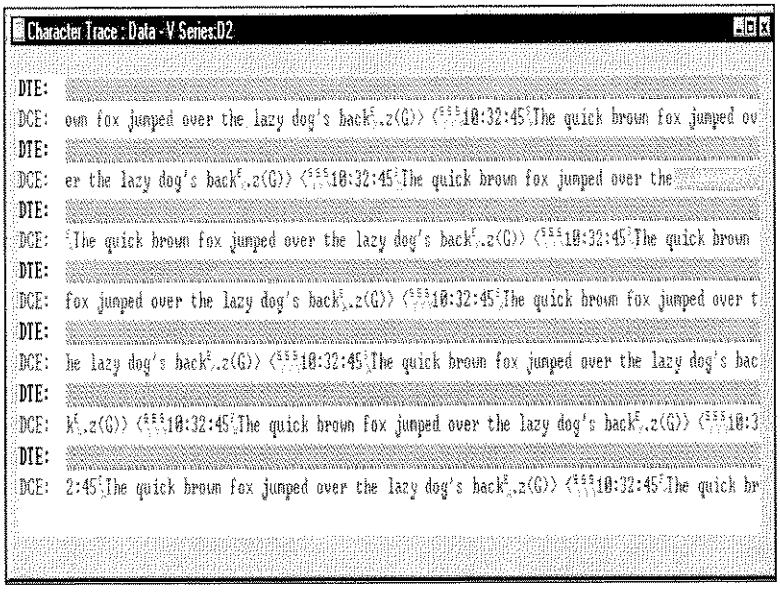


Figure 5-7. Character Trace window

Shortcut:
Click the Character Trace button on the Examine toolbar.

5.4.2.3 Changing the Character Code Format

In both the Hex Trace window and the Character Trace window, the default character code format is ASCII Extended. You can change the character code format using the character code commands on the **Buffer** menu.

To change the character code format:

1. From the menu bar, choose **Buffer/Character Code**.
2. Choose the format that you want from the Character Code submenu:
   - **ASCII**
   - **ASCII Extended**
   - **EBCD**
   - **EBCDIC**

5.4.3 Protocol Detail

The Protocol Detail window displays all decoded protocol elements for each frame in the current capture buffer. Frames are decoded layer-by-layer. The fields displayed in this window vary, depending on the protocols contained in each frame.

To display the Protocol Detail window:

♦ From the menu bar, choose **Display/Protocol Detail**.

The Protocol Detail window appears (Figure 5-8).

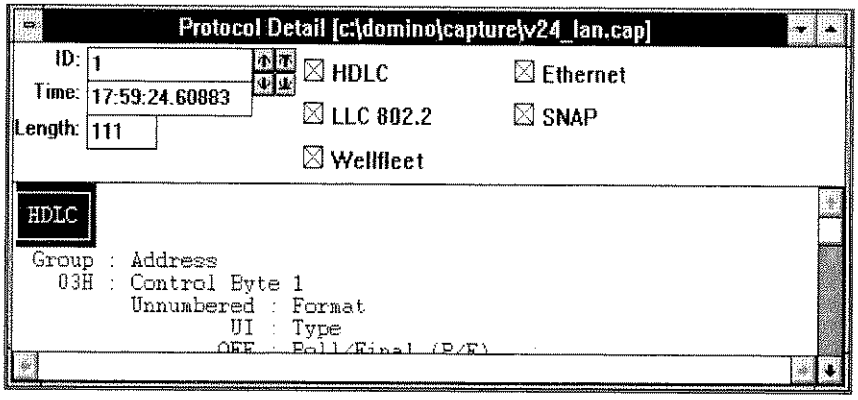


Figure 5-8. Protocol Detail window

Shortcut:
Click the Protocol Detail button  on the Examine toolbar.

5.4.4 Protocol Summary

The protocol summary windows display protocol-specific information for each frame in the capture buffer. You can display a protocol summary window for each protocol contained in the currently highlighted frame. For information about selecting fields to display, see Section Section 5.8.8, "Displaying or Hiding Fields in Summary Windows." To display a protocol summary window:

1. From the menu bar, choose **Display/Decodes**.

   The available protocols are listed (Figure 5-9).

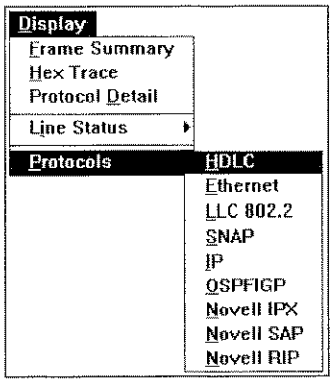


Figure 5-9. Protocol list

2. Choose one of the protocols from the list.

   The corresponding protocol-specific protocol summary window appears (Figure 5-10).

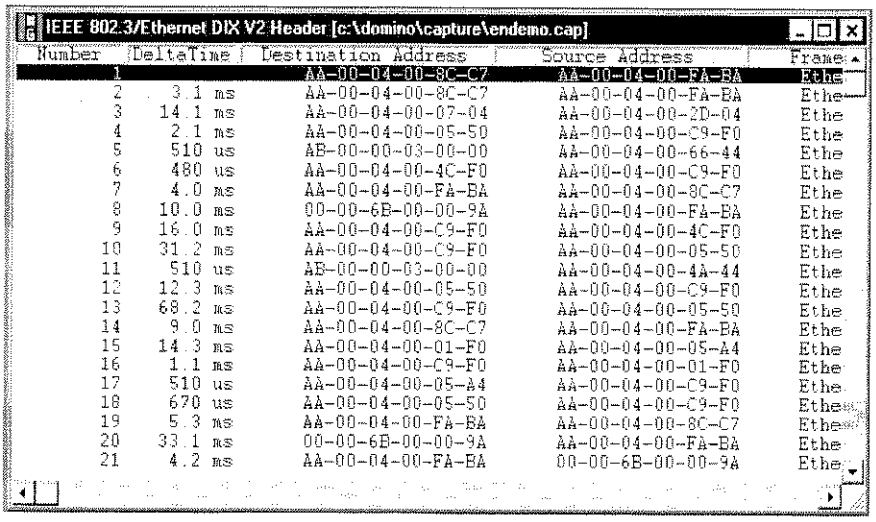


Figure 5-10. A Sample Protocol Summary window

Shortcut:

Click the protocol-specific button from the window's toolbar.

5.5 Searching for Specific Frames

Examine provides a full-featured search function that allows you to search through the entire capture buffer for frames that match specific criteria.

To search for a specific frame:

1. From the menu bar, choose **Buffer/Search**.

   The Search dialog box appears (Figure 5-11).

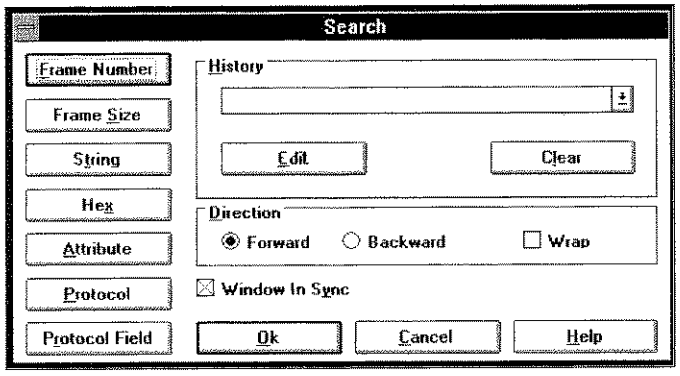


Figure 5-11. Search dialog box

2. Specify the search criteria.
3. Click **OK**.

   Examine performs a search through the capture buffer based on the specified criteria and moves the cursor to the first frame that matches the search criteria.

To search forward or backward from the current frame:

1. From the Search dialog box (Figure 5-11), select **Forward** or **Backward** in the **Direction** box.
2. Specify the search criteria and click **OK**.

   Examine searches through the capture buffer starting at the currently highlighted frame.

To continue the search through the capture file when you reach the beginning or the end:

- Before starting the search, select **Wrap** in the **Direction** box.

  The search wrap feature is enabled. When you perform the search, Examine will start over at the beginning of the capture buffer when it reaches the end or it will start over at the end of the capture buffer when it reaches the beginning.

Shortcut:
Click the Search button on the Examine toolbar.

5.5.1 Repeating a Search Using Previously Selected Criteria

You can repeat the search command that you most recently executed without having to redefine the search criteria.

To repeat the immediately previous search:

- From the menu bar, choose **Buffer/Repeat Search**.

  Examine performs a search through the capture buffer based on the criteria used during the previous search and moves the cursor to the first frame that matches the search criteria.

Shortcut:
Click the Repeat Search button on the Examine toolbar.

To repeat a search that was not immediately previous:

1. From the menu bar, choose **Buffer/Search**.

   The Search dialog box appears (Figure 5-11).

2. In the **History** box, select the search that you want to repeat.
3. Click **OK**.

   Examine performs a search through the capture buffer based on the criteria used during the selected search and moves the cursor to the first frame that matches the search criteria.

5.5.2 Searching by Frame Error

You can search through the capture buffer to locate the frames for which frame errors were detected.

To search for frames with frame errors:

- From the Search dialog box (Figure 5-11), click **Frame Error**.

  Examine moves the cursor to the first frame for which a frame error was detected.

5.5.3 Searching by Frame Size

You can search through the capture buffer to locate frames based on a specific frame size or range of sizes. When you specify the frame size to search for and start the search, Examine moves the cursor to the first frame that matches the frame size search criteria.

To search for frames by frame size:

1. From the Search dialog box (Figure 5-11), click **Frame Size**.

   The Frame Size Search dialog box appears (Figure 5-12).

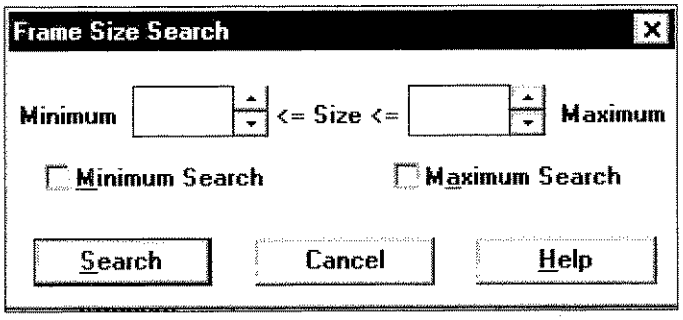


Figure 5-12. Frame Size Search dialog box

2. Do one of the following:

   To search for frames of a specific size:

   - In the **Minimum** box, type the frame size for which you want to search.

   or

   - In the **Maximum** box, type the frame size for which you want to search.

   To search for frames within a range of frame sizes:

   - In the **Minimum** box, type the minimum frame size of the range of frame sizes for which you want to search.

   and

   - In the **Maximum** box, type the maximum frame size of the range of frame sizes for which you want to search.

3. Click **Search**.

   Examine performs the search and moves the cursor to the first frame with the specified frame size or one that falls within the specified frame size range.

5.5.4 Searching by Address

You can search through the capture buffer to locate a frame or frames that include specific source or destination addresses. When you specify an address to search for and start the search, Examine moves the cursor to the first frame that has the specified address. When you specify both source and destination addresses, it indicates a search for frames passing between the two stations.

To search for frames based on addresses:

1. From the Search dialog box (Figure 5-11), click **Addresses**.

   The Addresses Search dialog box appears (Figure 5-13).

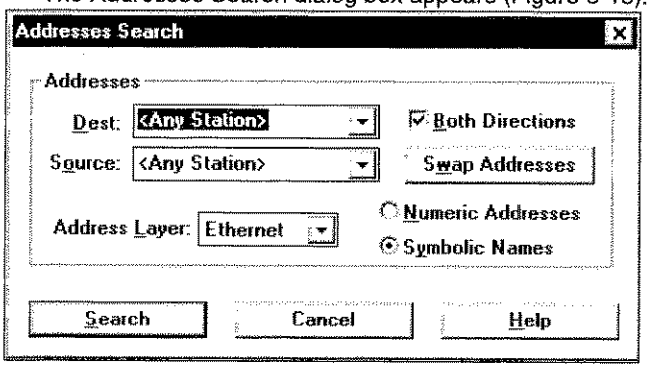


Figure 5-13. Addresses Search dialog box

2. In **Address Layer**, select the protocol layer for the addresses that you want to base the filter on.

   The address boxes display an address format consistent with the layer that you selected.

3. Type a destination address or a source address, or both, in the appropriate boxes.

   If symbolic names substitution is enabled in the interface setup, you can use names in place of numeric addresses.

4. To specify that you want to search for frames containing both specified addresses, regardless of which is the source address and which the destination address, choose **Both Directions**.

   If this option is not enabled, the search is only performed on frames going from the specified source to the specified destination.

5. Click **Search**.

   Examine performs the search and moves the cursor to the next frame in the buffer that has the specified address or combination of addresses.

5.5.5 Searching by Pattern

You can search through the capture buffer to locate frames containing a specific pattern or character string. When you specify the pattern to search for and start the search, Examine moves the cursor to the first frame that contains the character string that you specified.

You can specify the pattern in binary, hexadecimal, or text format. The currently selected character code determines the format of text patterns. To learn how to set the character code, see section Section 5.4.2.3, "Changing the Character Code Format." To search for frames based on a hexadecimal string:

1. From the Search dialog box (Figure 5-11), click **Pattern**.

   The Pattern Search dialog box appears (Figure 5-14).

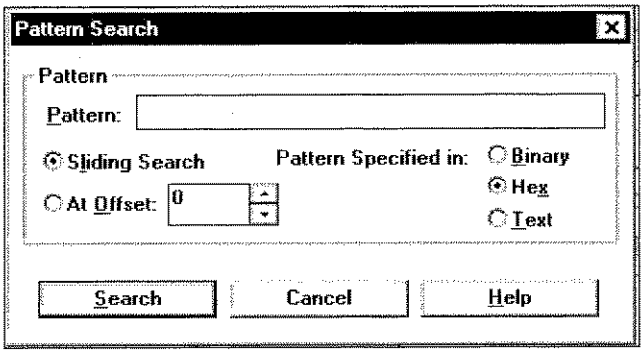


Figure 5-14. Pattern Search dialog box

2. In the **Pattern** box, enter the string to use as the search condition.

   The maximum string length is 32 bytes.

3. Specify the pattern location method:

   - **Sliding Search** specifies that the entire frame is to be searched for a pattern match. This is the default.
   - **At Offset (#)** specifies a search for the specified string at a specific offset into the frame. The offset is zero-based.

4. Select the format of the pattern: **Binary**, **Hex**, or **Text**.

   The pattern you have entered in the Pattern box is displayed in the format you select.

5. Click **Search**.

   Examine performs the search and moves the cursor to the first frame that contains the specified pattern.

5.5.6 Searching by Frame Attributes

You can search through the capture buffer to locate frames that have specific frame attributes. When you specify the frame attributes to search for and start the search, Examine moves the cursor to the first frame that has the frame attributes that you specified.

To search for frames based on frame attributes:

1. From the Search dialog box (Figure 5-11), click **Attribute**.

   The Attribute Search dialog box appears (Figure 5-15).

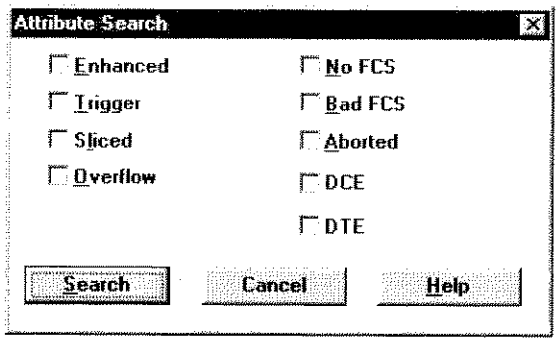


Figure 5-15. Attribute Search dialog box

2. Choose one or more of the frame attributes as part of the search criteria by selecting the corresponding check box as described in Table 5-3:

3. A check mark appears in the check box for each selected frame attribute. Examine searches for frames with all the checked attributes.Click **Search**.

   Examine performs the search and moves the cursor to the first frame that has the specified frame attributes.

Attribute	Description
Enhanced	A frame that is highlighted in reverse video. You define frame enhancement in a network event program for character-based applications.
Trigger	A frame that is set as the trigger in the capture buffer. In buffers that were captured using a character-based application, Trigger searches for the frames that are marked (set in the network event program) with the MARK.FRAME keyword
Sliced	A frame that was shortened before being processed. Frame slicing is covered in Section Section 2.5.4, "Setting Up Frame Slicing."
Overflow	A frame that overflows the frame buffer size.
No FCS	A frame that does not contain a frame check sequence.
Bad FCS	A frame that contains a bad frame check sequence.
Aborted	A frame that was aborted due to hardware errors.

Table 5-4. Frame attributes for searching in the Examine application

Attribute	Description
Receiver Options:	You can set an attribute filter to filter captured frames according to which line the frame was received on. The receiver options differ depending on the analyzer type you are using.
RX1/RX2	**Domino-E1, -T1, ATM, FE, and Gigabit:** Specifies whether the analyzer filters captured frames that were received on the Domino port labeled RX1 or RX2.
DTE/DCE	**WAN V-series and HSSI:** Specifies whether the analyzer filters captured frames according to the destination of the frame, either DTE or DCE. When the frame attribute is DTE, it indicates that the destination of the frame is the DTE; the frame was received on the Domino DCE line. When the frame attribute is DCE, it indicates that the destination of the frame is the DCE; the frame was received on the Domino DTE line.
NT/TE	**ISDN:** Specifies whether the analyzer filters captured frames according to the destination of the frame, either NT or TE. When the frame attribute is NT, it indicates that the destination of the frame is the NT; the frame was received on the Domino TE line. When the frame attribute is TE, it indicates that the destination of the frame is the TE; the frame was received on the Domino NT line.

Table 5-4. Frame attributes for searching in the Examine application

5.5.7 Searching by Protocol

You can search through the capture buffer to locate frames that contain a specific protocol. When you specify the protocol to search for and start the search, Examine moves the cursor to the first frame that contains the specified protocol.

To search for frames based on protocol:

1. From the Search dialog box (Figure 5-11), click **Protocol.**

   The Protocol Search dialog box appears (Figure 5-16).

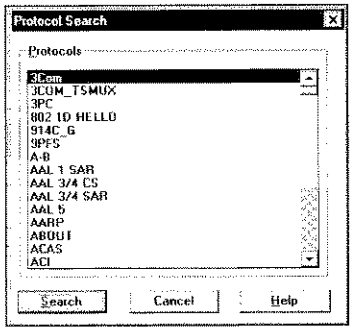


Figure 5-16. Protocol Search dialog box

2. Select the protocol you want from the **Protocols** box.
3. Click **Search**.

   Examine performs the search and moves the cursor to the first frame that contains the specified protocol.

5.5.8 Searching by Protocol-Specific Fields

You can search through the capture buffer to locate frames that contain a protocol-specific field with a specific value. When you specify the protocol field value to search for and start the search, Examine moves the cursor to the first frame that contains the specified protocol field value.

