To detect other installations of Network Monitor on the network

1 On the Capture window's Tools menu, click Identify Network Monitor users.

2 To sort the values in a column, double-click on the column heading.

3 To move a column, point to the column heading with your mouse, hold down the primary mouse button, and then drag the column to its new position.

4 To add the addresses of the displayed computers to your address database, click Add Names to Address Database.

5 To refresh the statistics that appear in this dialog box, click Refresh List.

To sort the values in a column

1 Position your cursor at the column heading of the column you want to sort.

2 Double-click on the column heading.

Note

- When you sort a numeric column, the highest number is moved to the top of the column. When you sort a word-based column, the column is sorted alphabetically.

To capture in dedicated capture mode

1 On the Capture menu, click Dedicated Capture Mode. If a checkmark appears next to this command, the command is activated.

2 On the Capture menu, click Start.

3 During the capture, the following options are available in the Dedicated Capture Mode status box:
- To stop the capture, click Stop.
- To stop the capture and view the frames, click Stop and View.
- To pause the capture, click Pause.
- To continue a paused capture, click Continue.
- To resume capturing in Normal mode, click Dedicated Capture Mode on the Capture menu to clear the checkmark that indicates the option is active.

Note
- When you use dedicated capture mode, capture statistics are not displayed or refreshed as <u>frames</u> are copied to the <u>capture buffer</u>, and the Network Monitor window is minimized.
- Because dedicated capture mode frees more resources for capturing data, it is useful when Network Monitor drop frames due to a lack of resources.

To modify the size of the capture buffer or number of bytes per frame to capture

1 On the Capture menu, click Buffer Settings.

2 To modify the size of the capture buffer, select a buffer size in the Buffer Size box.

3 To modify the number of bytes per frame that Network Monitor captures, select a frame size from the Frame Size box.

   Notes
▪   If you set the buffer size to a value greater that the amount of memory available on your system, Network Monitor might drop frames because of memory swapping. If you are using the Network Monitor Agent to capture on a remote Windows NT computer, the size of your buffer cannot exceed the amount of memory available on the remote system.
▪   If your system becomes low on resources while you are capturing, reduce the size of the capture buffer or reduce the number of bytes-per-frame that Network Monitor captures.

To open an existing capture file

1 On the File menu, click Open.

2 In the File Name box, type or select the file you want to open. If necessary, choose a different drive or directory.

Notes

▪   If a comment was associated with the file when it was saved, a descriptive remark appears in the Comment box.

▪   Optionally, if you drag a capture file from Windows NT Explorer into Network Monitor's screen area, Network Monitor automatically opens this file and displays its contents in a Frame Viewer window. Several capture files can be opened at one time; Network Monitor opens a separate Frame Viewer window for each capture file that you open.

To save the captured frames to a capture file or text file

1 On the File menu, click Save As.

2 Specify the directory and drive where you want to store the file.

3 Type the filename.

4 To save only those frames that meet the specifications of the current display filter, click Filtered.

 This option is available only if you are saving data from the Frame Viewer window.

5 To save a particular range of frames, type the beginning and ending frame numbers in the From and To boxes.

Notes

- When a range of frames is saved to a capture file, the numbers associated with the frames are changed; in a capture file, frame numbers always begin with 1, regardless of the number associated with the original frame. Similarly, if you apply a display filter, and then save the filtered frames, the frame numbers in the capture file begin with 1. If, however, you use the Print to File option in the Print dialog box, the original frame numbers associated with the frames are preserved.

To design a capture filter

1 On the Capture menu, click Filter.

2 Select the appropriate options in this dialog box, and then click OK. You can do any of the following:
- Choose the computer address to capture.
- Choose the protocols to capture
- Choose the data patterns to capture

See Also

Choosing the Computer Addresses to Capture

Choosing the Protocols to Capture

Choosing the Data Patterns to Capture

Loading a Capture Filter

Saving a Filter

To save a filter

1 On the Capture or Display menu, click Filter.

2 When you have finished editing the filter, click Save.
- To save the filter to a capture filter file, use a .CF filename extension.
- To save the data to a display filter file, use a .DF filename extension.

3 Select the options you want to use:
- To associate a comment with the file so that it is easy to locate, type a descriptive remark in the Comment box.
- To save the file to a different directory, select a directory in the Directories box.
- To save the file to a different drive, select a drive in the Drives box.
- To save the file to a network share to which you are not connected, click Network, and then make the necessary network connection.