To search for frames based on protocol-specific fields:

1. From the Search dialog box (Figure 5-11), click **Protocol Field**.

   The Protocol Field Search dialog box appears (Figure 5-17).

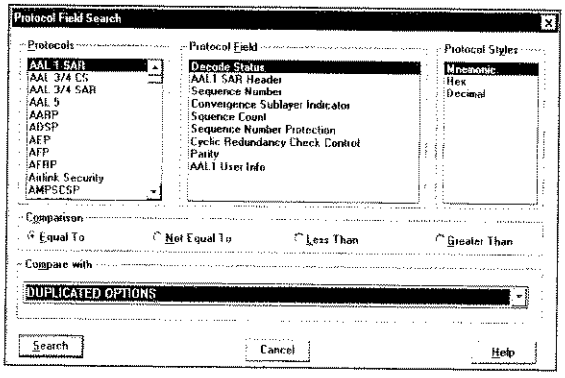


Figure 5-17. Protocol Field Search dialog box

2. In the **Protocols** box, select the protocol that contains the field for which you want to search.

   The fields of the selected protocol are displayed in the **Protocol Field** box.

3. Select the protocol-specific field for which you want to search.

4. To change the style used to display the field contents, move the cursor to the **Protocol Styles** box and select the desired style.

5. In the **Comparison** box, select the operator to compare the protocol field content with the value you specify in the **Compare With** box. The options are: **Equal To**, **Not Equal To**, **Less Than**, and **Greater Than**.

6. In the **Compare With** box specify the value that you want to use as the search condition for the selected Protocol Field.

   Either select a value from the list of possible values that is provided for a given field or type in the value.

7. Click **Search**.

   Examine performs the search and moves the cursor to the first frame that contains the specified protocol field value.

5.6 Jumping to Specific Frames

Examine provides a number of shortcuts that you can use to mark and jump directly to specific frames. With these tools you can move easily through the capture buffer as you examine its contents and begin to narrow your focus to specific items of interest.

5.6.1 Jumping to a Frame Number

The Domino analyzer numbers frames chronologically as they are received, beginning with the number 1. You can move through the capture buffer to locate a specific frame based on its frame number. When you specify the frame number to jump to, Examine moves the cursor to the frame that has the specified frame number.

To jump to a frame number:

1. From the menu bar, choose **Buffer/Jump to Frame Number**.

   The Jump to Frame Number dialog box (Figure 5-18) appears.

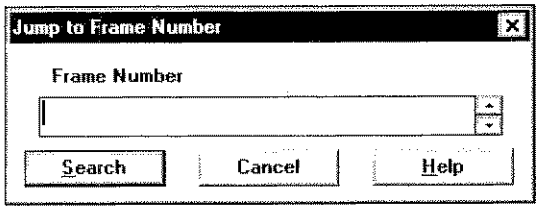


Figure 5-18. Jump to Frame Number dialog box

2. Type the frame number that you want to locate.
3. Click **Search**.

   Examine performs the search and moves the cursor to the frame that has the specified frame number.

5.6.2 Setting and Jumping to a Relative Mark

You can mark a frame in the capture buffer to measure the amount of time that elapses and the number of bytes that are received between the marked frame and each successive frame in the buffer. Marking a frame in this way is called setting a relative mark.

When you set a relative mark, you can use the **Display Options** command from the **View** menu to display the following fields for each frame that appears in the Frame Summary window or the Protocol Summary window:

- **Relative Time**, which displays the number of seconds that elapsed between the receipt of the marked frame and the receipt of the current frame.
- **Cumulative Bytes**, which displays the number of bytes that the analyzer received between the marked frame and the current frame.
- **Average Cumulative Bytes/Second**, which displays the average rate, in bytes per second, for the interval from the time you set a mark with the Set Mark command and the time the current frame was received.

- **Average Cumulative Bits/Second**, which displays the average rate, in bits per second, for the interval from the time you set a mark with the **Set Mark** command and the time the current frame was received.

The relative mark is set at the first frame in the capture buffer by default, and remains there until you set it on another frame. With the relative mark in the default position, all of the relative measurements are calculated from the first frame in the capture buffer

To set the relative mark:

1. In one of the results windows, move the cursor to the frame that you want to use as the mark.
2. From the menu bar, choose **Buffer/Set Relative Mark**.

   A box is displayed surrounding the marked frame. Relative time, cumulative bytes, and average cumulative bytes and bits per second for each successive frame are calculated, based on the marked frame.

To jump to the relative mark:

♦ From the menu bar, choose **Buffer/Jump to Relative Mark**.

The cursor jumps to the frame on which you previously set the relative mark.

5.6.3 Setting and Jumping to a Bookmark

When you want quick access to specific frames in the capture buffer, you can set bookmarks on those frames. After you have set a bookmark on a frame, you can jump to that frame quickly by using the **Jump to Bookmark** menu command or by using the shortcut keys that you assign to the bookmark. You can assign up to ten bookmarks within a capture buffer. Bookmarks are removed when you close a capture file or exit Examine.

To set a bookmark on a frame:

1. In one of the results windows, move the cursor to the frame that you want to mark.
2. From the menu bar, choose **Buffer/Set Bookmark**.
3. From the **Set Bookmark** submenu, choose one of the bookmarks (0 through 9).

   Examine sets a bookmark on the current frame.

To jump to a bookmark:

1. From the menu bar, choose **Buffer/Jump to Bookmark**.

   The **Jump to Bookmark submenu** displays the frame numbers of each frame to which a bookmark has been assigned.

2. From the **Jump to Bookmark** submenu, choose the bookmark that corresponds to the frame that you want.

   The cursor jumps to the frame that corresponds to that bookmark.

TIPS

- You can also set a bookmark on the current frame by pressing **Ctrl + x** on your keyboard, where x is an unassigned bookmark number 0 through 9.
- You can jump to a bookmark by pressing **Shift + x** on your keyboard, where x is the bookmark number assigned to the frame that you want.

5.7 Filtering Captured Frames

Examine provides three options that you can use to filter the frames in the capture buffer.

Filter option	Description
Basic Filter	The default option for filtering captured traffic. The Basic Filters dialog box provides setup procedures for three of the most commonly used filtering criteria: address, protocol, and pattern. You can create filters that combine all three criteria or use them individually. When you invoke the filter, only those frames that match the filtering criteria are displayed.
Quick Filtering	A shortcut for applying a filter based on the attributes of the current frame.
Advanced Filter	A tool that you can use to define a filter equation that logically combines up to six types of single-event filters for greatly increased filtering flexibility. Frames targeted by filter criteria can be either included in or excluded from the displayed traffic data. Individual sections of the filter can be saved, as can the entire filter equation.

Table 5-5. Filter options in the Examine application

You can print, save, or export all of the frames in the capture buffer or only those frames that were filtered in, based on the filtering criteria.

Network interface (hardware) filters allow you to specify the monitoring criteria for packets on a network. For information on interface filters, see the on-line Help topic "Setting Up the Network Interface Filter."

Shortcut:

You can start filter setup by clicking the Filter button on the Examine toolbar.

5.7.1 Basic Filtering

The basic filter option enables you to filter frames according to address, protocol, and pattern. You can set up all three filter criteria and then selectively enable them to filter on one, two, or all three characteristics. The filter criteria are logically ANDed. When you invoke the filter, only those frames that match the filtering criteria are displayed. You can also save and retrieve the filter.

To create a basic filter:

1. From the menu bar, choose **Buffer/Filter**.

   The Basic Filters dialog box appears (Figure 5-19).

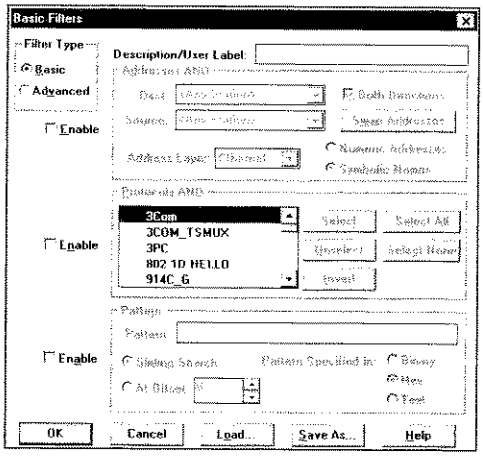


Figure 5-19. Basic Filters dialog box

2. In the **Description/User Label** box, type a description for the filter equation that you want to create.
3. Click **Enable** next to the filter condition that you want to set up.

   The setup for that filter type becomes active. When you click **OK** to invoke the filter, the captured frames will be filtered according to the filter conditions that you have enabled.

4. Complete the setup for the filter type or types that you have enabled. The three filter criteria types are:

Filter criteria type	Setup summary
Addresses	Select the **Address Layer** for the addresses that you want to filter on and enter the source and destination addresses.
Protocols	Highlight the **Protocol** that you want to filter on and click Select. Use the control buttons to make changes in your selections.
Pattern	In the **Pattern** box, type the pattern that you want to filter on. Select the format of the pattern and the frame search method.

Table 5-6. Setups for the Basic filter types in the Examine application

5. Click **OK**.

   Frames that match the defined filter criteria are displayed in the results windows.

5.7.1.1 Setting Up the Basic Addresses Filter

The basic addresses filter enables you to filter captured traffic according to source and destination address. Only frames that match the address filtering criteria that you specify are displayed.

The format of the addresses that you enter is determined by the **Address Layer** that you select. The layers supported and the appropriate address format for each are as follows:

Address layer	Address format
Ethernet	Ethernet address, specified as a six-byte MAC address, for example: 00-80-16-96-00-B0
TKR802.5	Token Ring address, specified as a six-byte MAC address, for example: 00:01:68:69:00:0D

Table 5-7. Address filter formats in the Examine application

Address layer	Address format
HDLC	Source address: DCE Destination address: DTE
IP	TCP/IP network address specified in dotted decimal format, for example, 9.67.102.37
Novell IPX	Novell IPX network address specified as network.node, for example: 11223344.5566778899AA
XNS IDP	XNS IDP network address, specified as network.node, for example: 045C819D.10005A112233
DECnet DRP	DECnet network address, specified as area.node, for example: 56.1011
Apple DRP	AppleTalk network address, specified as network number.node, for example: 63.255
VINES IP	Banyan VINES network address, specified as network.subnet, for example: 12345678.6677

Table 5-7. Address filter formats in the Examine application

To set up a basic addresses filter:

1. In the Basic Filters dialog box (Figure 5-19), click **Enable** next to the **Addresses** section of the dialog box.

   The **Addresses** filter setup becomes active.

2. In the **Address Layer** box, select the protocol layer for the addresses that you want to base the filter on.

   The address boxes display a format consistent with the layer that you select.

3. In the **Destination** box, select or type an address.

4. In the **Source** box, select or type an address.

5. To specify that filtering should occur in both directions, select **Both Directions**. If this option is not enabled, filtering is performed only on frames going from the source to the destination.

When you click **OK** on the Basic Filters dialog box, captured frames will be displayed according to the address filter criteria that you specified.

NOTE: **Address** is also one of the six filter criteria available with the advanced filter. You access the Advanced Filters dialog box by choosing **Buffer/Filter** from menu bar, and then selecting **Advanced** in the **Filter Type** box.

5.7.1.2 Setting Up the Basic Protocols Filter

The basic protocols filter enables you to filter captured network traffic based on the protocols that are contained in the frame.

To set up a basic protocols filter:

1. In the Basic Filters dialog box (Figure 5-19), select **Enable** next to the **Protocols** section of the dialog box.

   The **Protocols** filter setup becomes active.

2. In the **Protocols** box, select the desired protocol, then click Select.

   Repeat this step to select all of the protocols that you want to specify as the filtering criteria. Use the other control buttons (**Unselect**, **Select All**, **Select None**, and **Invert**) to modify your selections.

When you click **OK** on the Basic Filters dialog box, captured frames will be displayed according to the protocols filter criteria that you specified.

NOTE: **Protocol** is one of the six filter criteria available with the advanced filter. You access the Advanced Filter dialog box by choosing **Buffer/Filter** from the menu bar, and then selecting **Advanced** in the **Filter Type** box.

5.7.1.3 Setting Up the Basic Pattern Filter

The basic pattern filter enables you to filter captured network traffic based on whether a frame contains a specific pattern or character string. You can specify the pattern in **Binary**, **Hexadecimal**, or **Text** format. The currently selected character code determines the format of Text patterns. To learn how to set the character code, see Section Section 5.4.2.3, "Changing the Character Code Format.".

The basic pattern filter allows you to use wildcard characters to mask portions of a pattern that are not significant to the filter you are defining. For hexadecimal and binary patterns, the wildcard character is an 'X'; for text patterns it is a question mark(?). For example, if you were interested only in binary sequences in which the digits '1010' appeared in the second four bits, you could filter for the pattern 'XXXX1010'.

An inverted question mark appears in the pattern to signify an unprintable character. It also appears if the appropriate character cannot be displayed when you switch formats, for example, when you specify a single bit as a wildcard in **Binary** format, and then switch to **Hexadecimal** or **Text** format.

To set up a basic pattern filter:

1. In the Basic Filters dialog box (Figure 5-19), select **Enable** next to the **Pattern** section of the dialog box.

   The **Pattern** filter setup becomes active.

2. In the **Pattern** box, type the character string to use as the filtering criteria.

   The maximum string length is 32 bytes.

3. Specify the pattern location method. The options are:

Option	Description
Sliding Search	Specifies that the entire frame is to be searched for a pattern match. This is the default.
At Offset (#)	Specifies a search for the filter string at a specific offset into the frame. The offset is zero-based.

Table 5-8. Pattern location options for Examine filter

4. Specify the format of the pattern: **Binary**, **Hexadecimal**, or **Text**.

   The pattern you have entered in the **Pattern** box is displayed in the format that you select, and the captured frames are searched for a pattern match in the specified format.

When you click **OK** on the Basic Filters dialog box, captured frames will be displayed according to the pattern filter criteria you specified.

NOTE: **Pattern** is one of the six filter criteria available with the advanced filter. You access the Advanced Filter dialog box by choosing **Buffer/Filter** from the menu bar, and then selecting **Advanced** in the **Filter Type** box.

5.7.1.4 Saving a Basic Filter

The **Save As** option on the Basic Filters dialog box enables you to save the filter that you create.

To save a basic filter:

1. In the Basic Filters dialog box (Figure 5-19), click **Save As**.

   The Save As dialog box is displayed.

2. Type the name of the filter file you are saving. (The default extension for filter files is .FLT.)

3. Click **OK**.

   Your filter is saved to the DOMINO/FILTERS directory and you return to the Basic Filters dialog box.

5.7.1.5 Loading a Saved Basic Filter

The **Load** option enables you to load a previously saved filter into the Basic Filters dialog box.

To load a basic filter:

1. In the Basic Filters dialog box (Figure 5-19), click **Load**.

   The Open dialog box is displayed.

2. Highlight the name of the filter file that you want to load.

   The **Description** field displays the descriptive label that you saved with the file.

3. Click **OK**.

   Your filter is loaded into the Basic Filters dialog box.

NOTE: If the filter that you select is not a basic filter, an error box is displayed to inform you that the filter that you have selected contains the wrong information.

5.7.2 Quick Filtering

The quick filter option enables you to create a filter based on the attributes of the current frame with only a few clicks or key strokes. You can create a quick filter when you are working in any of the following results windows:

- Frame Summary window.
- Protocol Summary window.
- Protocol Detail window.

To create a quick filter:

1. Select the frame on which you want to base the quick filter.
2. Click the window with your right mouse button.
3. Choose **Quick Filter** from the shortcut menu.

   The Basic Filters dialog box (Figure 5-19) appears. The fields in the dialog box contain the corresponding attributes of the frame that you selected.

4. Click **Enable** for each of the criteria you want to use.
5. Click **OK**.

   The dialog box closes and the filtered frames are displayed based on the attributes that you selected.

5.7.3 Advanced Filtering

The advanced filter option enables you to create filter equations using six filter criteria and a full set of logical operators to customize the display of captured frames. You can specify whether frames that match the filter criteria are included in or excluded from the display, and you have the option to temporarily disable the filter and display all captured frames. You can also save filter equations to a file and retrieve them to reuse or edit.

To create an advanced filter equation:

1. From the menu bar, choose **Buffer/Filter**.

   The Basic Filters dialog box appears (Figure 5-19).

2. In the **Filter Type** box, click **Advanced**.

   The Advanced Filter dialog box appears (Figure 5-20).

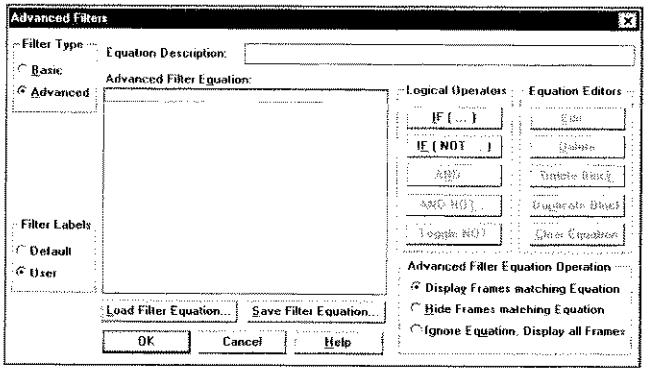


Figure 5-20. Advanced Filter Dialog Box

3. In **Equation Description**, type a description for the filter equation that you want to create.

   When you choose the **Save Filter Equation** button, the equation description is saved with the filter equation.

4. Click **IF(...)** or **IF (NOT...)** to add the first block to the equation.

The New Filter dialog box is displayed (Figure 5-21).

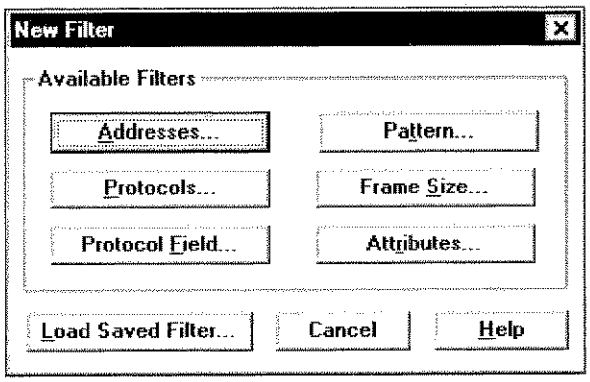


Figure 5-21. New Filter dialog box

5. In the New Filter dialog box, choose one of the available filter types.

   The dialog box that corresponds to the filter type that you selected is displayed.

6. Complete the filter specification and click **OK** on the filter type dialog box.

   The Advanced Filter dialog box is displayed. The new filter description is added to the equation in a block with the logical operator that you selected. The **IF(...)** and **IF(NOT...)** buttons change to **OR(...)** and **OR(NOT...)**, respectively, and all other logical operator buttons are enabled to allow you to add other criteria to the equation.

7. Repeat the process of selecting logical operators and adding filter conditions to the equation until you have defined all of the conditions that you want to filter on.