Note
- By saving filters that you have designed or edited, you avoid creating filters from scratch every time you want to filter <u>frames</u> from the network.

To load a capture filter

1 On the Capture menu, click Filter.

2 Click the Load button.

3 Specify the capture file.

   If the file is located on a network share to which you are not currently connected, use the Network button to connect to this share.

   Notes

▪   Use the Capture Filter dialog box to load <u>filters</u> that you have previously designed and saved to a file. By doing this, you avoid creating filters from scratch every time you want to capture filtered data.

▪   The <u>decision tree</u> reflects the contents of the filter file that you have loaded. When you begin <u>capturing</u> data, Network Monitor applies this filter.

To load a display filter

1 On the Display menu, click Filter.

2 Click the Load button.

3 Specify the display filter.

If the file is located on a network share to which you are not currently connected, use the Network button to connect to this share.

Notes
- Use the Display Filter dialog box to load <u>filters</u> that you have previously designed and saved to a file. By doing this, you avoid creating filters from scratch every time you want to filter captured data.
- The <u>decision tree</u> reflects the contents of the filter file that you have loaded. When you display captured data, Network Monitor applies this filter.

To add an address to a capture filter

1 On the Capture window's Capture menu, click Filter.

2 Under Add, click Address.

3 In the Station 1 box, select the first computer address that you want to include in the decision tree.

4 In the Station 2 box, select the second computer you that want to include in the decision tree.

5 In the Direction box, select the relational operator that specified the direction of traffic you want to monitor.
   Note that you cannot construct a statement in which the source address is either broadcast or multicast;
   broadcast and multicast are always destination addresses.

▪   Select <--> to specify frames that travel in either direction between the computers you specified in the
Station 1 and Station 2 boxes.

▪   Select --> to capture frames that travel in only one direction between the computers you specified in the
Station 1 and Station 2 boxes.

6 Select Include if you want the filter to capture data from the computers and direction specified in the Station 1
   and Station 2 boxes.

7 Select Exclude if you want the filter to ignore data from the computers and direction specified in the Station 1
   and Station 2 boxes.

8 To edit any of the addresses in either the Station 1 or Station 2 boxes, click Edit.

Notes

▪   You can design a <u>capture filter</u> to single out or ignore frames that originate with or are destined to the
address that you specify. All the computers that you include in your filter are listed on the line in the Capture Filter
<u>decision tree</u> that begins with INCLUDE. When two computers are included in the decision tree and a relational
operator appears between them, they are called an address pair. For example, if you include the line LOCAL --> ANY
in a decision tree, Network Monitor captures all frames directed from your computer to any other. If you do not use
a capture filter, Network Monitor captures frames from all of the computers on your network.

▪   As Network Monitor internally processes the decisions in your filter, EXCLUDE statements take logical
precedence over INCLUDE statements, regardless of the sequence in which statements appear in the Capture Filter
dialog box. Therefore, in a filter containing both an EXCLUDE and INCLUDE statement, if a frame meets the criteria
specified in an EXCLUDE statement, that frame is discarded; Network Monitor does not test that frame by any
INCLUDE statements to see if it meets their criteria also.

To enable or disable a protocol

1 On the Capture window's Capture menu, click Filter.

2 Double-click on the SAP/ETYPE line.

The Capture Filter SAPs and ETYPEs dialog box appears. Enabled protocols are listed in the top box and disabled protocols are listed in the lower box. You can sort any column in either box by double-clicking on the column heading.

3 To enable a disabled protocol, select a protocol that appears in the bottom box, and then click Enable.

4 To disable an enabled protocol, select a protocol from the top box, and then click Disable.

5 To enable or disable one or more protocols, highlight the protocols that you want to move from one box to another and then click Enable or Disable.

6 To enable all protocols, click Enable All.

7 To disable all protocols, click Disable All.

Note
▪ You can use a capture filter to single out frames sent using the protocols that you specify. All protocols that you include in your filter are listed on the line in the Capture Filter <u>decision tree</u> that begins with SAP/ETYPE=. By default, all of the protocols that Network Monitor supports are listed in this line and are enabled.