8. In the Advanced Filter Equation Operation box, choose the option that describes how you want the filter to affect the display of frames. The options are:

Option	Description
Display Frames Matching Equation	Only frames matching the filter criteria are included in the Frame Summary.
Hide Frames Matching Equation	Frames matching the filter criteria are excluded from the Frame Summary.
Ignore Equation, Display All Frames	Temporarily disables the filter you have defined so that you can view all captured frames.

Table 5-9. Advanced filter equation options in the Examine application

9. Click **Save Filter Equation** to save the equation if you expect to use it again.

10. Click **OK**.

    The Frame Summary window displays frames filtered according to the filter that you have defined.

5.7.3.1 Filtering Based on Address

The advanced addresses filter enables you to filter captured traffic according to source and destination address. **Addresses** is one of the six filter criteria available with the advanced filter option.

The format of the addresses that you enter is determined by the **Address Layer** that you select. The layers supported and the appropriate address format for each are as follows (Table 5-10):

Address Layer	Address Format
Ethernet	Ethernet address, specified as a six-byte MAC address, for example: 00-80-16-96-00-B0
TKR802.5	Token Ring address, specified as a six-byte MAC address, for example: 00:01:68:69:00:0D
IP	TCP/IP network address specified in dotted decimal format, for example, 9.67.102.37
Novell IPX	Novell IPX network address specified as network.node, for example: 11223344.5566778899AA
XNS IDP	XNS IDP network address, specified as network.node, for example: 045C819D.10005A112233
DECnet DRP	DECnet network address, specified as area.node, for example: 56.1011
Apple DRP	AppleTalk network address, specified as network number.node, for example: 63.255
VINES IP	Banyan VINES network address, specified as newwork.subnet, for example: 12345678.6677

Table 5-10. Address filter formats in the Examine application

To set up an addresses filter:

1. In the Advanced Filter dialog box (Figure 5-20), choose a logical operator button to add a new block to the filter equation.

   The New Filter dialog box is displayed (Figure 5-21).

2. In the New Filter dialog box, click **Addresses**.

   The Addresses Filter dialog box is displayed (Figure 5-22).

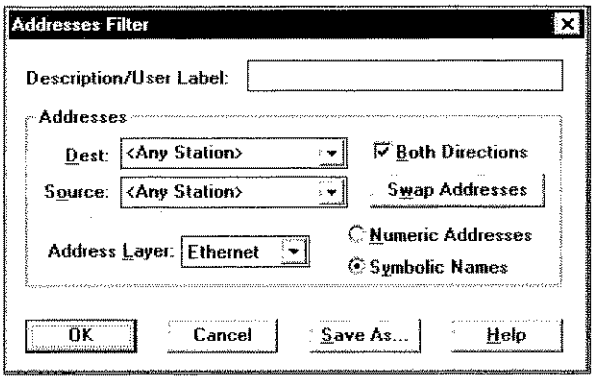


Figure 5-22. Addresses Filter dialog box

3. In **Description/User Label**, type a description of the filter.

   If you save the filter, the description is stored with the filter. If you chose the **User Filter Labels** option on the Advanced Filter dialog box, the description that you enter in **Description/User Label**will appear as the filter label in the Advanced Filter Equation.

4. In **Address Layer** , select the protocol layer for the addresses that you want to base the filter on.

   The address boxes display an address format consistent with the layer that you select.

5. In **Destination**, select or type an address.

6. In **Source**, select or type an address.

7. To specify that filtering should occur in both directions, choose **Both Directions**. If this option is not enabled, filtering is performed only on frames going from the source to the destination.

8. Click **OK**.

   You return to the Advanced Filter dialog box. The address filter that you created is added to the filter equation. When you click **OK** to accept the equation, Examine displays the captured traffic using the address filter that you specified.

NOTE: You can also create an address filter with the basic filter option. The filter can be implemented by itself, or logically ANDed with pattern and protocol filters.

5.7.3.2 Filtering Based on Frame Size

The advanced frame size filter enables you to filter captured traffic according to minimum frame size, maximum frame size, a specific frame size, or a range of frame sizes. Frame size is one of the six filter criteria available with the advanced filter option.

To set up a frame size filter:

1. In the Advanced Filter dialog box (Figure 5-20), choose a logical operator button to add a new block to the filter equation.

   The New Filter dialog box is displayed (Figure 5-21).

2. In the New Filter dialog box, click **Frame Size**.

   The Frame Size Filter dialog box is displayed (Figure 5-23).

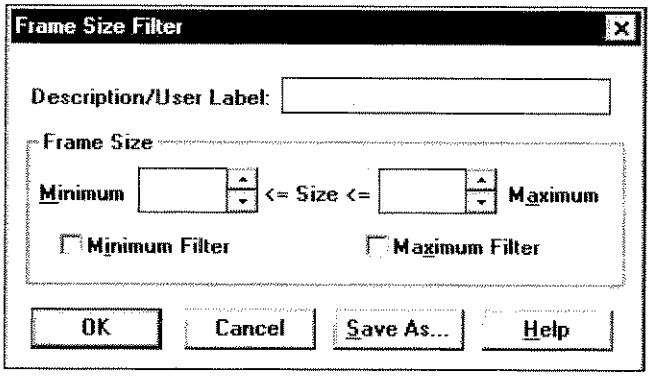


Figure 5-23. Frame Size Filter dialog box

3. In **Description/User Label**, type a description of the filter.

   If you save the filter, the description is stored with the filter. If you chose the **User Filter Labels** option on the Advanced Filter dialog box, the description that you enter in **Description/User Label** will appear as the filter label in the Advanced Filter Equation.

4. To create your filter, enter frame size values in the **Minimum** and **Maximum** boxes as follows:

To filter based on...	Do this...
Minimum frame size	In the **Minimum** box, enter the smallest frame size that you want to include in the filter. The minimum search check box is enabled.
Maximum frame size	In the **Maximum** box, enter the largest frame size that you want to include in the filter. The maximum search check box is enabled
Specific frame size	Enter the specific frame size that you want to include in the filter in both the **Minimum** and **Maximum** boxes.
Range of frame sizes	In the **Minimum** box, enter the smallest frame size in the range. In the **Maximum** box, enter the largest frame size in the range.

Table 5-11. Setups for Advanced frame size filters in the Examine application

5. Click **OK**.

   You return to the Advanced Filter dialog box. The frame size filter that you created is added to the filter equation. When you click **OK** to accept the equation, Examine displays the captured traffic using the frame size filter that you specified.

5.7.3.3 Filtering Based on Pattern

The pattern filter enables you to filter captured network traffic based on whether a frame contains a specific pattern or character string. Pattern is one of the six filter criteria available with the advanced filter option.

You can specify the pattern in binary, hexadecimal, or text format. The currently selected character code determines the format of text patterns. To learn how set the character code, see Section Section 5.4.2.3, "Changing the Character Code Format.".

With the pattern filter that you can use wildcard characters to mask portions of a pattern that are not significant to the filter that you are defining. For hexadecimal and binary patterns, the wildcard character is the letter X; for text patterns it is a question mark(?). For example, if you were interested only in binary sequences in which the digits '1010' appeared in the second four bits, you could filter for the pattern 'XXXX1010'.

An inverted question mark in the pattern signifies an unprintable character. It also appears if the appropriate character cannot be displayed when you switch formats, for example, when you specify a single bit as a wildcard in binary format, and then switch to hexadecimal or text format.

To filter captured traffic based on pattern:

1. In the Advanced Filter dialog box (Figure 5-20), choose a logical operator button to add a new block to the filter equation.

   The New Filter dialog box is displayed (Figure 5-21).

2. Click **Pattern**.

   The Pattern Filter dialog box is displayed (Figure 5-24).

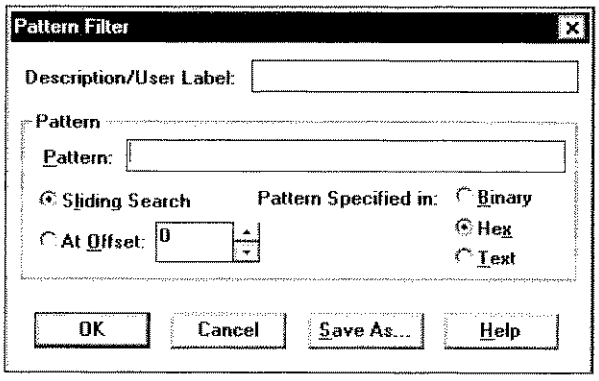


Figure 5-24. Pattern Filter dialog box

3. In **Description/User Label**, type a description of the filter.

   If you save the filter, the description is stored with the filter. If you chose the **User Filter Labels** option on the Advanced Filter dialog box, the description that you enter in **Description/User Label** will appear as the filter label in the Advanced Filter Equation.

4. In **Pattern**, enter the character string to use as the filtering criteria.

   The maximum string length is 32 bytes.

5. Specify the pattern location method. The options are:

Option	Description
Sliding Search	Specifies that the entire frame is to be searched for a pattern match. This is the default.
At Offset (#)	Specifies a search for the filter string at a specific offset into the frame. The offset is zero-based.

Table 5-12. Pattern location options for Examine filters

6. Specify the format of the pattern: **Binary**, **Hexadecimal**, or **Text**.

   The pattern that you entered in the **Pattern** box is displayed in the format that you select, and the captured frames are searched for a pattern match in the specified format.

7. Click **OK**.

   You return to the Advanced Filter dialog box. The pattern filter that you created is added to the filter equation. When you click **OK** to accept the equation, Examine displays the captured traffic using the pattern filter that you specified.

NOTE: You can also create a pattern filter with the basic filter option. The filter can be implemented by itself, or logically ANDed with address and protocol filters.

5.7.3.4 Filtering Based on Frame Attribute

The frame attribute filter enables you to specify certain frame characteristics as criteria for filtering captured traffic. Frame attribute is one of the six filter criteria available with the advanced filter option.

To filter captured traffic based on frame attributes:

1. In the Advanced Filter dialog box (Figure 5-20), choose a logical operator button to add a new block to the filter equation.

   The New Filter dialog box is displayed (Figure 5-21).

2. Click **Attributes**.

   The Attribute Filter dialog box is displayed (Figure 5-25).

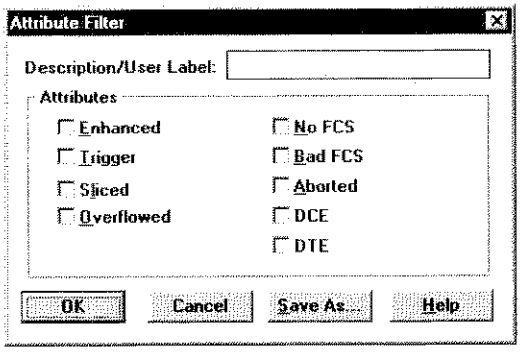


Figure 5-25. Attribute Filter dialog box

3. In **Description/User Label**, enter a description of the filter.

   If you save the filter, the description is stored with the filter. If you chose the **User Filter Labels** option on the Advanced Filter dialog box, the description that you type in **Description/User Label** will appear as the filter label in the Advanced Filter Equation.

4. Choose one or more of the frame attributes as part of the filtering criteria by selecting the corresponding check box as described in Table 5-13):

Attribute	Description
Enhanced	A frame that is highlighted in reverse video. You define frame enhancement in a network event program for character-based applications.
Trigger	A frame that is set as the trigger in the capture buffer. In buffers that were captured using a character-based application, Trigger searches for the frames that are marked (set in the network event program) with the MARK.FRAME keyword
Sliced	A frame that was shortened before being processed. Frame slicing is covered in Section Section 2.5.4, "Setting Up Frame Slicing.".
Overflow	A frame that overflows the frame buffer size.
No FCS	A frame that does not contain a frame check sequence.
Bad FCS	A frame that contains a bad frame check sequence.
Aborted	A frame that was aborted due to hardware errors.

Table 5-13. Frame attributes for filtering captured data in the Examine application

Attribute	Description
Receiver Options:	You can set an attribute filter to filter captured frames according to which line the frame was received on. The receiver options differ depending on the analyzer type you are using.
RX1/RX2	**Domino-E1, -T1, ATM, FE, and Gigabit:** Specifies whether the analyzer filters captured frames that were received on the Domino port labeled RX1 or RX2.
DTE/DCE	**WAN V-series and HSSI:** Specifies whether the analyzer filters captured frames according to the destination of the frame, either DTE or DCE. When the frame attribute is DTE, it indicates that the destination of the frame is the DTE; the frame was received on the Domino DCE line. When the frame attribute is DCE, it indicates that the destination of the frame is the DCE; the frame was received on the Domino DTE line.
NT/TE	**ISDN:** Specifies whether the analyzer filters captured frames according to the destination of the frame, either NT or TE. When the frame attribute is NT, it indicates that the destination of the frame is the NT; the frame was received on the Domino TE line. When the frame attribute is TE, it indicates that the destination of the frame is the TE; the frame was received on the Domino NT line.

Table 5-13. Frame attributes for filtering captured data in the Examine application

5. A check mark appears in the check box for each selected frame attribute.
6. Click **OK**.

   You return to the Advanced Filter dialog box. The frame attribute filter that you created is added to the filter equation. When you click **OK** to accept the equation, Examine displays the captured traffic using the frame attribute filter that you specified.

5.7.3.5 Filtering Based on Protocol

The protocols filter enables you to filter captured network traffic based on the protocol contained in the frame. Protocol is one of the six filter criteria available with the advanced filter option.

To filter captured traffic based on protocol:

1. In the Advanced Filter dialog box (Figure 5-20), choose a logical operator button to add a new block to the filter equation.

   The New Filter dialog box is displayed (Figure 5-21).

2. Click **Protocol**.

   The Protocol Filter dialog box is displayed (Figure 5-26).

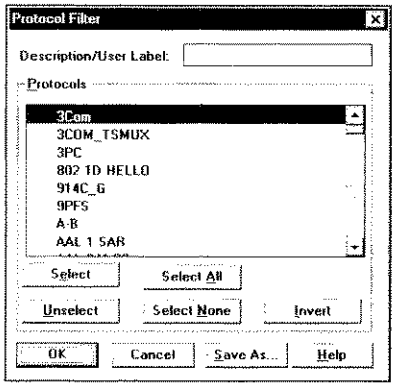


Figure 5-26. Protocol Filter Dialog Box

3. In **Description/User Label**, type a description of the filter.

   If you save the filter, the description is stored with the filter. If you chose the **User Filter Labels** option on the Advanced Filter dialog box, the description that you type in **Description/User Label** will appear as the filter label in the Advanced Filter Equation.

4. In **Protocols**, select the desired protocol, then click **Select**.

   Repeat this step to select all of the protocols that you want to specify as the filtering criteria.

5. Click **OK**.

   You return to the Advanced Filter dialog box. The protocol filter that you created is added to the filter equation. When you click **OK** to accept the equation, Examine displays the captured traffic using the protocol filter that you specified.

NOTE: You can also create a protocol filter with the basic filter option. The filter can be implemented by itself, or logically ANDed with address and pattern filters.

5.7.3.6 Filtering Based on Protocol-Specific Fields

The protocol field filter enables you to filter captured network traffic based on the content of protocol-specific fields in the frame. Protocol field is one of the six filter criteria available with the advanced filter option.

To filter captured traffic based on protocol-specific fields:

1. In the Advanced Filter dialog box (Figure 5-20), choose a logical operator button to add a new block to the filter equation.

   The New Filter dialog box is displayed (Figure 5-21).

2. Click **Protocol Fields**.

   The Protocol Field Filter dialog box is displayed (Figure 5-27).

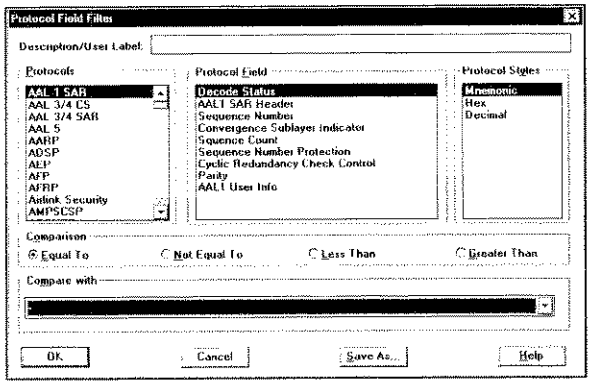


Figure 5-27. Protocol Field Filter dialog box

3. In **Description/User Label**, type a description of the filter.

   If you save the filter, the description is stored with the filter. If you chose the **User Filter Labels** option on the Advanced Filter dialog box, the description that you type **Description/User Label** will appear as the filter label in the Advanced Filter Equation.

4. In **Protocols**, select the protocol that contains the field that you want to use as the filtering criteria.

5. In **Protocol Field**, select the field that you want to use as the filtering criteria.

   A list of styles appropriate for the selected field is displayed in the **Protocols Styles** box. Also, depending on the selected field, the **Compare With** box displays selectable values appropriate to the field, or is blank so that you can enter a value.

6. In **Protocol Styles**, select the format of the field as you want it to be matched in the filter.

7. In **Comparison**, select the operator to compare the protocol field content with the value that you specify in the **Compare with** box. The options are **Equal To**, **Not Equal To**, **Less Than**, and **Greater Than**.
8. In **Compare With**, specify the value that you want to use as the filtering criteria for the selected **Protocol Field**.

   Either select from the list of possible values that is provided for a given field or type the value.
9. Click **OK**.

   You return to the Advanced Filter dialog box. The protocol field filter that you created is added to the filter equation. When you click **OK** to accept the equation, Examine displays the captured traffic using the protocol filter that you specified.

5.7.3.7 Saving an Advanced Filter

In each of the single-event filter dialog boxes that you use for adding conditions to an advanced filter equation, you can save the filter that you create.

To save a single-event filter:

1. In the filter dialog box, click **Save As**.

   The Save As dialog box is displayed.
2. Type the name of the filter file that you are saving. (The default extension for filter files is .FLT.)
3. Click **OK**.

   Your filter is saved to the /FILTERS directory and you return to the filter dialog box.

5.7.3.8 Loading a Saved Advanced Filter

The **Load Saved Filter** option on the New Filter dialog box enables you to load a previously saved filter into a single event filter dialog box.

To load a saved filter:

1. In the Advanced Filter dialog box (Figure 5-20), choose a logical operator button to add a new block to the filter equation.

   The New Filter dialog box is displayed (Figure 5-21).
2. In the New Filter dialog box, click **Load Saved Filter**.

   The Open dialog box is displayed.

3. Highlight the name of the filter file that you want to load.

   The **Description** field displays the descriptive label that you saved with the file.

4. Click **OK**.

   The filter is loaded into the appropriate single event filter dialog box.

NOTE: If the filter that you select is not a single-event filter, an error box is displayed to inform you that the filter that you have selected contains the wrong information.

5.7.3.9 Modifying Advanced Filtering Conditions

When you create a filter equation in the Advanced Filter dialog box and click **OK**, the Frame Summary window appears on the Examine screen with the captured frames displayed according to the filtering conditions that you specified. If you want to change the filter conditions, return to the Advanced Filter dialog box; the current filter is displayed in the Advanced Filter Equation box.