To capture frames that contain a specific data pattern

1 On the Capture window's Capture menu, click Filter.

2 Double-click on the (Pattern Matches) line.

3 To specify the byte on which the pattern begins, type a number in the Offset (in hex) box.

4 To start the search for the pattern at the beginning of the frame, click From Start of Frame.

5 To start the search for the pattern beyond the <u>topology header</u>, click From End of Topology Header.

6 In the Pattern box, type the pattern that you want to match.

7 Specify the format of the pattern you want to match. To match a hexadecimal pattern, click Hex. To match an ASCII pattern, click ASCII.

To add a protocol parser

1 Copy your parser file to the \PARSERS folder under your Network Monitor folder. The file should have a file type of .DLL.

2 Edit the PARSERS.INI file to include information about the parser that you are adding.

3 On the Options menu, click Default Parsers.

   In the left pane of this dialog box appear all of the protocols that are currently enabled. By default, all parsers that are present in your \PARSERS subdirectory are enabled.

4 Select the newly available parser in the Disabled Protocol Parsers pane.

5 Click the Enable button.

   The name of the protocol is moved to the Enabled Protocol Parsers pane.

6 If you want the parsers that appear in the Enabled Protocol Parsers pane to be your default configuration, select the Save as Default box.

   Note
▪   In the future, unless you design or load a capture filter, every data capture will collect network data sent using the protocols that appear in the Enabled Protocol Parsers pane.

To create an address database

1 On the Capture window's Capture menu, click Start to initiate the capture process.

2 When you have finished capturing, click Stop on the Capture menu.

3 On the Capture menu, click Find All Names to associate the captured computer addresses with the friendly names of the computers from which the frames have been captured.

   After the frames are processed, a message appears telling you how many non-duplicate names have been added to the address database.

4 Click OK.

5 On the Capture menu, click Addresses. This dialog box displays the names that have been added to the database.

6 To use these addresses to design a filter in the future, click the Save button in the Address Database dialog box to save the database to a file.

When you design a capture filter, you can load this database to specify the address pairs from which you want to capture frames.

To save the address database to a file

1 On the Capture menu, click Addresses.

2 When you have modified the database, click Save.

3 Specify the filename and location.

Note

▪   The next time you design a capture filter that involves address pairs, you can use this database. If you assign the database the DEFAULT.ADR filename, it becomes your default address database.

To load an address file

1 On the Capture menu, click Addresses.

2 Click Load. If a message box appears prompting you whether you want to cancel your changes and load another address database, click Yes.

3 Specify the filename.

Note

▪ If you load an <u>address database</u> while another address database is open, changes made to the open database are lost.

To specify the time that is associated with a frame

  1 On the Frame Viewer window's Display menu, click Options.

  2 Specify one of the available time options:
- Time of day. Associates the frame with the system time at which it was captured (for example, 10:35:48.358).
- Seconds from the beginning of capture. Displays the time, in milliseconds, that transpired between the beginning of the capture and the capture of the currently selected frame.
- Seconds from previous frame. Displays the time, in milliseconds, that transpired between the capture of the previous frame and the capture of the currently selected one.

To specify the protocol header that you want to display

1 On the Display menu, click Options.

2 Specify one of the following protocol options:
▪   Last protocol in frame. Displays in the Protocol column the last protocol that appears in the captured frame.
▪   Auto (Based on protocols in display filter). Displays in the Protocol column the protocol Network Monitor selects to be of interest to you, based on the settings in the current Display filter.

Notes
▪   You can choose the time format you want to associate with a captured <u>frame</u>. In addition, from the protocols used to send a frame, you can specify the one you want to display.
▪   When you specify a time setting, the setting appears in the Time column of the Frame Viewer window's Summary pane. When you specify a protocol setting, the setting appears in the Protocol column of the Summary pane.

To move between windows

▶ Press CTRL + TAB.

Note

▪ You can also use the Window menu to activate a window. The bottom of the Window menu displays a list of open windows, and a checkmark appears next to the name of the currently active window. To make a window the active window, choose its name from this list.

To use keyboard shortcuts to move among frames in the summary pane

- Press CTRL + HOME to move to the first frame in the Summary pane
- Press CTRL + END to move to the last frame in the Summary pane
- Press CTRL + UP to move to the previous frame in the Summary pane
- Press CTRL + DOWN to move to the next frame in the Summary pane

To expanding and collapsing details on a frame

- To expand details on a collapsed frame, double-click on the plus sign (+) icon in the Detail pane.
- To collapse details on an expanded frame, double-click on the minus sign (-) icon in the Detail pane.