You can modify the filter conditions using the Equation Editor buttons on the side of the dialog box. These buttons enable you to edit or delete individual conditions, delete or duplicate entire blocks of filtering conditions, or clear all entries from the equation.

NOTE: A block is the set of ANDed filter conditions enclosed in parentheses that follows a logical operator (such as IF, IF(NOT), OR, or OR(NOT)) in a filter equation.

To modify filtering criteria:

1. Display the Advanced Filter dialog box (Figure 5-20).
2. To make changes to the filter conditions, use the procedures described in Table 5-14:

To make this change...	Use this procedure:
Edit a filter condition	1. Position the cursor on the filter condition that you want to change. Click **Edit** to display the appropriate filter dialog box. 2. Make the desired changes to the filter. Click **OK** to return to the Advanced Filter dialog box.
Delete a filter condition	Position the cursor on the filter condition that you want to delete and click **Delete**.

Table 5-14. Procedures for modifying advanced filters

To make this change...	Use this procedure:
Delete an entire block of the equation	Position the cursor on the logical operator at the beginning of the block that you want to delete and click **Delete Block**.
Duplicate an entire block of the equation	Position the cursor on the logical operator at the beginning of the block that you want to duplicate and click **Duplicate Block**.
Discard the entire equation	Click **Clear Equation**. When the Verification box is displayed, click **Yes**.

Table 5-14. Procedures for modifying advanced filters

5.7.3.10 Saving a Filter Equation

You can save the filter equations that you create and retrieve them for later use.

To save a filter equation:

1. In the Advanced Filter dialog box (Figure 5-20), click **Save Filter Equation**.

   The Save As dialog box is displayed.

2. Type the name of the filter equation file that you are saving. (The default extension for filter equation files is .FEQ.)

3. Click **OK**.

   Your filter equation is saved to the /FILTERS directory and you return to the Advanced Filter dialog box.

5.7.3.11 Loading a Filter Equation

The **Load Filter Equation** option on the Advanced Filter dialog box enables you to load a previously saved filter equation into the Advanced Filter dialog box.

To load a saved filter equation:

1. In the Advanced Filter dialog box (Figure 5-20), click **Load Filter Equation**.

   The Open dialog box is displayed.

2. Highlight the name of the filter equation file that you want to load.

   Description displays the descriptive label that you saved with the file.

3. Click **OK**.

   You return to the Advanced Filter dialog box and the filter equation that you specified appears in the Advanced Filter Equation box.

5.7.4 Saving Filtered Frames to a Capture File

After filtering the network traffic in the capture buffer, you can save the filtered frames to a new capture file.

To save filtered frames to a new capture file:

1. From the menu bar, choose **File/Save As**.

   The Save Capture File dialog box appears (Figure 5-28).

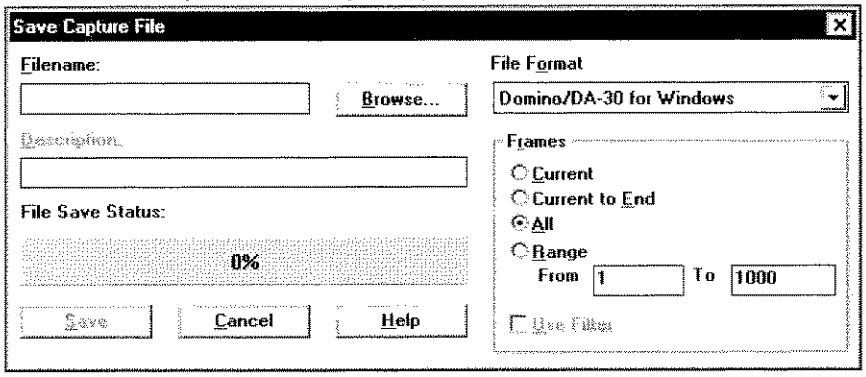


Figure 5-28. Save Capture File dialog box

2. In **Filename**, type a filename to use for the new capture file.
3. To save the file to a different drive or directory, click **Browse**.

   The Capture Filename dialog box appears, allowing you to specify the drive, directory, or file type for the new capture file.
4. When you return to the Save Capture File dialog box, select a file format for the new capture file.
5. In **Frames**, select **Use Filter** and choose the range of frames that you want to save. You can choose any of the following:
   - the current frame
   - all of the frames between the current frame and the end of the capture buffer
   - all of the frames in the capture buffer
   - a specified range of frames
6. Click **Save**.

   Examine saves the filtered frames to the specified capture file. The File Save Status bar indicates the progress of the save. After Examine has saved the new capture file, you return to the Examine screen.

5.8 Working with Data from the Capture Buffer

While you are using Examine to view captured traffic you can:

- modify the protocol stack
- select the character code
- manage timestamping
- enable packet reassembly
- enable protocol scanning
- select the protocol display format and colors
- select the fields that you want to display or hide in the results windows
- synchronize displays

These tasks are explained in the sections that follow.

5.8.1 Modifying the Protocol Stack

While you are examining captured network traffic, you can use the **Protocol Stack** command on the **Buffer** menu to rearrange the protocols that are loaded on the stack. You can also remove protocols that are loaded, replaced loaded protocols, or load additional protocols, as needed.

To modify the protocol stack:

♦ From the menu bar, choose **Buffer/Protocol Stack**.

The Protocol Stack dialog box appears (Figure 5-29).

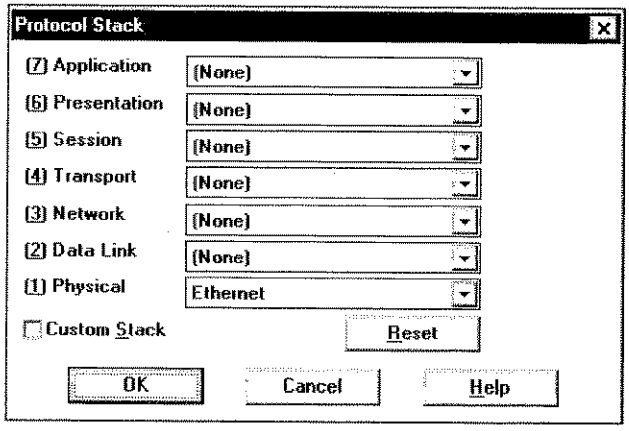


Figure 5-29. Protocol Stack dialog box

NOTE: For the Domino analyzer to be able to decode a protocol, the software for that protocol must be installed and the protocol must be identifiable by the protocol at the preceding layer. A protocol that cannot be identified by the preceding protocol can be decoded only if you load that protocol and the one that precedes it at the appropriate layers on the protocol stack.

When analyzing WAN traffic, you must load the first protocol on the protocol stack, for example, Frame Relay, HDLC, or SDLC. Also, because WAN protocols typically lack the ability to detect the next layer protocol, it is advisable to load the upper layer protocols that you want to decode on the stack as well.

5.8.1.1 Rearranging the Protocol Stack

You can load protocols on the protocol stack at their default layer or at any layer that you choose. This is controlled by the **Custom Stack** feature on the Protocol Stack dialog box (Figure 5-29).

To select protocols to load:

Task	Action
To load a protocol at any layer	Select **Custom Stack** to enable the feature.
To load a protocol at its default layer	Clear **Custom Stack** to disable the feature.

Table 5-15. Protocol loading procedures

5.8.1.2 Changing Protocols

You can use the Protocol Stack dialog box (Figure 5-29) for the following protocol tasks:

- Add
- Replace
- Remove
- Set up

To change the protocol stack:

Task	Action
To add an additional protocol:	1. Use the cursor to select the layer where you want to load the additional protocol. 2. Use the Up Arrow or Down Arrow to scroll through the list of available protocols and select the protocol that you want to load. 3. Click **OK** to re-analyze the capture network traffic.
To remove a protocol:	1. From the Protocol Stack dialog box select the layer and the protocol to be deleted. 2. Select **(None)** option and click **OK**.
To replace a protocol:	1. From the Protocol Stack dialog box select the layer and the new protocol that you want to load. 2. Click **OK**.
To set up a protocol:	1. If the selected protocol has a Setup button, click **Setup**. 2. Make any necessary changes to the protocol setup.

Table 5-16. Procedures for modifying the protocol stack

The protocol stack options enable you to decode traffic at all layers of the OSI Reference Model. However, the analyzer's ability to decode all traffic correctly is limited if the traffic includes proprietary protocol encapsulations.

The Glue protocol software lets you obtain accurate protocol decodes at all layers, even when proprietary protocol information is present. With the Glue software, you can define fields that account for the bytes occupied by the proprietary protocol. When the software is loaded at the appropriate layer and customized in this way, the analyzer can decode the intervening protocol encapsulation. Then the protocols loaded at succeeding layers can be decoded accurately.

For information about loading and using the Glue protocol software, see Chapter 2 "Setting Up."

5.8.2 Changing the Character Code Format

While examining captured frames, you can select the data transmission character code. The character code:

- controls the way the Domino system interprets the data that it captures from or transmits onto the network
- affects the display of the Hexadecimal Trace and Character Trace windows

To select the character code:

1. From the menu bar, choose **Buffer/Character Code**.
2. From the **Character Code** submenu, choose one of the following options:
   - **ASCII_EXT**
   - **ASCII**
   - **EBCDIC**
   - **EBCD**

   The character code is set and a check mark appears next to the selected option.

5.8.3 Timestamping

In the Examine results windows, the Domino analyzer assigns a timestamp to each frame. The timestamp is expressed in tens of microseconds in the form HH:MM:SS.ssss. The Examine **View** menu provides you with options to display the timestamp in three different types:

- **absolute time**
- **relative time**
- **delta time**

The timestamp types and their functions are described in Table 5-17.

Timestamp type	Function
Absolute time	Indicates the time at which the analyzer received the frame.
Relative time	Indicates the number of seconds that have elapsed between the mark that you have set using the **Set Mark** command and when the analyzer receives the current frame.

Table 5-17. Timestamp types

Timestamp type	Function
Delta time	Indicates the interframe delay - the number of seconds elapsed between the time that the analyzer received the previous frame and the time that it received the current frame.

Table 5-17. Timestamp types

You can select the timestamp type that appears in the Hex Trace window and the Protocol Detail window.

In the Frame Summary window and the protocol summary windows, you can display none, any, or all of the timestamp types.

On the **View** menu, a check mark appears next to the type that is in effect.

To select the timestamp type:

Task	Action
To select the timestamp type	From the menu bar, choose **View**, and then choose **Absolute**, **Relative**, or **Delta Time** to toggle the option on.
To hide the timestamp type	From the menu bar, choose **View**, and then choose **Absolute**, **Relative**, or **Delta Time** to toggle the option off.
To set the relative time mark	1. In a results window, move the cursor to the frame that you want to use as the mark. 2. From the menu bar, choose **Buffer/Set Relative Mark**. A box surrounds the marked frame.

Table 5-18. Procedures for selecting the timestamp type

Figure 5-30 illustrates a frame marked for relative timestamping.

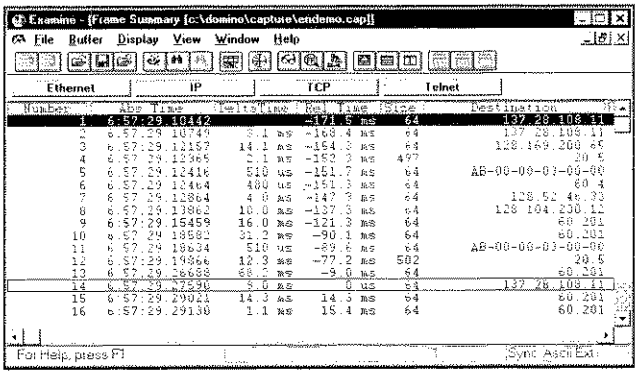


Figure 5-30. Example frame 14 with the relative time mark set

5.8.4 Enabling Packet Reassembly

The **Analysis Options** command on the Examine **Buffer** menu allows you to enable and disable the packet reassembly feature. When packet reassembly is enabled, fragmented frames in the capture buffer are reassembled, which allows correct decoding of upper-level protocol information.

NOTE:

Not all protocols support packet reassembly. A list of the protocols that support reassembly, and for which Domino supports reassembly, is provided in the README.HLP file.

To enable the packet reassembly option:

1. From the menu bar, choose **Buffer/Analysis Options**.

   The Analysis Options dialog box is displayed (Figure 5-31).

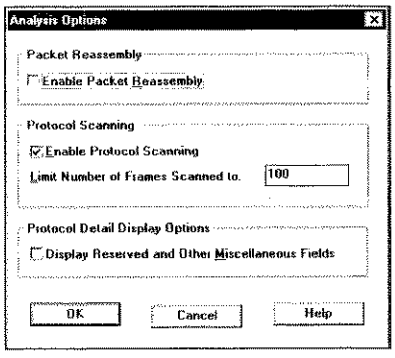


Figure 5-31. Analysis Options dialog box

2. Select **Enable Packet Reassembly** and click **OK**.

   Packet reassembly is enabled for the active capture buffer. The Protocol Detail window specifies which frames contain successfully reassembled fragmented data, and also specifies the frame numbers from which the fragments were reassembled.

To disable the packet reassembly option:

1. From the menu bar, choose **Buffer/Analysis Options**.

   The Analysis Options dialog box (Figure 5-31) is displayed.

2. Clear **Enable Packet Reassembly** and click **OK**.

   Packet reassembly is disabled for the active capture buffer.

5.8.5 Enabling Protocol Scanning

In certain protocols (such as NCP, NFS, and RPC), some frames are dependent on earlier information frames. You can ensure full interpretation of decoded information by enabling Examine to perform protocol scanning. When protocol scanning is enabled, Examine scans the frames preceding a dependent frame to find the information frame that corresponds to it. Because this option might slow down protocol interpretation, you can limit the number of preceding frames that the system scans in search of a corresponding information frame.

To enable protocol scanning:

1. From the menu bar, choose **Buffer/Analysis Options**.

   The Analysis Options dialog box is displayed (Figure 5-31).

2. Under **Frame Detail Display Options**, select **Enable Protocol Scanning**.

3. Specify the maximum number of frames preceding a dependent frame that you want Examine to scan for a corresponding information frame.

4. Click **OK**.

   Protocol scanning is enabled for the current capture buffer.

To disable protocol scanning:

1. From the menu bar, choose **Buffer/Analysis Options**.

   The Analysis Options dialog box is displayed (Figure 5-31).

2. Clear **Enable Protocol Scanning** and click **OK**.

   Protocol scanning is disabled for the active capture buffer.

5.8.6 Selecting the Display Format for Protocol Fields

Examine allows you to select the format that is used to display protocol-specific fields in the Frame Summary, Protocol Summary, and Protocol Detail windows. For example, you can display the Ethernet type field as a mnemonic, decimal, or hexadecimal value.

To select the display format for a protocol field:

1. From the menu bar, choose **View/Protocol Styles**.

   The Select Protocol Styles dialog box appears (Figure 5-32).

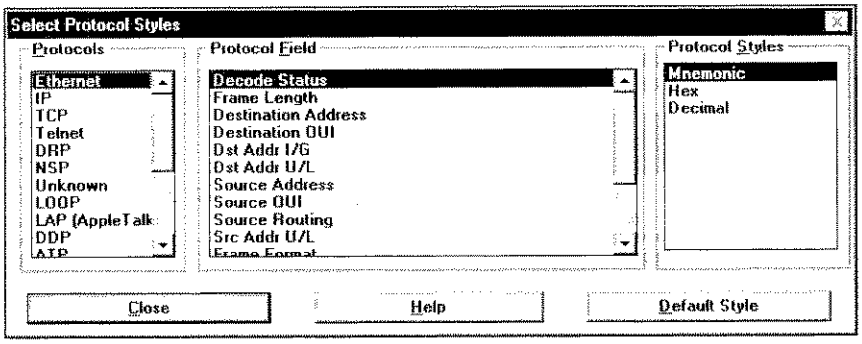


Figure 5-32. Select Protocol Styles dialog box

2. Select the protocol in the **Protocols** box.

   The fields for the selected protocol are displayed in the **Protocol Field** box.

3. In the **Protocol Field** box, select the field for which you want to change the display format.

   The available display formats are displayed in the **Protocol Styles** box.

4. In the **Protocol Styles** box, select one of the available display formats.

5. Click **OK**.

   You return to the Examine screen and the field is displayed in the selected display format.

5.8.7 Selecting Display Colors by Protocol

Examine allows you to define the colors that are used for displaying each protocol in the frame contents. Colors can make it easier for you to locate specific protocols or protocol-specific information. You can use this feature if the computer connected to your Domino analyzer has a VGA monitor.

To select display colors by protocol:

1. From the menu bar, choose **View/Protocol Colors**.

   The Select Protocol Colors dialog box appears (Figure 5-33).

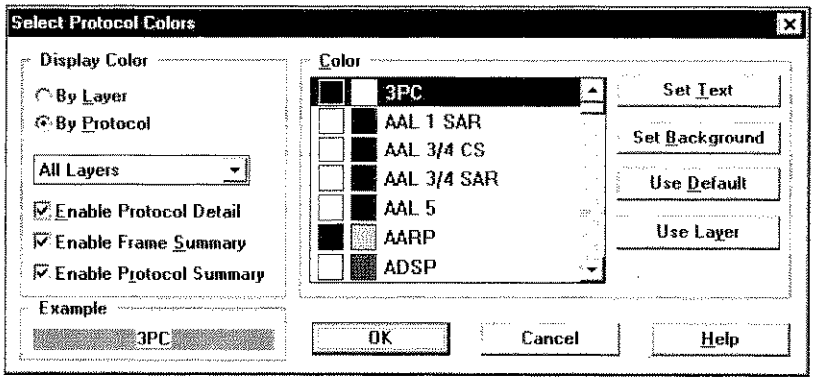


Figure 5-33. Select Protocol Colors dialog box

2. Choose **By Protocol** in the **Display Color** box.
3. Choose **All Layers** in the **Layers** list box.

   All of the protocols that have been detected in the capture buffer are displayed in the **Color** box.

4. In the **Color** box, choose a protocol to which you want to assign a color.
5. Do one of the following:

   - To change the color that is used to display the text of the protocol, click **Set Text**.
   - To change the color that is used to display the background for the protocol, click **Set Background**.

   The Select Color dialog box appears (Figure 5-34).

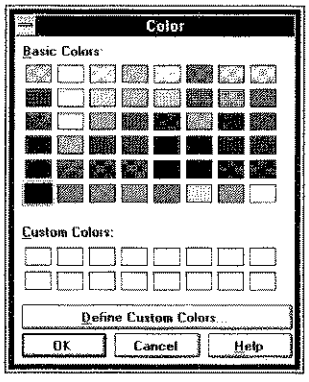


Figure 5-34. Select Color dialog box

6. Do one of the following:
   - Choose one of the basic colors.
   - Click **Define Custom Colors** to expand the dialog box and define a custom color.
7. Click **OK**.