Notes

- Frames displayed in the Detail pane of the Frame Viewer window are collapsed by default.
- If you expand details on a frame, all other lines using the expanded protocol are automatically expanded as they are displayed. If a plus sign icon appears to the left of a line in the Detail pane, the associated frame can be expanded. If a minus sign icon appears to the left of a line, it can be collapsed.
- If you search for the property of a frame, and the property is found, the frame is automatically expanded to display the property that you specified in your search.

To design a display filter

1 On the Display menu, click Filter.

2 Choose the addresses to display.

3 Choose the protocols to display.

4 Choose the properties to display.

Notes

▪   A Network Monitor display filter functions like a database query, enabling you to specify the types of captured data you want to examine. You can also use display filters to specify the types of displayed data you want to save to a file.

▪   Save the display filter if you might want to use it later.

See Also

Choosing the Addresses to Display

Choosing the Protocols to Display

Choosing the Properties to Display

Loading a Display Filter

Saving a Filter

To specify the protocols that you want to display

1 On the Display menu, click Filter.

2 In the Display Filter decision tree, double-click on the PROTOCOL == line.

3 Select the Protocol tab.

4 Select protocols by highlighting the protocol in the Disabled Protocols box and choosing Enable.

5 Disable protocols by highlighting the protocol in the Enabled Protocols box and choosing Disable.

6 Click OK to add the line to the decision tree.

Notes

- You can only add one expression at a time to a display filter. If you specify an expression and choose another tab category, that expression is lost. You must click OK to save the specified expression and add it to the decision tree.
- Disabling a protocol does not ensure that the protocol will not appear in the Frame Viewer window. For example, if you disable the SMB protocol, the frame will still be displayed if it contains protocols that are not disabled.
- To ensure that a protocol will not appear in the Frame Viewer window, enable only that protocol, and then apply the NOT operator to the line in the decision tree that references the protocol.

To specify address pairs

1 On the Display menu, click Filter.

2 In the Display Filter decision tree, double-click on the ANY <-> ANY line.

3 Select the Address tab.

4 In each of the Station boxes, select a computer name, and then specify a direction of traffic by choosing the appropriate arrow button.

5 Click OK to add the line to the decision tree and to return to the Display Filter dialog box.

Note

▪ You can add only one expression at a time. If you specify an expression and choose another tab category, that expression is lost. You must click OK to save the specified expression and add it to the <u>decision tree</u>.

To specify protocol properties that you want to display

1 On the Display menu, click Filter.

2 In the Display Filter decision tree, highlight the line above where you want the expression to appear.

3 Under Add, click Expression.

4 Select the Property tab.

5 Double-click on a protocol name, or the plus (+) icon next to it, to expand properties for that protocol.

6 Select a property, a relation symbol, and a value from the appropriate boxes.

7 Click OK to add the line to the decision tree and to return to the Display Filter dialog box.

Note
▪   You can add only one expression at a time. If you specify an expression and select another tab category, that expression is lost. You must click OK to save the specified expression and add it to the decision tree.

To search for a frame by characteristic

1 On the Display menu, click Find Next Frame.

2 Do one of the following:
- To search for a frame on the basis of its source or destination address, select the Address tab, and then specify the appropriate options.
- To search for a frame on the basis of the protocols that were used to send it, select the Protocol tab, and then specify the appropriate options.
- To search for a frame on the basis of protocol properties, select the Property tab, and then specify the appropriate options.

To find the next frame having the specified characteristics
- On the Display menu, click Repeat Find Next Frame.

To find the previous frame having the specified characteristics
- On the Display menu, click Repeat Find Previous Frame.

Note

The search remains active until you close the active window or begin a new search.

To view a specific frame in the Frame Viewer window

1 On the Display menu, click Go To Frame.

2 In the Frame Number box, type the number of the frame you want to view.

Network Monitor highlights the frame that you specified.

To start the Network Monitor Agent in Control Panel

1 In the Control Panel, double-click on the Services icon.

2 In the list of Service Names, select Remote Network Monitoring Agent.

3 Click Startup.

4 In the Services Startup dialog box, select a startup type of Automatic, Manual, or Disabled.

Note
▪   Before a computer can be used as a remote capture site, the <u>Network Monitor Agent</u> must be started on that computer.

To start the Network Monitor Agent from the Command Prompt

▪ From the Command Prompt, type **net start nmagent**.

Note

▪ Before a computer can be used as a remote capture site, the <u>Network Monitor Agent</u> must be started on that computer.

To start the Network Monitor Agent from Server Manager

1 Select a computer from the list in the Server Manager window.

2 On the Computer menu, click Services.

3 In the Services dialog box, select the Remote Network Monitor service.

4 Click Start.

5 In the Services Dialog box, click Close.

Notes

▪   Before a computer can be used as a remote capture site, the <u>Network Monitor Agent</u> must be started on that computer.

▪   By default, when the Network Monitor Agent is started, the startup type is Manual, which means that you must start the service every time you want to use it. If you want the service to run automatically, you must configure the startup.

To connect to the Network Monitor Agent on another computer

1 On the Capture window's Capture menu, click Networks.

2 In the Select Capture Network dialog box, select the name of the connection that you want to use. Until you have made a connection, this entry is REMOTE. When you have made the connection, REMOTE will be replaced by the name of the connection.

3 Click Connect.

4 In the Agent Name box, specify the name of the agent to which you're connecting.

5 In the User Comment box, associate a comment with the Agent Name.

   This comment is displayed to users who attempt to connect to the Network Monitor Agent that you are using. Also, it is displayed for you when you attempt to reconnect to this agent.

6 In the Agent Status Update frequency, specify the frequency, in seconds, which you want the statistics from the remote capture displayed on your local computer. This number must be between 1 and 65.

7 Select the Slow Link option. This option extends the period of time that your connection can be idle before Network Monitor concludes that the connection has failed and Network Monitor disconnects from the Agent.

   Though it is critical to use the Slow Link option when connecting over an expensive or unreliable line, this option is recommended for all asynchronous connections.

8 Click Connect.

   If the Network Monitor Agent on the remote computer is password protected, you are prompted for a password.

   If the Agent to which you've connected is running on a computer that has only one network adapter card installed, the Network Monitor connects to that card. If the Agent is installed on a computer that has more than one network card installed, a dialog box appears, displaying the network adapter cards installed on the remote computer. An asterisk appears next to the card that Network Monitor used to make the connection to the remote computer. This card is connected to the same network segment to which you are connected. Unless you want to capture statistics from your own your local network segment, you should select one of the other network cards displayed.

9 To begin capturing, click Start on the Capture menu.

To suspend a connection

1 On the Capture window's Capture menu, click Networks.

2 Select the line that contains information on the remote connection.

3 Click Suspend.

Notes

▪   You cannot suspend a connection until you have started capturing on it. If your connection is lost before you suspend it, the Network Monitor Agent stops capturing, and the unsaved data is lost.

▪   If you are <u>capturing</u> over an expensive or unreliable line, you should suspend your connection to the <u>Network Monitor Agent</u> as soon as you have started capturing. When a connection is suspended, the Network Monitor Agent continues to capture on the remote computer. When you reconnect to the Agent, you can retrieve and save the statistics captured while the connection was suspended.

To reconnect to a suspended connection

1 On the Capture window's Capture menu, click Networks.

2 Click Connect.

3 In the Agent Name box, specify the name of the agent to which you are connecting.

4 In the User Comment box, associate a comment with the Agent Name.

This comment is displayed to users who attempt to connect to the Network Monitor Agent while you are using it to capture. Also, it is displayed when you attempt to connect to the remote computer after suspending the connection.

5 In the Agent Status Update frequency, specify the frequency, in minutes, with which you want the statistics from the remote capture displayed on your local computer. This number must be between 2 and 60.

6 If you have a slow connection (for example, 2400 baud or less), use the slow link option.

This option extends the period of time that your connection can be idle before Network Monitor concludes that something has gone wrong with the connection.

7 Click the Connect button.

A message box appears, informing you that the Network Monitor Agent was previously capturing and offering you the option to reconnect.

▪   Though it is critical that you use the Slow Link option when capturing over an expensive or unreliable connection, this option is recommended for all asynchronous connections.

Note

▪   When you suspend a connection to the Network Monitor Agent, the Agent continues to capture and store frames. To retrieve and save the statistics that have been captured while the connection was suspended, reconnect to the Agent.