   You return to the Select Protocol Colors dialog box and the selected color is assigned to the selected protocol.
8. Repeat steps 4 through 7 to assign text or background colors to each of the protocols.
9. Click **OK**.

   You return to the Examine screen and the assigned protocol colors are activated.

5.8.8 Displaying or Hiding Fields in Summary Windows

The **Display Options** command on the **View** menu allows you to specify which fields are displayed in the current window. This command is available for the Frame Summary window or any Protocol Summary window.

When you choose the **Display Options** command, Examine displays either the Frame Summary Display Options dialog box or the Protocol Summary Display Options dialog box, depending on which results window is active when you choose the command. In either dialog box you can specify which fields are displayed and which fields are hidden in the corresponding results window.

5.8.8.1 Displaying or Hiding Fields in Frame Summary

To display or hide fields in the Frame Summary window:

1. If necessary, select the Frame Summary window to make it the active window.
2. From the menu bar, chose **View/Display Options**.

   The Frame Summary Display Options dialog box appears (Figure 5-35).

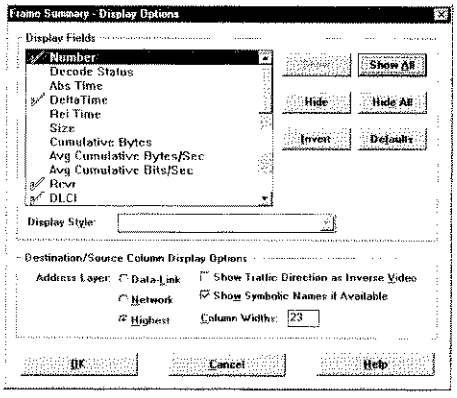


Figure 5-35. Frame Summary Display Options dialog box

3. In **Display Fields**, select the fields that you want to display:
   - To display a field, click **Show**.
   - To hide a field, click **Hide**.
   - To display all of the available fields, click **Show All**.
   - To clear all of the selections, click **Hide All**.
   - To display all of the currently hidden fields and hide all of the currently displayed fields, click **Invert**.
   - To display the default fields, click **Defaults**.

   Check marks appear next to each field that is selected for display.
4. For some fields, you can select the format in which the field is displayed. For such fields, **Display Style** becomes active when the field is highlighted in the **Display Fields** list. Select the format that you want for each of these fields.
5. Click **OK**.

   You return to the Examine screen and the selected fields are displayed in or hidden from the Frame Summary window.

5.8.8.2 Selecting Display Options for the Frame Summary

Examine offers a number of display options that you can apply to the data in the Frame Summary window:

- You can specify the layer for which source and destination addresses will be displayed.
- If you are examining WAN data, you can choose to reverse the background and typeface colors to indicate the change of direction of WAN traffic flow.

- You can choose to display symbolic names instead of addresses in the **Destination** and **Source** columns.

To select display options for the Frame Summary:

1. If necessary, select the Frame Summary window to make it the active window.
2. From the menu bar, chose **View/Display Options**.

   The Frame Summary Display Options dialog box appears (Figure 5-35).
3. Select the display options that you want; then click **OK**.

   The display in the Frame Summary window changes to match your selections.

To specify the layer for source and destination addresses:

♦ From the Frame Summary Display Options dialog box (Figure 5-35), in the **Layer of Addresses** box, select the layer that you want:

- **Data-Link** displays the lowest layer addresses: DTE, DCE, DLC, CPE, NET.
- **Network** displays IP addresses.
- **Highest** displays the highest layer address that is detected by the decode.

To display changes of direction in WAN traffic flow:

♦ From the Frame Summary Display Options dialog box (Figure 5-35), click **Show WAN Direction as Inverse Video**.

The direction of traffic flow for each frame is indicated by color: Frames going from DTE to DCE are shown in white, and frames going from DCE to DTE are shown in black. (Black and white are the default colors. If you have selected other default colors, the traffic direction display will reflect those selections.)

To display symbolic names instead of addresses:

1. From the Frame Summary Display Options dialog box (Figure 5-35), click **Show Symbolic Names if Available**.
2. You might want to adjust the column width if you are displaying names instead of addresses. Adjust the width in the **Column Widths** box.

5.8.8.3 Displaying or Hiding Fields in Protocol Summary

To display or hide fields in the Protocol Summary window:

1. If necessary, select the Protocol Summary window to make it the active window.
2. From the **View** menu, choose **Display Options**.

   The Protocol Summary Display Options dialog box is displayed (Figure 5-36).

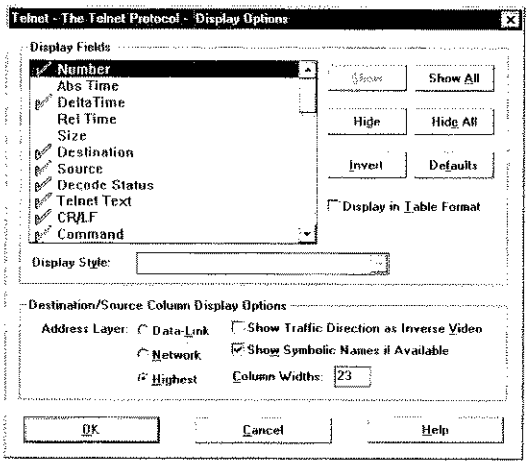


Figure 5-36. Protocol Summary Display Options dialog box

3. In **Fields**, select the fields that you want to display or hide:
   - To display a field, click **Show**.
   - To hide a field, click **Hide**.
   - To display all of the available fields, click **Show All**.
   - To clear all of the selections, click **Hide All**.
   - To display all of the currently hidden fields and hide all of the currently displayed fields, click **Invert**.
   - To display the default fields, click **Default**.

   Check marks appear next to each field that is selected for display.
4. For some fields, you can select the format in which the field is displayed. For such fields, **Protocol Styles** becomes active when the field is highlighted in the **Protocol Fields** list. Select the format that you want for each of these fields.
5. Click **OK**.

   You return to the Examine screen and the selected fields are displayed in or hidden from the Protocol Summary window.

5.8.8.4 Selecting Display Options for a Protocol Summary

You can choose to display protocol summary data in a table instead of the more compressed Interpretation format. If you are examining WAN data, you can choose to reverse the background and typeface colors to indicate the change of direction of WAN traffic flow.

To select display options for a protocol summary:

1. If necessary, select the protocol summary window to make it the active window.
2. From the **View** menu, choose **Display Options**.

   The Protocol Summary Display Options dialog box is displayed (Figure 5-36).
3. Select the display options that you want; then click **OK**.

   The display in the protocol summary window changes to match your selections.

To display the protocol summary in table format:

- From the Protocol Summary Display Options dialog box (Figure 5-36), select **Display in Table Format**.

To display changes of direction in WAN traffic flow:

- From the Protocol Summary Display Options dialog box (Figure 5-36), select **Show WAN Direction in Inverse Video**.

  The direction of traffic flow for each frame is indicated by color: Frames going from DTE to DCE are shown in black on white, and frames going from DCE to DTE are shown in white on black. (If you have selected a background color other than white, the traffic direction display reflects that selection.)

5.8.8.5 Displaying Miscellaneous Fields

You can enable the Protocol Detail window to display reserved fields and other miscellaneous limited-use protocol fields.

To display reserved and miscellaneous protocol fields:

1. From the menu bar, choose **Buffer/Analysis Options**.

   The Analysis Options dialog box appears (Figure 5-37).

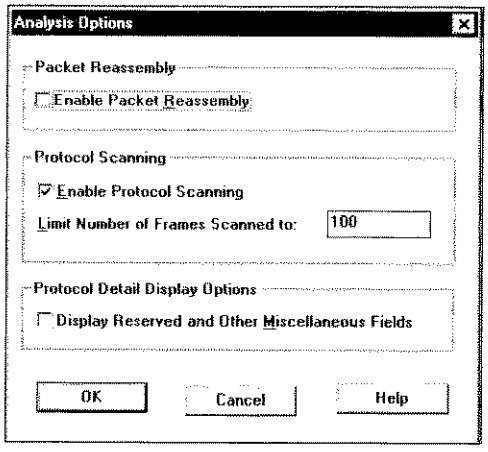


Figure 5-37. Analysis Options dialog box

2. Select **Display Reserved and Other Miscellaneous Fields**.
3. Click **OK**.

   You return to the Examine screen and the miscellaneous fields are displayed when you view the Protocol Detail window.

5.8.9 Synchronizing the Currently Displayed Results Windows

When you are working in Examine, you can synchronize all of the currently displayed windows for a capture buffer. When you synchronize the windows, you can scroll through the buffer and display the same frame in all of the windows at the same time.

To synchronize the currently displayed windows:

- From the Examine menu bar, choose **Buffer/Sync All**.

All of the currently displayed windows for the current capture buffer are synchronized

Shortcut:
Click the Sync button  on the Examine toolbar.

5.9 Printing Captured Network Traffic

You can print the frame content in the format in which it appears in the following results windows:

- Frame Summary
- Hexadecimal Trace
- Character Trace (DominoWAN only)
- Protocol Detail
- Protocol Summary

5.9.1 Setting Up to Print

Examine offers a number of print options that you can apply when you print capture data:

- You can select the printer and the font that you want to use.
- You can select whether to wrap or clip the data to fit it on a page or whether to extend the data across pages.
- You can specify a header or a footer to appear on each printed page.
- You can include the Receiver column in your printout.

To select the printer, the page orientation, and the paper size:

♦ From the menu bar, choose **File/Print Setup**.

The Print Setup dialog box (Figure 5-38) appears, in which you can make your selections.

You can also open the Print Setup dialog box by clicking **Printer Setup** in the Examine Print dialog box (Figure 5-39).

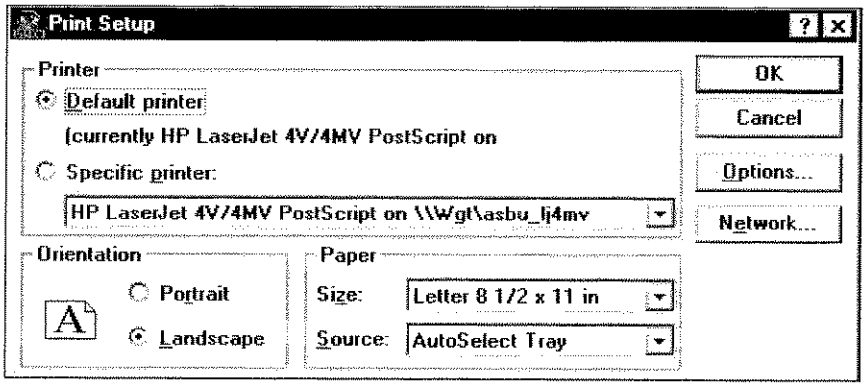


Figure 5-38. Print Setup dialog box

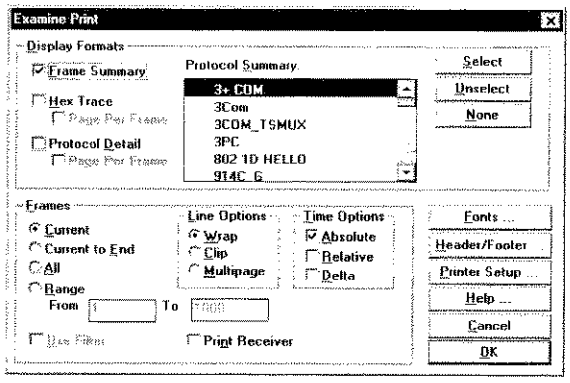


Figure 5-39. Examine Print dialog box

To select the font in which you want to print:

1. From the menu bar, choose **File/Print**.

   The Examine Print dialog box appears (Figure 5-39).

2. Click **Fonts**.

   The Font dialog box appears, in which you can select from the font types and sizes that are available on the selected printer.

To select whether to wrap, clip, or extend data:

1. From the menu bar, choose **File/Print**.

   The Examine Print dialog box appears (Figure 5-39).

2. Under **Line Options**, select one of the following:

Option	Prints...
Wrap	The full contents of each frame, wrapped to the next line if necessary.
Clip	As much of the contents of each frame as will fit on a single line.
Multipage	The full contents of each frame, extended across multiple pages if necessary.

Table 5-19. Print line options

To specify a header or footer:

1. From the menu bar, choose **File/Print**.

   The Examine Print dialog box appears (Figure 5-39).

   Click **Header/Footer**.

2. The Header/Footer Setup dialog box (Figure 5-40) appears, in which you can select what you want to print in a header or footer and how you want the header or footer aligned on the printed page.

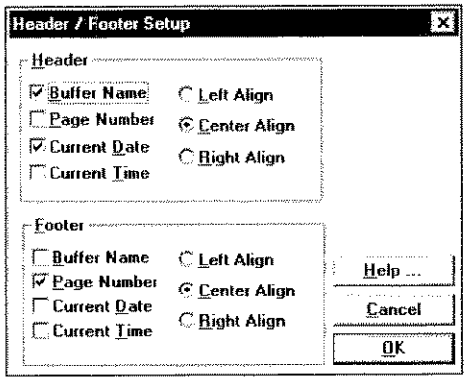


Figure 5-40. Header/Footer Setup dialog box

To include the Receiver column in your printout:

1. From the menu bar, choose **File/Print**.

   The Examine Print dialog box appears (Figure 5-62).

2. Click **Print Receiver**.

   The Receiver column will be included in your printout whether or not it is currently displayed in the results window.

5.9.2 Selecting What You Want to Print

In the Examine Print dialog box, you can select the results windows or the portion of the capture buffer that you want to print. You can print the current frame, all of the frames between the current frame and the end of the capture buffer, all of the frames in the capture buffer, or a specified range of frames. You can also choose whether you want to print all of the specified frames or just those that have been filtered in.

To select what you want to print:

1. From the menu bar, choose **File/Print**.

   The Examine Print dialog box appears (Figure 5-39).

2. In the **Display formats** box, select the type of results window that you want to print.

   If you want to print frames from one of the protocol summary windows, select the protocol types for the windows that you want. Click the **Select** and **Unselect** buttons to make your protocol selections.

3. In **Frames**, select the frames that you want. You can choose from the following:

Option	Prints...
Current	The current frame in each of the results windows that you selected under Display Formats
Current to End	The range of frames that starts with the current frame and ends with the last frame in the capture buffer for each results window that you selected
All	To print all of the frames in the capture buffer for the results windows that you selected
Range	The frames numbered in the range that you specify in the From and To boxes

Table 5-20. Print frame selection options

4. Under **Time Options**, select which of the timestamp options that you want to use when printing the specified frames.
5. Select **Use Filter** if you want to print only filtered frames.
6. Click **OK**.

Examine prints the specified frames in the selected format and you return to the Examine screen.

If you are working in a results window and you know that you want to print a particular frame, or all of the frames from a particular frame forward, move your cursor to that frame before you select **Print** from the menu bar. Then you can select **Current** or **Current to End** in the Print dialog box.

5.10 Exporting Captured Frames to a CSV File

In Examine, you can export the contents of the capture buffer to a comma-separated value (CSV) file. The system exports the contents from the location that corresponds to your cursor position to the end of the buffer. You can initiate export from either the Frame Summary window (Figure 5-5) or a protocol summary window (Figure 5-10).

To export captured frames to a CSV file:

1. Position your cursor at the point from which you want to start the export.
2. From the **File** menu, choose **Export to CSV**.

   The Export to CSV File dialog box is displayed (Figure 5-41).

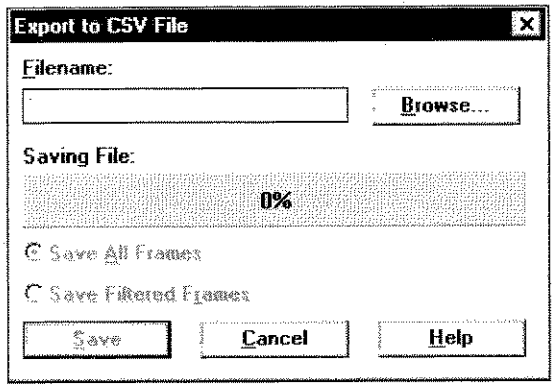


Figure 5-41. Export to CSV File dialog box

3. In **Filename**, type a filename to use for the CSV file.
4. To save the file to a different drive or directory click **Browse**.

   The Export Filename dialog box is displayed allowing you to specify the drive,

directory, or file type for the CSV file.

5. When you return to the Export to CSV File dialog box, do one of the following:
   - To export all of the frames in the capture buffer to the CSV file, click **Save All Frames**.
   - To export only the filtered frames to the CSV file, click **Save Filtered Frames**.
6. Click **Save**.

   Examine saves the exports of the capture buffer to the specified CSV file. The Saving File bar indicates the progress of the export procedure. After Examine has finished exporting the frames to the CSV file, you return to the Examine screen.

5.11 Exporting Captured Frames to a Text File

In Examine, you can export the contents of the capture buffer to a text file. The system exports the contents from the location that corresponds to your cursor position to the end of the buffer. You can initiate export from either the Frame Summary window or a protocol summary window.

To export captured frames to a text file:

1. Position your cursor at the point from which you want to start the export.
2. From the **File** menu, choose **Export to Text**.

   The Export to Text File dialog box is displayed.
3. In **Filename**, type a filename to use for the text file.
4. To save the file to a different drive or directory click **Browse**.

   The Export Filename dialog box is displayed allowing you to specify the drive, directory, or file type for the text file.
5. When you return to the Export to Text File dialog box, do one of the following:
   - To export all of the frames in the capture buffer to the text file, click **Save All Frames**.
   - To export only the filtered frames to the text file, click **Save Filtered Frames**.
6. Click **Save**.

   Examine saves the contents of the capture buffer to the specified text file. The Saving File bar indicates the progress of the export procedure. After Examine has finished exporting the frames to the text file, you return to the Examine screen.

6. Transmitting Traffic to the Network

The Transmit application enables you to play back a capture file while simultaneously transmitting it onto the network. It also enables you to edit single frames from a capture file and transmit them onto the network.

6.1 Starting the Transmit Application

Transmit is one of the four main Domino functions that are available from the Workbench screen, which is the first screen you see when you start the Domino software. To learn more about the Workbench screen and how to prepare to use an application, see Section 1.3, "The Domino Workbench."

To start the Transmit application:

- Choose **Transmit** from the **Workbench** menu or click the Transmit button.

  The Transmit screen is displayed (Figure 6-1).