To disconnect from the Network Monitor Agent

1 On the Capture window's Capture menu, click Networks.

2 Select the line that displays information on the remote connection.

3 Click Disconnect.

If the Prompt to Save Data under the Tools menu is selected, you are prompted to save captured frames.

If you are still capturing on the remote connection, a dialog box appears, and gives you the option to suspend the session. Choose one of the following options:

- Click Yes to suspend your connection to the Network Monitor Agent. When you choose this option, the Agent continues to capture.
- Click No to terminate your connection to the Network Monitor Agent. If you choose this option, any unsaved data is lost.
- Click Cancel to return to the Network Monitor window.

4 Click Yes, and then save the capture. Or, click No to disconnect.

Notes

- After you have disconnected, the Select Capture Network box reappears. Use this dialog box to establish another remote connection. Or, click Cancel to return to the Network Monitor Capture window.
- When you disconnect from the Network Monitor Agent, the Agent stops capturing, and all unsaved captured data is lost.

To start Performance Monitor from Network Monitor

- On the Tools menu, click Performance Monitor.

Notes

- When you activate Performance Monitor and add Network Monitor counters, Performance Monitor automatically puts your network card into promiscuous mode. Performance Monitor does not take your card out of promiscuous mode until you exit Performance Monitor. Although you can still use your network card while using Performance Monitor, network performance is reduced while you are in promiscuous mode.
- To view the Network Monitor related counters, click the Ad to on the Edit menu, choose the Network Segment object type, and click Explain. Click the different counters and read the corresponding Counter Definition text.

To transmit a single frame across the network

1 In the Summary pane of the Frame Viewer window, select the frame that you want to transmit.

2 On the Tools menu, click Allow Transmit.

3 In the Select Transmit Network dialog box, select the network onto which you want to transmit the frame, and then click OK.

4 On the Tools menu, click Transmit Frame.

Note

▪   You can transmit as many frames as you want. Also, you can transmit the same group of frames repeatedly and specify the amount of time to elapse between each transmission.

To transmit a range of frames, or a capture file across the network one or more times

1 In the Frame Viewer window's Summary pane, display the frames you want to send.

2 On the Tools menu, click Allow Transmit.

3 In the Select Transmit Network dialog box, select the network onto which you want to transmit, and then click OK.

4 Click Transmit Capture.

5 Choose from the following options:
- To send the entire capture file, select All Frames.
- To send a range of frames, select Selected Frames, and then type a number in the From and To boxes to specify the range.
- To send the frames one time, select Send Entire Range Once.
- To send the frames multiple time, click Send Entire Range Multiple times; then type numbers to specify the number of times you want to send the frames and the number of milliseconds you want to pass between transmissions.
- To send the frames using the same time intervals they had when they were initially captured, select Use Time Interval on Frame.
- To send the frames using a constant time interval between frames, select Set Time Interval Between Frames, and then type a number to specify the time interval.

Note
- You can transmit as many frames as you want. Also, you can transmit the same group of frames repeatedly and specify the amount of time to elapse between each transmission.

To edit frames for transmission

1 In the Frame Viewer window, display the frames you want to transmit.

2 Select a frame.

3 In the Detail pane, expand the Ethernet or Token Ring entry until a Destination Address or Source Address entry appears.

4 Select this entry.

   In the Hex pane, Network Monitor highlights the section of characters that represent the address.

5 Click anywhere in the highlighted section.

   The color of the character on which you've clicked changes color to indicate that the character can be edited.

6 Enter the new address.

 Note
▪   Before transmitting frames onto the network, carefully edit the destination addresses associated with these frames. This precaution can prevent a large transmission from abruptly overloading your network.

To print frames

1 Display a capture or capture file in the Frame Viewer window.

2 On the File menu, click Print.

3 Click Printer, or click File and then specify the file to which you want to print.

4 Under Print Range, choose the number of captured frames you want to print.

5 Click Print Setup to specify a different printer, which tray you want to print to, or print orientation settings.

6 Click Edit Fonts to specify the font in which output will be printed. If you are printing to a text file, this option has no effect.

7 Click Advanced to expand the Print dialog box. Use the expanded part of the dialog box to set printing options such as whether or not you want to apply the current display filter to printed output.

Notes

▪   When you print frames, columns that don't fit on the page horizontally are truncated. To avoid losing important information, before printing, resize the columns so they display only the information you really need and choose the landscape print option. If you resize a column to it smallest possible size, it does not print at all.

▪   To eliminate selected columns, print If you use the Print to File option in the Print dialog box, the original frame numbers associated with the frames appear in the file to which the frames are printed.

▪   If you use the Print to File option in the Print dialog box, the original frame numbers associated with the frames appear in the file to which the frames are printed.

To specify advanced printing options

1 On the Frame Viewer windows File menu, click Print.

2 Click Advanced to expand the dialog box and show the advanced printing options.

3 To print the output displayed in the Summary pane, select Print Frame Summary Lines.

4 To print the output displayed in the Detail pane, select Print Protocol Details.

5 To make the output easier to read by indenting each protocol level, select Indent Levels, and then specify how many spaces to indent.

6 To print the output using the same format as displayed in the Detail pane, select Print Same As View.

7 To print the output using an expanded view of the protocols listed in the Detail pane Select Expand All Levels.

8 To print the output displayed in the Hexadecimal pane, select Print Hex Data, and then specify the number of lines to print.

9 To apply a display filter to the output during printing, select Apply Display Filter.

10   To edit the display filter before printing the output, click Edit Filter, and then specify the appropriate options.

11   To add page breaks to the output, select Add Page Breaks.

Note

▪   If you use the Print to File option in the Print dialog box, the original frame numbers associated with the frames are preserved. If you save the filtered frames to a capture file (.cap), the original numbering on the frames is lost; the frames in a capture file always begin with 1.

To set the Print filter

1 On the File menu, click Print.

2 Click the Advanced button to expand the Print dialog box.

   In the expanded dialog box, the Apply Display Filter box is checked by default.

3 Click Edit Filter.

Note
- The Print filter is just like the Display filter, except that it applies only to the current print job.

To print all data in the capture file without applying any filters

1 On the File menu, click Print.

2 Click the Advanced button to expand the Print dialog box.

3 Clear the Apply Display Filter check box.

Notes

- The Print filter is just like the Display filter, except that it applies only to the current print job.
- If you use the Print to File option in the Print dialog box, the original frame numbers associated with the frames are preserved, even if the frames are filtered. If you save the filtered frames to a capture file (.CAP), the original numbering on the frames is lost; the frames in a capture file always begin with 1.

To display address names

- To display friendly names, click Show Address Names on the Options menu.
- To replace   names with hexadecimal addresses, click Show Address Names on the Options menu, if a checkmark appears next to the command name.

Note

- When you use the Show Address Names command, Network Monitor replaces addresses with the friendly names of the computers from which frames have been captured. If a checkmark appears next to the Show Address Names command name, this option is active.

To display vendor names

- To display vendor names, click Show Vendor Names on the Options menu.
- To replace vendor names with hexadecimal addresses, click Show Vendor Names on the Options menu, if a checkmark appears next to the command name.

Note

- When you use the Show Vendor Names option, Network Monitor replaces computer addresses with the names of the vendor that produces the network adapter card on the remote computer. If a checkmark appears next to the Show Vendor Names option, this command is active.

To rearrange columns

1 Right-click on a column heading and then drag the column to the new position. As you move the column, the word "COLUMN" appears between double arrows.

2 Release the primary mouse button.

Note

▪ If you want your modifications to be saved from session to session, after modifying column settings, select the Save Configuration option from the Capture or Display menu.

To resize columns

1 Right-click between column headings on the boundary and then drag the boundary to the new position.

2 Release the primary mouse button.

Note

▪   If you want your modifications to be saved from session to session, after modifying column settings, select the Save Configuration option from the Capture or Display menu.

To assign a label to a Frame Viewer window

1 On the Frame Viewer window's Window menu, click Label.

2 In the Description box, type the text that you want to appear in the window's title bar.

Note

▪   When you display a capture in the Frame Viewer window, the capture displays "Capture:", followed by the number that identifies the windows sequence in the currently active capture windows. If you display a capture file (.cap) in the Frame Viewer window, the title bar displays the path to the capture file.

To choose a color scheme for protocols

1 On the Display menu, click Colors.

2 In the X column, click next to the protocol for which you want to specify a color.

3 To apply the color combination you are specifying to all of the currently supported protocols, click Select All.

4 To remove all currently assigned color combinations, click Clear All.

5 From the Foreground box, select the color you want for the lettering of the text.

6 From the Background box, select the color you want for the background.

7 To save the color combination that you have specified so that it appears every time you display data in the Frame Viewer window, click Save as Default.