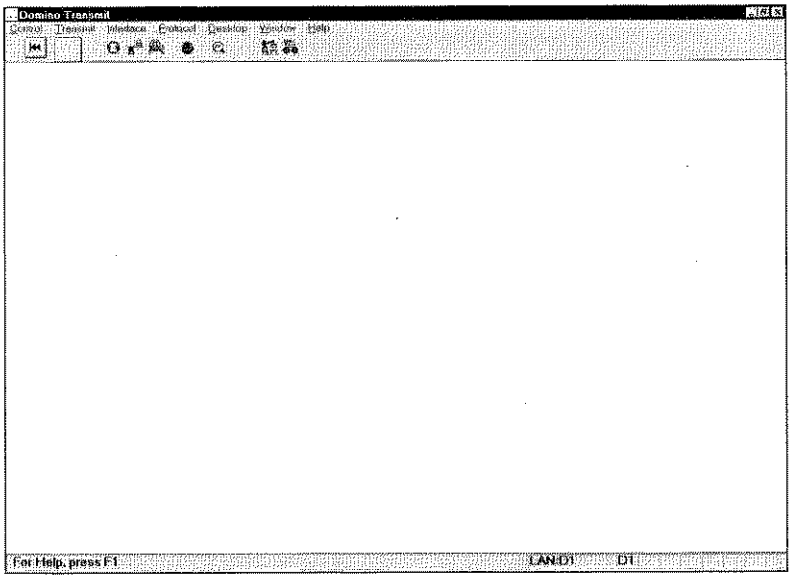


Figure 6-1. Transmit screen

6.2 Playing Back a Capture File

Transmit provides an External Playback feature, which plays back a capture file to the Domino analyzer and simultaneously transmits the file's contents onto the network.

To play back a capture file:

1. From the menu bar, choose **Transmit/Playback**.

   The Open Capture File dialog box is displayed (Figure 6-2).

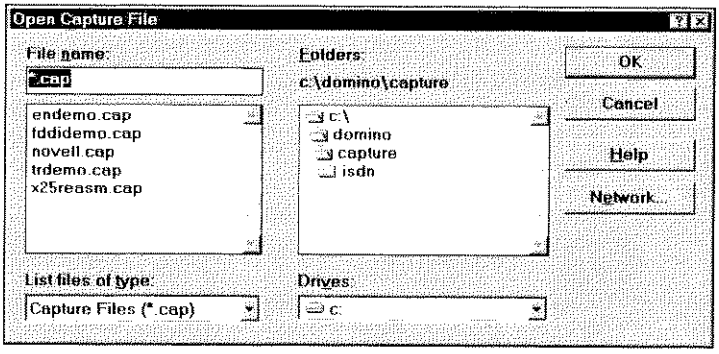


Figure 6-2. Open Capture File dialog box

2. Select a capture file to play back.

   The External Playback dialog box is displayed and playback starts (Figure 6-3).

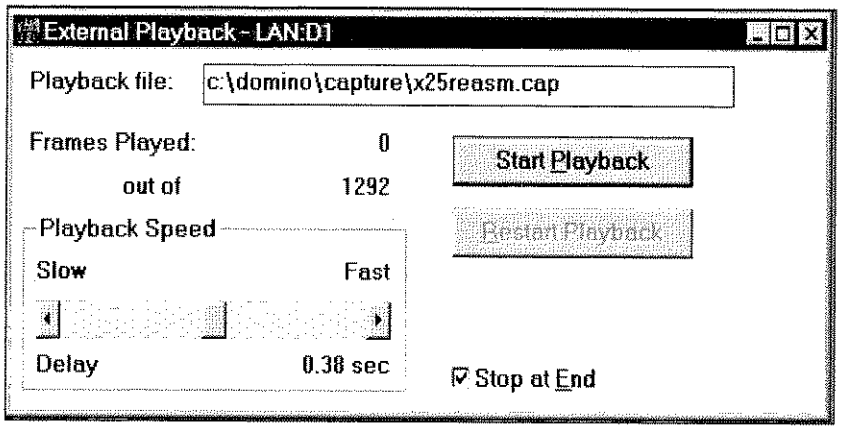


Figure 6-3. External Playback dialog box

3. After the capture file has been played back, close the External Playback dialog box.

If the **Stop at End** option is enabled (the default), transmission stops when the last frame in the capture file has been played back. When all frames in the capture file have been played back, the **Pause/Resume** button changes to the **Playback Again** button; and the External Playback dialog box displays the message "All Frames Played!"

To repeat playback of the capture file:

- In the External Playback dialog box, click **Playback Again**.

  Transmission of the capture file begins and continues until all frames have been transmitted or until you click **Pause** or close the dialog box.

6.2.1 Changing the Playback Speed

Use the **Playback Speed** control on the External Playback dialog box to adjust the speed at which the capture file is played back.

To change the speed at which the capture file is played back:

- In the External Playback dialog box, move the scroll box to the right to speed up the playback or to the left to slow down the playback of the capture file.

6.2.2 Stopping the Playback of a Capture File

While playing back a capture file, you might need to stop the playback of frames. For example, if a specific frame or event that you are looking for has occurred, you might not need to see the remaining frames in the capture file.

To stop the playback of a capture file:

- In the External Playback dialog box, click **Pause**.

To restart the playback of a capture file:

- In the External Playback dialog box, click **Resume**.

6.2.3 Playing Back a Capture File Frame by Frame

You might find it useful to play back a capture file frame by frame. In this way, you can view statistics and protocol information for each frame in succession to isolate an event that has occurred on the network.

To play back one frame at a time:

1. In the External Playback dialog box, move the **Playback Speed** alll the way to the left.

   This changes the playback speed to **Manual** and enables the **Play Next Frame** button.

2. Click **Play Next Frame** to play back the next frame in the capture file.

   Repeat this step each time that you want to play back another frame from the capture file.

6.2.4 Enabling Continuous Playback of a Capture File

When you play back a capture file from the Playback dialog box, transmission stops at the end of the file or when you click **Pause**. However, you might want to set up a network test that requires uninterrupted transmission of data for an unspecified period of time. You can do this by disabling the **Stop at End** option in the Playback dialog box. Then, when you start Playback, the file will be transmitted repeatedly until you stop it.

To enable continuous playback of a capture file:

- In the External Playback dialog box, clear the **Stop at End** check box.

6.3 Building and Editing Frames

The Build Frame component of the Transmit application enables you to build a test frame to your specifications by editing frames from a capture file. You can then transmit individual frames onto the network. Sample capture files are included for you to use with Build Frame. The general file is SAMPLES.CAP, and the two bisync files are SAMPBSCA.CAP and SAMPBSCB.CAP.

6.3.1 Opening a Capture File

When you select **Build Frame** from the **Transmit** menu, the Build Frame dialog box is displayed with SAMPLES.CAP, or the last opened capture file, loaded into the frame buffer. You may want to work with frames from another capture file. You can access previously saved capture files from this dialog box.

To open a capture file:

1. From the menu bar, choose **Transmit/Build Frame**.

   The Build Frame dialog box is displayed (Figure 6-4).

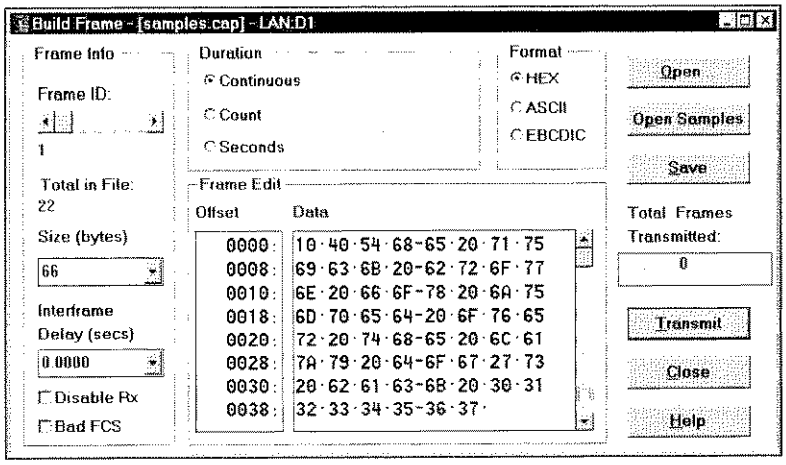


Figure 6-4. Build Frame dialog box

2. From the Build Frame dialog box, click **Open**.

   The Open Capture File dialog box is displayed (Figure 6-2).

3. From the **Capture** subdirectory, select the capture file that you want to work with and click **OK**.

   You return to the Build Frame dialog box. The first frame of the selected capture file appears in **Frame Edit**, and the name of the capture file is displayed on the Build Frame dialog box title bar.

6.3.2 Opening the Samples Capture File

The file SAMPLES.CAP is displayed by default the first time that you open the Build Frame dialog box. You close the SAMPLES.CAP file automatically when you select an alternate capture file to edit. Because it serves as the default frame buffer content, SAMPLES.CAP is not stored in the Capture subdirectory. This safeguards against accidental deletion of the file, but it also prevents access to the file through the Open Capture File dialog box when you want to restore SAMPLES.CAP to the frame buffer.

To open the SAMPLES.CAP file:

- From the Build Frame dialog box (Figure 6-4), click **Open Samples**.

  The first frame of the SAMPLES.CAP file appears in the Frame Edit box and the filename SAMPLES.CAP is displayed on the dialog box title bar.

6.3.3 Editing Frames

To edit a frame from a capture file:

1. In the Build Frame dialog box (Figure 6-4), under **Frame ID**, use the scrollbar to select the ID of the frame that you want to edit.
2. Under **Format**, select the format that you want the frame content displayed in, **HEX**, **ASCII**, or **EBCDIC**.
3. Under **Frame Edit**, edit the content of the frame.

   You cannot save the changes that you make to a frame in SAMPLES.CAP, SAMPBSCA.CAP, or SAMPBSCB.CAP. If you edit a frame from these files, your next step is to transmit the frame.

   If you are editing another capture file, you can transmit the frame that you have changed, or you can save the changes that you made and then either select another frame to edit or transmit the frame onto the network.

6.3.3.1 Selecting a Frame to Edit

When you select a capture file from the Build Frame dialog box, the **Frame Info** box shows:

- the ID of the frame that appears in the **Frame Edit** box
- the total number of frames in the file
- the size of the displayed frame in bytes

The first frame in the selected capture file is displayed by default. You can display any frame in the selected file to edit and transmit, or to transmit in its original state.

To select a frame to edit or transmit:

♦ In the Build Frame dialog box (Figure 6-4), under **Frame ID**, scroll to display the ID of the frame you want to edit.

The content of the selected frame appears in **Frame Edit** and the size of the frame is displayed in **Size**.

6.3.3.2 Changing the Frame Size

Use the **Size** option in the Build Frame dialog box to change the size of the currently-displayed frame.

To change the frame size:

1. In the Build Frame dialog box (Figure 6-4), select **Size**.

   The number of bytes in the currently displayed frame is highlighted in the **Size** list box.

2. Type a number that is smaller than the original number of bytes in the frame, or select a number from the scrollable list.

   The data that is displayed in **Frame Edit** is truncated to the number of bytes that you specified.

6.3.3.3 Selecting the Interframe Delay

You can control the speed at which frames are transmitted onto the network by changing the interframe delay.

To select the interframe delay:

1. In the Build Frame dialog box (Figure 6-4), select **Interframe Delay**.

   The current interframe delay is highlighted.

2. Type an interframe delay (up to one second in length), or select a delay from the scrollable list.

6.3.3.4 Selecting the Data Format for Display

You can select how to display the frame content in the **Data** segment of the **Frame Edit** box.

To select the data format for the frame display:

- In the Build Frame dialog box (Figure 6-4), under **Format**, select **HEX**, **ASCII**, or **EBCDIC**.

  If you select **HEX**, a hex dump of the frame is displayed. If you select **ASCII**, the printable ASCII character representation for the frame is displayed with non-printable characters shown in hexadecimal format. If you select **EBCDIC**, the printable EBCDIC character representation for the frame is displayed with non-printable characters shown in hexadecimal format.

6.3.3.5 Changing the Data in the Frame

The **Data** segment of the **Frame Edit** box in the Build Frame dialog box displays the data in the currently selected frame. You can scroll through the data in the frame, insert and delete data from the frame, and copy data from one part of the frame to another.

To scroll through the data:

- Use the scroll bar to move up and down through the contents of the frame. Use the arrow keys to move the cursor to a specific character.

To insert characters in the data:

- Place the cursor on the character before which you want the new data to be inserted and type the new data.

When you insert new data into the frame, characters are deleted from the end of the frame so that the original frame size is maintained.

To delete characters from the data:

- Highlight the character or characters that you want to delete and press **Delete**.

To copy data from one part of the frame to another:

1. Highlight the character or characters that you want to copy and press **Ctrl+C**.
2. Move the cursor to the place in the frame to which you want to copy the data and press **Ctrl+V**.

To add data from another application to a frame:

You can add data to a frame from any Windows application that enables you to copy information to the Clipboard.

1. Open the application. Highlight the text that you want to copy and press **Ctrl+C**.

   The highlighted text is copied to the Clipboard.
2. Press **Alt+Tab** to return to the Build Frame dialog box, position the cursor where you want the new data, and press **Ctrl+V**.

   The text from Clipboard is pasted into the frame that you are editing.

6.3.4 Saving the Edited Capture File

If you are working with a capture file other than SAMPLES.CAP, SAMPBSCA.CAP, or SAMPBSCB.CAP you can save any changes that you make to frames in the file from the Build Frame dialog box.

To save changes in frame data:

- In the Build Frame dialog box (Figure 6-4), click **Save**.

The changes you made to the selected frame are saved to the capture file.

6.4 Transmitting a Single Frame

You can transmit a single frame onto the network from the Build Frame dialog box. It provides options for specifying the duration of the transmission, and for starting and stopping the transmission.

To transmit a single frame:

1. From the menu bar, select **Transmit/Build Frame**.

   The Build Frame dialog box (Figure 6-4) is displayed.

2. From the SAMPLES.CAP capture file, or an alternate capture file, select a frame to transmit.
3. Under **Duration**, select one of the three following transmit duration options:

Option	Description
Continuous	Selecting this option floods the network; the selected frame is transmitted continuously until you select **Stop Transmit**.
Count	The selected frame is transmitted repeatedly for the specified number of times.
Seconds	The selected frame is transmitted for the specified number of seconds.

4. Click **Transmit**.

   Transmission of the frame continues until the selected duration condition is met or until you click **Stop Transmit**. The **Total Frames Transmitted** counter is incremented each time the frame is transmitted.

6.5 Using the Bit Error Ratio Test (BERT) Function

A bit error ratio test is used to test the reliability of a digital transmission channel between two points in a network. The test consists of sending a known pattern of bits through a transmission channel from one device to another, comparing the received pattern to the test pattern, and determining whether errors occurred.

BERT testing involves a transmitter and a receiver that independently generate the same bit (test) pattern. Typically, a BERT tester transmits a test pattern that is passed through the device under test and looped back to the BERT tester's receiver on the channel that is under test. This allows for duplex (transmit and receive) line testing with only one BERT tester. It is also possible to have one BERT tester transmit a test pattern on the channel under test to a second BERT tester, which allows for simplex (transmit or receive) line testing.

All the features of a BERT tester are built into the Domino software for the DominoWAN-E1, -T1, and V-series interfaces. The Domino BERT function provides:

- one-way and loopback test options
- twelve test bit patterns
- measurable error insertion (with the introduction of single bit errors or by specifying the ratio of errored bits to non-errored bits)

The error statistics and performance parameters provided by BERT can be used:

- to check the operation of a device (local or remote)
- as acceptance criteria to measure the performance of interconnection devices (such as repeaters) before installing them on a live network
- to check the reliability of the transmission channels between a DTE and DCE as a restart test whenever an interconnection device is upgraded or expanded.

On DominoWAN analyzers, all of the Real Time applications (Transmit, Capture, and Monitor) provide access to the BERT function from the Interface menu. When the analyzer is in Monitor test mode, it can receive BERT patterns in the Monitor or Capture applications. However, to transmit BERT patterns onto the network, you need to set up the analyzer in one of the Emulate test modes (Emulate DTE or Emulate DCE) and start the BERT function from the Transmit application.

The BERT function adjusts the internal configuration of the analyzer for bit-pattern processing. To return the analyzer to normal operating mode, you must exit the application or restart Real Time analysis.

6.5.1 Setting Up the E1 Interface for BERT Testing

You can use the DominoWAN-E1 BERT function for both one-way BERT testing and BERT testing on a looped-back line.

The one-way test configuration uses two analyzers configured as BERT testers, both of which transmit a specified BERT pattern and receive the transmission of the other tester. This configuration allows outgoing and incoming lines to be verified independently.

BERT testing on a looped-back line can be implemented with:

- a single analyzer in Emulate mode with loopback on the entire E1 link
- a single tester in Drop & Insert mode, with BERT patterns inserted on selected channels.

Preparing the DominoWAN-E1 to act as a BERT tester entails both:

- setting up the E1 interface
- making up the correct physical connections between the analyzer and the network or CPE

You need to perform these interface setup procedures before you set up and run a BERT.

Section 6.5.1.1 "Setting Up the E1 Interface for One-way BERT Testing" through Section 6.5.1.3 "Setting Up the E1 Interface for a Bit Error Ratio Test Using Drop & Insert", provide information about setting up for different types BERT testing on an E1 interface.

6.5.1.1 Setting Up the E1 Interface for One-way BERT Testing

For one-way BERT testing, you set up two DominoWAN-E1 analyzers to act as BERT testers. Both analyzers are set up in Emulate mode. Each analyzer transmits a specified BERT pattern through the network or devices under test and receives the transmission of the other tester. This configuration allows incoming and outgoing lines to be verified independently.

When you connect the E1 interface module to the network, you can use the setup that emulates either the network or a CPE.

To set up the E1 interface for one-way BERT testing:

1. From the **Analyzers Present** section of the Workbench screen, click **Setup** for the DominoWAN-E1 you want to configure for BERT testing.
2. From the 2 Mbps Interface Setup dialog box, click **Manual**.
3. On the 2 Mbps Manual Setup dialog box set the options for the transmitter and receivers on both analyzers as follows:

Transmitter:

Option	Selection
Test mode	**Emulate**.
Tx clock	Network dependent; typically **Loop Timed**.
Data channels	Select the channels that you intend to test.
Framing, line code	As required by the network.

Receiver:

Option	Selection
Test mode	**Emulate**.
Receiver 2	Must be selected for BERT testing. Set termination to **Terminate**.
Receiver 1	Not used for BERT testing.
Data channels	Same channels as on the transmitter.

4. To return to the 2 Mbps Interface Setup dialog box, click **OK**.

6.5.1.2 Setting Up the E1 Interface for BERT Testing with Loopback

The setup for BERT testing using a single tester with loopback entails setting up a DominoWAN-E1 in Emulate mode with both transmitter and receiver enabled. (You must also verify the implementation of loopback on the E1 link you are testing.)

To set up the E1 interface for BERT testing with loopback:

1. From the **Analyzers Present** section of the Workbench screen, click **Setup** for the DominoWAN-E1 you want to configure for BERT testing.
2. From the 2 Mbps Interface Setup dialog box, click **Manual**.
3. On the 2 Mbps Manual Setup dialog box set the options as follows:

Option	Setting
Test mode	**Emulate**.
Tx clock	Network dependent; typically **Loop Timed**.
Transmitter data channels	Select the channels that you intend to test.
Framing, line code	As required by the network.
Receiver 2	Must be selected for BERT testing. Set termination to **Terminate**.
Receiver 1	Not used for BERT testing.

4. To return to the 2 Mbps Interface Setup dialog box, click **OK**.
5. To confirm your setup selections and return to the Workbench, click **OK**.

6.5.1.3 Setting Up the E1 Interface for a Bit Error Ratio Test Using Drop & Insert

The setup for BERT testing using Drop & Insert on selected channels consists of setting up a DominoWAN-E1 in Drop & Insert mode with the transmitter and both receivers enabled. (Use of this option is dependent on whether or not your equipment supports loopback on individual data channels.)

To set up the E1 interface for BERT testing with loopback on selected data channels:

1. From the **Analyzers Present** section of the Workbench screen, click **Setup** for the DominoWAN-E1 you want to configure for BERT testing.
2. From the 2 Mbps Interface Setup dialog box, click **Manual**.
3. On the 2 Mbps Manual Setup dialog box set the options as follows:

Option	Setting
Test mode	**Drop and Insert**.
Tx clock	**Loop Timed**.
Framing, line code	As required by the network.
Transmitter data channels	Select the channels on which to insert the BERT pattern.
Receiver 2	Set termination to **Monitor**. Select the same data channels as for the Transmitter.
Receiver 1	Set termination to **Terminate**.

4. To return to the 2 Mbps Interface Setup dialog box, click **OK**.
5. To confirm your setup selections and return to the Workbench, click **OK**.

6.5.1.4 Setting Up and Running an E1 Bit Error Ratio Test

The Domino Internetwork Analyzer BERT tester is a Real Time function that is available as an **Interface** menu command from Transmit. When you choose the **BERT** command, or click the BERT button in the Real Time Toolbar, the BERT dialog box is displayed. It provides test setup and run options and displays test statistics.

Remember that before you can use your Domino analyzer as a BERT tester, you need to create the correct hardware configuration and E1 interface setup required for the type of testing (one-way or loopback) that you want to do. (For information about how to do this, see 6.5.1, "Setting Up the E1 Interface for BERT Testing" on page 6.-10.

To set up a BERT for an E1 network:

1. From the Workbench, click **Transmit**.
2. From the Real Time **Interface** menu, choose **BERT** to display the BERT dialog box.

3. From the **Pattern** list box, select a bit pattern to use for the test.
4. From the **Error Ratio** list box, select the ratio at which error bits will be inserted into the test data stream if you select **Insert Error Ratio**.

At this point the test setup is complete and you can start the test.

To run the BERT:

1. Click **Start** to begin transmitting the test pattern you selected.
2. To introduce errors into the test data stream, do one of the following:
   - click **Insert Error Ratio** to begin insert error bits into the data stream at the ratio that you selected from the **Error Ratio** list.

     (To stop inserting errors into the data stream, click **Error Off**.)
   - click **Insert Bit Error** to insert a single error bit.

   While the test is in progress, test statistics are displayed in the **Statistics** and **G.821** display areas.
3. To end the test, click **Stop**.

NOTE:

The BERT function adjusts the internal configuration of the analyzer for bit-pattern processing. To return the analyzer to normal operating mode, you must exit the application or restart Real Time analysis.

6.5.1.5 Monitoring BERT Patterns on an E1 Network

You can use the Domino BERT function to monitor BERT patterns on a network on which a BERT test is taking place. It entails connecting a Domino Internetwork Analyzer to the network and setting it up to monitor the line. Then, when you start the BERT function, as the analyzer decodes the incoming traffic, the BERT statistics are posted to the display areas on the BERT dialog box.

To set up the E1 interface to monitor BERT patterns:

1. From the **Analyzers Present** section of the Workbench screen, click **Setup** for the DominoWAN-E1 you want to configure for BERT testing.
2. From the 2 Mbps Interface Setup dialog box, click **Manual**.
3. On the 2 Mbps Manual Setup dialog box set the options for the Receivers on the analyzer as follows:

Option	Selection
Test mode	**Monitor**.

Option	Selection
Receiver 2	Must be selected for BERT testing. Set termination to **Monitor**.
Receiver 1	Not used for BERT testing.
Receiver data channels	Select the channels on which the BERT patterns are being transmitted.

4. To return to the 2 Mbps Interface Setup dialog box, click **OK**.
5. To confirm your setup selections and return to the Workbench, click **OK**.

To use the BERT function to monitor BERT patterns:

1. From the Workbench screen, click **Transmit**.
2. From the Real Time **Interface** menu, choose **BERT** to display the BERT dialog box.

As BERT patterns are detected in the network traffic being monitored, statistics are posted to the display areas on the BERT dialog box.

6.5.2 Setting Up the T1 Interface for BERT Testing

You can use the DominoWAN-T1 BERT function for both one-way BERT testing and BERT testing on a looped-back line.

The one-way test configuration uses two analyzers configured as BERT testers, both of which transmit a specified BERT pattern and receive the transmission of the other tester. This configuration allows outgoing and incoming lines to be verified independently.

BERT testing on a looped-back line requires a single analyzer set up in Emulate mode. You activate the loopback from the BERT dialog box by selecting the appropriate loopback code. All loopback codes are transmitted according to required specifications.

You can also set up an analyzer in Drop & Insert mode with channels selected for data insertion. When you run the BERT, the test pattern is inserted on the selected channels.

Setting up the DominoWAN-T1 to act as a BERT tester entails both setting up the T1 interface and setting up the correct physical connections between the analyzer and the network or CSU/DSU.

Section 6.5.2.1 "Setting Up the T1 Interface for One-way BERT Testing" through Section 6.5.2.3 "Setting Up the T1 Interface for BERT Testing Using Drop & Insert", provide information about setting up for different types BERT testing on a T1 interface.

6.5.2.1 Setting Up the T1 Interface for One-way BERT Testing

For one-way BERT testing, you set up two DominoWAN-T1 analyzers acting as BERT testers. Both analyzers are set up in Emulate mode. Each analyzer transmits a specified BERT pattern through the network or devices under test and receives the transmission of the other tester. This configuration allows incoming and outgoing lines to be verified independently.

You can run BERTs with the analyzer set up to emulate either the network or the CSU/DSU.

To set up the T1 interface for one-way BERT testing:

1. From the **Analyzers Present** section of the Workbench screen, click **Setup** for the DominoWAN-T1 you want to configure for BERT testing.
2. From the T1/DDS Interface Setup dialog box, click **Manual**.
3. On the T1 Interface Setup dialog box set the options for the transmitter and receivers on both analyzers as follows:

Transmitter:

Option	Selection
Test mode	**Emulate CSU/DSU** or **Emulate Network**.
Tx clock	Network dependent; typically **Loop Timed**; set **Line Build Out** as required.
Framing, line code, data format	As required by the network.
Data channels	Select the channels you intend to test.

Receiver:

Option	Setting
Receiver	Enable and select the same data channels as for the transmitter.

4. To return to the T1/DDS Interface Setup dialog box, click **OK**.
5. To confirm your setup selections and return to the Workbench, click **OK**.

6.5.2.2 Setting Up the T1 Interface for BERT Testing with Loopback

The setup for BERT testing using a single tester and with loopback consists of setting up a DominoWAN-T1 in Emulate mode with both transmitter and receiver enabled. Loopback is implemented with codes that you specify as part of setting up the BERT test.

To set up the T1 interface for BERT testing using loopback codes:

1. From the **Analyzers Present** section of the Workbench, click **Setup**.
2. From the T1/DDS Interface Setup dialog box, click **Manual**.
3. On the T1 Interface Setup dialog box set up the options as follows:

Option	Setting
Test mode	**Emulate**.
Tx clock	Network dependent; typically **Loop Timed**; set **Line Build Out** as required.
Transmitter	Select the channels that you intent to test
Framing, line code, data format	As required for the tests you intend to run.
Receiver	Enable and select the same data channels as for the Transmitter.

4. To return to the T1/DDS Interface Setup dialog box, click **OK**.
5. To confirm your setup selections and return to the Workbench, click **OK**.

6.5.2.3 Setting Up the T1 Interface for BERT Testing Using Drop & Insert

The setup for BERT testing on selected data channels using a single tester consists of setting up a DominoWAN-T1 in Drop & Insert mode with both transmitter and receiver enabled. (Use of this option is dependent on whether or not your equipment supports loopback on individual data channels.)

Verify that your analyzer is correctly cabled for Drop & Insert mode. Information on cabling the analyzer appears in Domino Getting Started.

To set up the T1 interface for BERT testing on selected data channels:

1. From the **Analyzers Present** section of the Workbench screen, click **Setup** for the DominoWAN-T1 you want to configure for BERT testing.
2. From the T1/DDS Interface Setup dialog box, click **Manual**.

3. On the T1 Interface Setup dialog box set up the options as follows::

Option	Setting
Test mode	**Drop & Insert to CSU/DSU** or **Drop & Insert to Network**
Tx clock	**Loop Timed**; set **Line Build Out** as required.
Transmitter data channels	Select the data channels on which the BERT pattern is to be inserted.
Framing, line code	As required by the network.
Receiver	Enable and select the same data channels as for the Transmitter.

4. To return to the T1/DDS Interface Setup dialog box, click **OK**.
5. To confirm your setup selections and return to the Workbench, click **OK**.

6.5.2.4 Setting Up and Running a Bit Error Ratio Test on a T1 Network

The Domino Internetwork Analyzer BERT tester is a Real Time function that is available as an **Interface** menu command from Transmit. When you choose the **BERT** command, or click the BERT button on the Real Time Toolbar, the BERT dialog box is displayed. It provides test setup and run options and displays test statistics.

Remember that before you can use your Domino analyzer as a BERT tester, you need to create the correct hardware configuration and T1 interface setup required for the type of test (one-way or loopback) that you want to run.

To set up a BERT for an T1 network:

1. From the Workbench screen, click **Transmit**.
2. From the Real Time **Interface** menu, choose **BERT** to display the BERT dialog box.
3. From the **Pattern** list box, select a bit pattern to use for the test.
4. To prepare to send a loopback code: from the **Loop Type** list box, select a loopback code to use for the BERT.

   Ensure that the loopback code you select is compatible with the type of framing in use. (An Invalid LoopCode message is displayed when the loopcode and type of framing are incompatible.)

5. From the **Error Ratio** list box, select the ratio at which error bits are to be inserted into the test data stream if you choose **Insert Error Ratio**.

The test setup is complete and you can start the test.

To run the BERT:

1. Click **Start** to begin transmitting the test pattern you selected.
2. To activate the loopback code (if selected), click **Send Loop Up**.
3. To introduce errors into the test data stream, do one of the following:
   - Click **Insert Error Ratio** to begin insert error bits into the data stream at the ratio that you selected from the **Error Ratio** list.

     (To stop inserting errors into the data stream, click **Error Off**.)
   - Click **Insert Bit Error** to insert a single error bit.

   While the test is in progress, test statistics are displayed in the **Statistics** and **G.821** display areas.
4. To cancel the loopback code (if selected), click **Send Loop Down**.
5. To end the test, click **Stop**.

NOTE:

The BERT function adjusts the internal configuration of the analyzer for bit-pattern processing. To return the analyzer to normal operating mode, you must exit the application or restart Real Time analysis.

6.5.2.5 Monitoring BERT Patterns on a T1 Network

You can use the Domino BERT function to monitor BERT patterns on a network on which a BERT test is taking place. It entails connecting a Domino Internetwork Analyzer to the network and setting it up to monitor the line. Then, when you start the BERT function, as the analyzer decodes the incoming traffic, the BERT statistics are posted to the display areas on the BERT dialog box.

To set up the T1 interface to monitor BERT patterns:

1. From the **Analyzers Present** section of the Workbench screen, click **Setup** for the DominoWAN-T1 you want to configure for BERT testing.
2. From the T1/DDS Interface Setup dialog box, click **Manual**.

3. On the T1 Interface Setup dialog box set the options for the Receivers on the analyzer as follows:

Option	Selection
Test mode	**Monitor**.
Receiver 1	**Enable**. Enable the DSX-1 checkbox if you are connected to a Digital Cross-Connect or Monitor Jack.
Receiver 2	Not used for BERT monitoring.
Receiver data channels	Select the channels on which the BERT patterns are being transmitted.

4. To return to the T1/DDS Interface Setup dialog box, click **OK**.
5. To confirm your setup selections and return to the Workbench, click **OK**.

To use the BERT function to monitor BERT patterns:

1. From the Workbench screen, click **Transmit**.
2. From the Real Time **Interface** menu, choose **BERT** to display the BERT dialog box.

   As BERT patterns are detected in the network traffic being monitored, statistics are posted to the display areas on the BERT dialog box.

6.5.2.6 T1 BERT Messages

Message	Description	
Invalid LoopCode	The selected frame type and loop code are not compatible:	
	Loop Type:	**Use with:**
	Inband CSU	All frame types
	Inband Smarkjack:	All frame types
	Outband CSU:	ESF only
	Outband CSU Payload	ESF only
	Outband Smartjack	ESF only
LoopDown Inband CSU	Inband CSU loop-down code transmitted	

Message	Description
LoopDown Inband Smartjack	Inband Smartjack loop-down code transmitted
LoopDown Outband CSU	Outband CSU loop-down code transmitted
LoopDown Outband CSU Payload	PayloadOutband CSU/Payload loop-down code transmitted.
LoopDown Outband Smartjack	Outband Smartjack loop-down code transmitted
LoopUp Inband CSU	Inband CSU loop-up code transmitted
LoopUp Inband Smartjack	Inband CSU loop-up code transmitted
LoopUp Outband CSU	Outband CSU loop-up code transmitted
LoopUp Outband CSU Payload	Outband CSU/Payload loop-up code transmitted
LoopUp Outband Smartjack	Outband Smartjack loop-up code transmitted

6.5.3 Setting Up DominoWAN V-series for BERT Testing

The DominoWAN V-series BERT function provides for both one-way and loopback BERT testing.

The one-way test configuration uses two analyzers configured as BERT testers, both of which transmit a specified BERT pattern and receive the transmission of the other tester. This configuration allows outgoing and incoming lines to be verified independently.

BERT testing on a looped-back line requires a single analyzer set up in Emulate mode. You enable the loopback with a software switch when you set up the BERT test.

Setting up the DominoWAN V-series to act as a BERT tester entails both setting up the WAN V-series interface and setting up the correct physical connections between the analyzer and the network or DCE.

Section 6.5.3.1 "Setting Up theWAN V-series Interface for One-way BERT Testing" through Section 6.5.3.2 "Setting Up the WAN V-series Interface for BERT Testing with Loopback", provide information about setting up for different types BERT testing on a WAN V-series interface.

6.5.3.1 Setting Up theWAN V-series Interface for One-way BERT Testing

For one-way BERT testing, you set up two DominoWAN V-series analyzers acting as BERT testers. Both analyzers are set up in Emulate mode. Each analyzer transmits a specified BERT pattern through the network or devices under test and receives the transmission of the other tester. This configuration allows incoming and outgoing lines to be verified independently.

When you connect the V-series interface module to the network, you can use the setup that emulates either the network or a DCE.

To set up the WAN V-series interface for one-way BERT testing:

1. From the **Analyzers Present** section of the Workbench screen, click **Setup** for the DominoWAN V-series you want to configure for BERT testing.
2. From the WAN V-series Setup dialog box, click **Manual**.
3. From the Manual Setup dialog box set up the options on both analyzers as follows:

Option	Setting
Test mode	**Emulate**.
Tx clock	As required by circuit; set the clock rate as required.
Link type, **link type setting**, **encoding**, and **control leads**	As required for the circuit you are testing.

4. To return to the WAN V-series Setup Interface Setup dialog box, click **OK**.
5. To confirm your setup selections and return to the Workbench, click **OK**.

6.5.3.2 Setting Up the WAN V-series Interface for BERT Testing with Loopback

The setup for BERT testing on a looped-back line requires a single analyzer set up in Emulate mode. You enable the loopback with a software switch when you set up the BERT test. (The WAN V-series BERT function supports remote loopback for V.24 and V.35.)

To set up the WAN V-series interface for loopback BERT testing with a loopback jumper:

1. From the **Analyzers Present** section of the Workbench screen, click **Setup** for the DominoWAN V-series you want to configure for BERT testing.

2. From the WAN V-series Setup dialog box, click **Manual**.
3. From the Manual Setup dialog box set up the options as follows:

Option	Setting
Test mode	**Emulate**.
Tx clock	As required by the circuit you are testing; set the clock rate as required.
Link type, **link type setting**, **encoding**, and **control leads**	As required for the circuit you are testing.

4. To return to the WAN V-series Setup dialog box, click **OK**.
5. To confirm your setup selections and return to the Workbench, click **OK**.

6.5.3.3 Setting Up and Running a Bit Error Ratio Test on a WAN V-series Network

The Domino Internetwork Analyzer BERT tester is a Real Time function that is available as an **Interface** menu command from Transmit. When you choose the **BERT** command, or click the BERT button on the Real Time Toolbar, the BERT dialog box is displayed. It provides test setup and run options and displays test statistics.

Remember that before you can use your Domino analyzer as a BERT tester, you need to create the correct hardware configuration and V-series interface setup required for the type of test (one-way or loopback) that you want to run. (For information about how to do this, see 6.5.3, "Setting Up DominoWAN V-series for BERT Testing" on page 6.-21)

To set up a BERT for a V-series network:

1. From the Workbench screen, click **Transmit**.
2. From the Real Time **Interface** menu, choose **BERT** to display the BERT dialog box.
3. From the **Pattern** list box, select a bit pattern to use for the test.
4. From the **Error Ratio** list box, select the ratio at which error bits are to be inserted into the test data stream if you choose **Insert Error Ratio**.

The test setup is complete and you can start the test.

To run the BERT:

1. Click **Start** to begin transmitting the test pattern you selected.
2. To turn on circuit 140/RL (Remote Loopback), click **Loop On**.

   (The WAN V-series BERT function supports remote loopback for V.24 and V.35.)
3. Introduce errors into the test data stream by doing one of the following:
   - Click **Insert Error Ratio** to begin insert error bits into the data stream at the ratio that you selected from the **Error Ratio** list.

     (To stop inserting errors into the data stream, click **Error Off**).
   - Click **Insert Bit Error** to insert a single error bit.

   While the test is in progress, test statistics are displayed in the **Statistics** and **G.821** display areas.
4. To end the test, click **Stop**.

NOTE:

The BERT function adjusts the internal configuration of the analyzer for bit-pattern processing. To return the analyzer to normal operating mode, you must exit the application or restart Real Time analysis.

6.5.3.4 Monitoring BERT Patterns on a WAN V-series Network

You can use the Domino BERT function to monitor BERT patterns on a network on which a BERT test is taking place. It entails connecting a Domino Internetwork Analyzer to the network and setting it up to monitor the line. Then, when you start the BERT function, as the analyzer decodes the incoming traffic, the BERT statistics are posted to the display areas on the BERT dialog box.

To set up the V-series interface to monitor BERT patterns:

1. From the **Analyzers Present** section of the Workbench screen, click **Setup** for the DominoWAN V-series you want to configure for BERT testing.
2. From the WAN V-series Setup dialog box, click **Manual**.
3. From the Manual Setup dialog box set up the options as follows:

Option	Selection
Test mode	**Monitor**
Clock source	**External**

Option	Selection
Link type, **link type setting**, **encoding**, and **control leads**	As required for the circuit you are testing.

4. To return to the WAN V-series Setup dialog box, click **OK**.
5. To confirm your setup selections and return to the Workbench, click **OK**.

To use the BERT function to monitor BERT patterns:

1. From the Workbench screen, click **Transmit**.
2. From the Real Time **Interface** menu, choose **BERT** to display the BERT dialog box.

   As BERT patterns are detected in the network traffic being monitored, statistics are posted to the display areas on the BERT dialog box.

A. Toolbar Reference

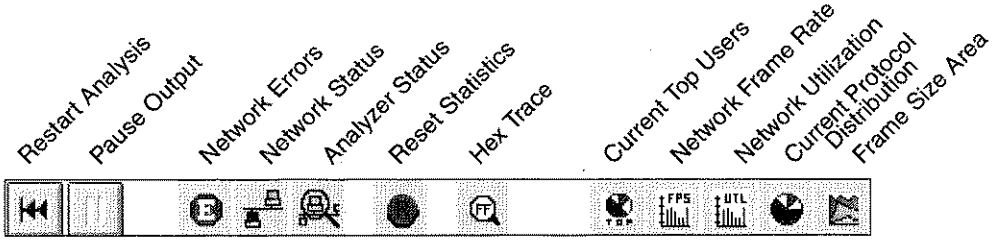
The Toolbars on the Domino application screens consist of a set of buttons that provide you with quick mouse access to the screen's most often used features. Each application screen has a distinct Toolbar.

This reference describes the Toolbars on the Core application screens for the DominoLAN and DominoWAN interfaces. The Domino software for other network interfaces might add Toolbar buttons that are specific to an individual interface.

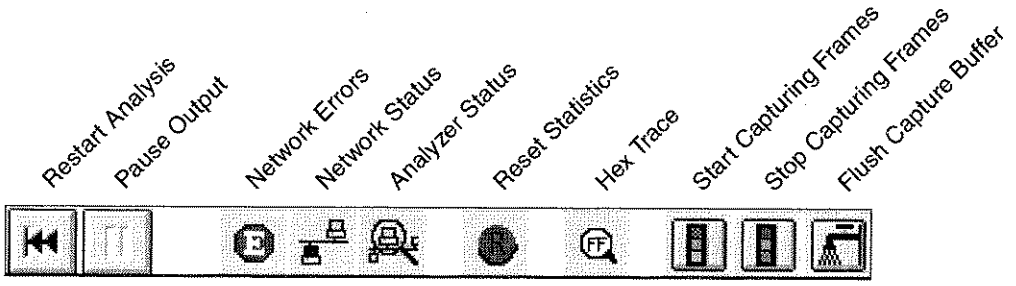
While you are using a screen you can learn more about a button by pointing your mouse at the button. A yellow label identifies the name of the button and the button's function is described in the status bar at the bottom of the screen.

A.1 DominoLAN Toolbars

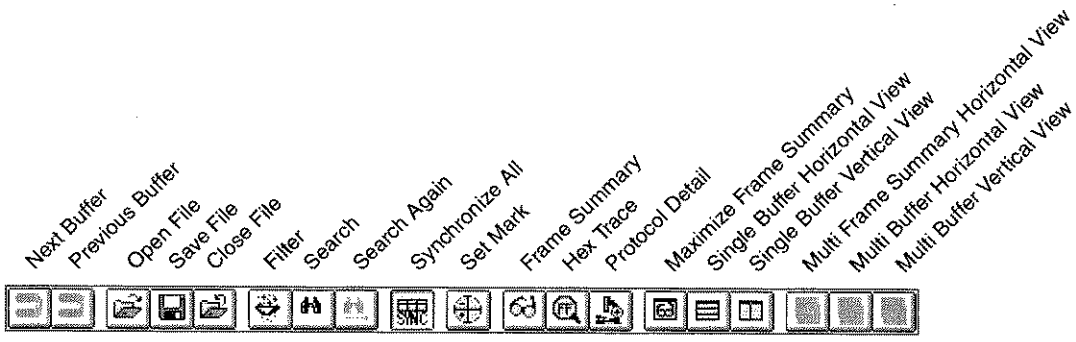
A.1.1 DominoLAN Monitor Toolbar



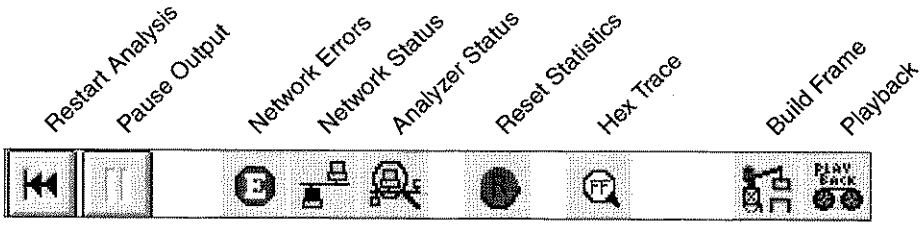
A.1.2 DominoLAN Capture Toolbar



A.1.3 DominoLAN Examine Toolbar

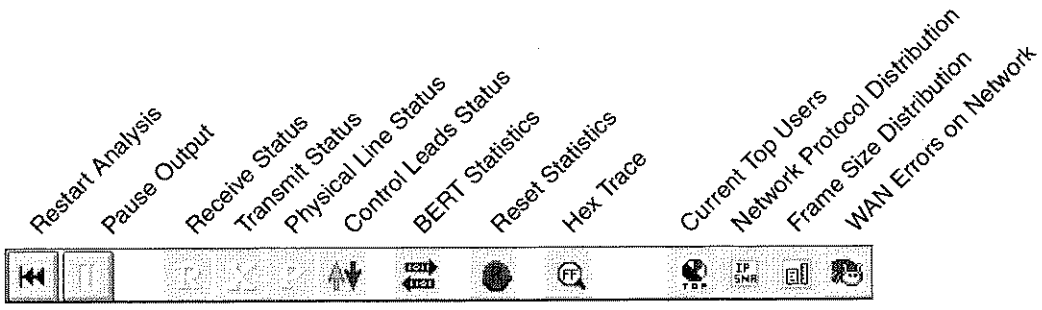


A.1.4 DominoLAN Transmit Toolbar

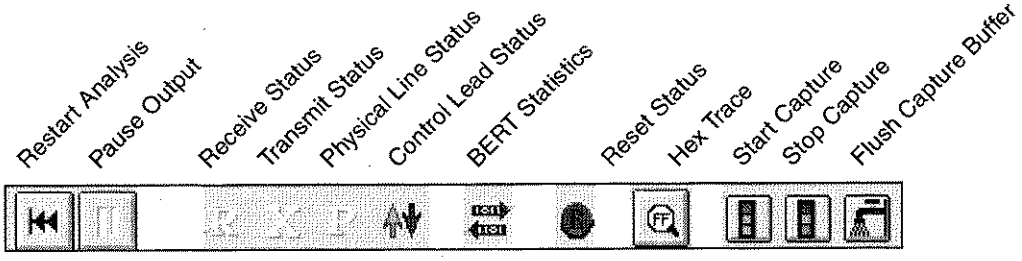


A.2 DominoWAN Toolbars

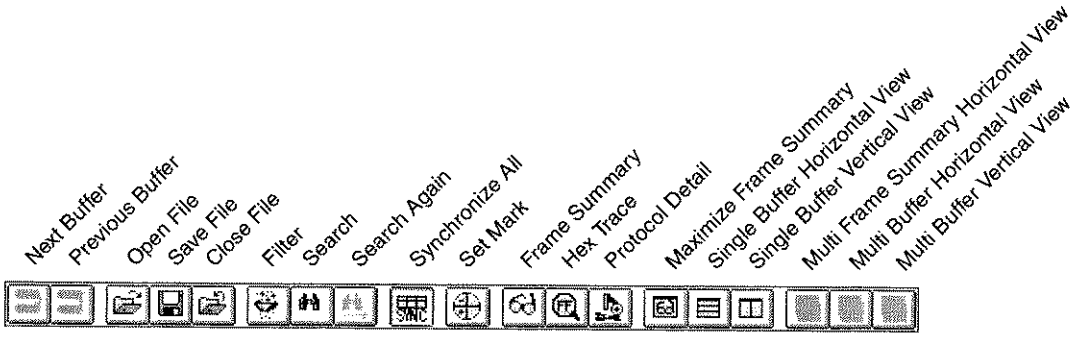
A.2.1 DominoWAN Monitor Toolbar



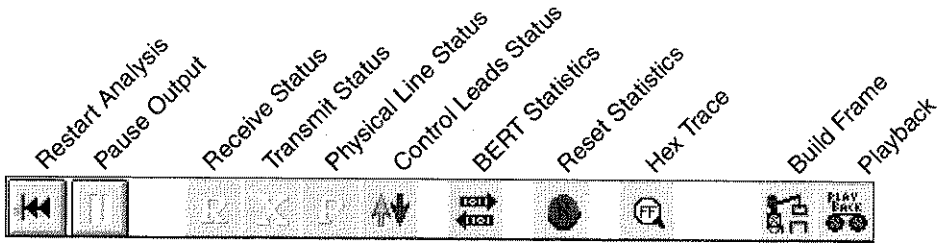
A.2.2 DominoWAN Capture Toolbar



A.2.3 DominoWAN Examine Toolbar



A.2.4 DominoWAN Transmit Toolbar



Glossary

absolute time — The timestamp that indicates the time at which the Domino analyzer received the frame. The timestamp appears in the format HH:MM:SS.sssss.

analyzer module — The protocol analysis processor that analyzes high frame rate data streams at network speeds. It executes multiple parallel processes, one for each layer of the OSI-model and one for central control and interaction with the other processors.

application — Software provided by WWG that allows you to monitor, analyze, generate, or filter network traffic, or test network hardware.

ASCII — American Standard Code for Information Interchange. A 7-bit data representation code adopted as a standard to promote data exchange between varying types of data processing and data communications equipment.

ASCII Extended — The 8-bit version of the American Standard Code for Information Interchange.

assignable buttons — Buttons at the bottom of the Workbench screen to which you can assign frequently used applications for quick access.

asynchronous — A method of transmitting data that uses unequal time intervals between characters. Transmission is timed by using a start and stop bit.

ATT 62411 — T1 physical layer specification. It specifies the QRSS pattern.

attribute — One of these seven distinguishing frame characteristics: enhanced, marked, sliced, overflow, no FCS, bad FCS, or aborted.

autodecode — The Domino feature that decodes any protocol in captured data, provided that the protocol software is installed on the computer that provides your Domino user interface.

automatic protocol recognition	A feature of the Domino system that enables it to recognize protocols for which no layer protocol package is loaded by using the protocol identifier bytes in the frame header.
BA	Balanced Asynchronous.
BER	The ratio of Bit Errors to Bits Received.
BERT	Bit Error Ratio Test.
bisync	Bisynchronous data transmission.
bisynchronous	A method of transmitting data that uses a specific set of control characters to synchronize half-duplex, character-oriented transmission.
canonical	The canonical address format displays a network address as six groups of two hexadecimal digits; each group is separated by a dash (-).
Capture	The Domino application that temporarily stores network traffic in a buffer.
capture buffer	A part of the available Domino RAM set aside for the temporary storage of frames as they are received from the network.
capture file	A file used to store the frames from the capture buffer, which can be loaded into the Domino RAM for post-capture examination.
CCITT G.821	This standard pertains to Error Performance of an International Digital Connection that forms part of an Integrated Services Digital Network (ISDN). It specifies the standard BERT statistics.
CCITT O.151	Specification for Instrumentation to measure error performance on digital systems (requirement for BERT testers). It specifies the PRBS15 and PRBS23 patterns.
CCITT O.152	Specification for Instrumentation to measure the error performance on 64 Kbps circuits. It specifies the PRBS11 pattern.
character code	The Domino feature that allows the selection of the data transmission character code such as EBCDIC or ASCII. This controls the way Domino interprets the data it captures from and transmits to the network.

CSV Comma-separated value. A file format accepted by many software packages, especially spreadsheet software. The Export to CSV command on the Examine screen allows you to export the contents of the current capture buffer to a CSV file.

custom stack An option available on the Protocol Setup that allows you to load a protocol at any layer of the protocol stack for decoding.

DA-3x The term used to refer to an unspecified member the WWG family of network protocol analyzers (DA-30, DA-31, or DA-30C).

DCE Data Communications Equipment. Interfacing equipment that helps the terminal equipment communicate over the network. It establishes, maintains, and terminates the connection in a data conversation. An example is a modem.

delta time A timestamp that indicates the interframe delay, which is the number of seconds elapsed between the time when a frame is received by the Domino analyzer and the time when the next frame is received.

desktop A desktop is a retrievable screen configuration that you define while working with a Real Time application. It contains a set of results windows that you can recall to the screen with a single menu command. Desktops are analyzer-specific, interface-specific, and application-specific.

desktop file A file in which you can save the set of currently-defined desktops for an application. When you load the desktop file, the desktops that it contains are listed on the Real Time Desktop menu. Desktop files are interface-specific and application-specific, but not Domino-specific.

destination address Field in a network frame indicating the address of the node targeted for receipt of the frame.

DSU Data Service Unit. The customer interface between the DTE and a digital (E1 or T1) network.

DTE Data Terminating Equipment. Any piece of equipment at which a communication path begins or ends. Examples include a PC, printer, or PBX.

EBCD	Extended Binary Coded Decimal
EBCDIC	Extended Binary Coded Decimal Interchange Code. An 8-bit data representation code that can represent up to 256 distinct characters.
Examine	The Domino application that provides detailed analysis of real time or captured data including viewing details, summaries, and interpretive statistical information.
export	To save captured data in a format that can be used with other software, such as a spreadsheet. From the Examine screen, you can export captured data to a comma-separated value (CSV) file.
FCS	Frame Check Sequence. A field added to the end of a frame that contains transmission error-checking information. A source computer calculates a value which it includes in the FCS field of a frame that it transmits. The receiving computer performs the same calculation when it receives the frame. If the calculations do not match, the receiving computer determines that the packet is corrupt and discards it. An FCS calculation is made for each packet.
filtering	A Domino function that allows you to display only those capture buffer frames that match specific criteria.
frame slicing	An option that allows you to shorten the data frame before it is passed to the analyzer for processing.
HDLC	High-Level Data Link Control protocol.
IETF	Internet Engineering Task Force.
initial interface setup dialog box	The interface setup dialog box that appears when you choose the Setup button on the Workbench or when you choose the Setup command from the Real Time Interface menu.
IP	Internet Network Layer protocol.
ISO	International Standards Organization. An organization composed of several committees that establish standards in telecommunications and data communications technology and other fields.

LAN Acronym for Local Area Network. A network that spans a limited geographical area and that permits interconnection and intercommunication between a group of computers in order to share resources.

LED indicators Display on the front panel of the Domino analyzer that shows the selected test mode and the status of the data and control leads.

MSB first The MSB First address format displays a network address as six groups of two hexadecimal digits. Each group is separated by a colon (:), with the most significant bits first.

network event program A software program you can create to customize an application to perform tasks such as monitoring specific network interface conditions and protocol conditions or generating network traffic.

network interface setup A network-interface-specific dialog box which enables you to set up the parameters for the network interface in use.

network interface software Software that works with the network interface module to allow the Domino analyzer to correctly interact with the type of network being monitored.

NLPID Network Level Protocol ID

NI Network Interface - This is defined in ANSI T1.403 as the point of demarcation between the network and the Customer Installation (CI).

non-canonical The non-canonical address format displays a network address as six groups of two hexadecimal digit; each group is separated by a colon (:).

playback A Domino feature that allows you to use a capture file as the source of network traffic for an application rather than the live network. When you invoke the Internal Playback option from the Advanced Setup dialog box, the capture file is played back to the Domino. The Transmit application includes an External Playback option that enables you to play back a capture file onto the network and simultaneously play the file back to the Domino.

PRBS Pseudorandom Bit Sequence.

protocol software	Domino software that decodes the protocols used by the devices on the network being monitored. All devices on the same network use a minimum of one shared protocol.
protocol stack	The Domino feature that provides an OSI Model for layer-by-layer loading of protocols at default or custom layers.
QRSS	Quasi-Random Signal Source - This test pattern is specified in ATT Technical Reference 62411.
RAM capture	The Domino action that buffers network traffic in a RAM file while continuing to capture network traffic in real time.
Real Time	The part of the Domino software that monitors network traffic and interfaces with the analyzer and the network interface module. Capture, Monitor, Transmit and the Toolbox applications run over the Real Time software and add their own unique features to those available from Real Time.
relative mark	A mark that you set on a frame in the capture buffer with the Set Mark command. Examine calculates the relative time and the cumulative bytes for each frame in the buffer that succeeds the relative mark.
relative time	A timestamp that indicates the interframe delay or the number of seconds that have elapsed between the mark that you set using the Set Mark command and the time when the Domino analyzer received the current frame.
results windows	Windows that display information about the frames in the capture buffer, such as summary information, statistics and graphs.
SNAP	Subnetwork Access Protocol.
source address	Field in a network frame indicating the address of the node originating the frame.
status bar	The area at the bottom of the screen that provides information about the current screen or window, such as a description of the current menu option.
stop condition	The condition for RAM capturing that controls how the Domino analyzer responds when the user-specified maximum capture buffer or capture file size is reached.

summary windows Frame Summary or Protocol Summary windows. The Frame Summary window displays summary information about each frame in the current capture buffer. The Protocol Summary window displays protocol-specific information for each frame in the capture buffer.

symbolic name A user-defined name which is equated with the IEEE-specific address of a network interface card. Symbolic names, which can be up to 48 characters long, cannot contain commas or double-quotation marks.

test mode The function of the Domino analyzer in a network test, which is specified during interface setup. The options are Monitor and Emulate for DominoLAN, and Monitor, Emulate DCE, and Emulate DCE on DominoWAN.

timestamping The process by which Domino assigns a time to each received frame, which is expressed as either absolute time, relative time, or delta time.

Toolbar The graphic area across the top of the screen, below the menu bar, comprised of buttons that provide quick mouse access to a screen's most commonly used functions.

transmission channel A transmission channel consists of interface cables as well as any interconnecting devices that are on the line.

Transmit The Domino application that enables you to play back a capture file onto the network and simultaneously play the file back to the Domino analyzer. Transmit also provides options for building a test frame by editing a frame from a capture file, and transmitting the test frame onto the network.

WAN Acronym for Wide Area Network. A communications network that services devices over a large physical distance.

WAN interface module A plug-in module that provides WAN V-series interface support on Domino units.

Workbench The first screen that you see when you start the Domino software and from which you can access all of the features of the Domino software. The name on the title bar is Domino Internetwork Analyzer.

A

B

C

D

E

F

G

T

U

V

W