Notes
- Assign color schemes to supported protocols to quickly identify the protocol used to send a frame.
- When you select a line that appears in color, the color arrangement of the selected line is reversed.

To show and hide the toolbar

▪   To hide the toolbar, click Show Toolbar on the Options menu, if a check mark appears next to the command name.

▪   To display the toolbar, click Show Toolbar on the Options menu.

Note

▪   When the toolbar is displayed, a checkmark appears next to the corresponding command name on the Options menu. By default, the toolbar is displayed.

To assign a font to a protocol

1 On the Display menu, click Font.

2 In the Font box, select the Font that you want to use.

3 In the Font Style box, select the style that you want to use.

4 In the Size box, select the font size that you want to use. The larger the number that appears in this box, the larger the font that appears in the Frame Viewer window.

5 If you want to use the options that you have specified every time that the Frame Viewer window appears, select the Save As Default option.

To show and hide panes in a window
- To show a pane that is currently hidden, click the name of the pane from the Window menu.
  A checkmark appears next to the menu item that you have selected, and the pane that this item represents appears in the window.
- To hide a pane that is currently displayed, click the name of the pane from the Window menu.
  The checkmark is removed from the menu item that you have selected, and the pane that this item represents no longer appears in the window. The space formerly occupied by this pane is taken by the panes that remain visible.

Notes
- To close all panes, click Close All on the Window menu. This closes all opened Frame Viewer windows.
- To zoom in on a pane, select the pane and then click Zoom Pane on the Window menu. The selected pane expands to occupy the entire window.

To set a capture trigger

1 On the Capture menu, click Trigger.

2 To specify the event that you want to initiate the <u>trigger</u> select one or more of the following:
- To initiate a trigger when a particular pattern occurs, select Pattern Match.
- To initiate a trigger when a specified percentage of the capture buffer is filled, select Buffer Space.
- To initiate a trigger when a particular pattern occurs, and then a specified percentage of the capture buffer is filled, select Pattern Match Then Buffer Space.
- To initiate a trigger when a specified percentage of the capture buffer is filled, and then a specific pattern occurs, select Buffer Space Then Pattern Match.

3 In the Pattern group box, specify the pattern combination that must be met. If you selected Nothing or Buffer Space in the Trigger On group box, the Pattern group box is dimmed.
- To specify what byte the pattern begins on, type a hexadecimal number in the Offset box. This pattern can be measured from the beginning of the frame or from the beginning of the <u>topology header</u>.
- To specify the pattern that you want to match, type a pattern in the Pattern box.
- To specify that the pattern is in hexadecimal format, select Hex.
- To specify that the pattern is in ASCII format, select ASCII.

4 If you select an option that involves a pattern match, specify where you want to search for the pattern.
- To search for the pattern at the beginning of the frame, select From Start of Frame.
- To search for the pattern after the end of the topology header, select From End of Topology Header.

5 In the Buffer Space group box, specify the percentage of the capture buffer that must be filled. If you selected Nothing or Pattern match in the Trigger On group box, the Buffer Space group box is dimmed.

6 In the Trigger Action group box, specify the action that you want to occur when the trigger conditions are met. The default is No Action (do not initiate a trigger action).
- To stop the capture, select Stop Capture.
- To execute a command or executable file, Select Execute, and then type the command or the path to the executable file.

Note
- If you use the Network Monitor Agent to capture remotely, you can set a trigger on the remote capture. If this trigger involves the execution of a program or batch file, the execution will be invisible to users of the remote system.

To save your default configuration

- On the Capture or Display menu, click Save Configuration.

The following settings are saved for the Capture Window:
- The default panes, including size and position
- The rate at which capture statistics are refreshed
- The order and size of columns in the Session Statistics pane
- The order and size of columns in the Station Statistics pane

The following settings are saved for the Frame Viewer Window:
- The default panes, including size and position
- The foreground and background colors assigned to protocols
- Selected fonts
- The options selected in the Options dialog box. Select Options from the Display menu to view these options.
- The order and size of columns in the Summary pane

The following general settings are saved:
- Default parsers
- The default network
- Default printer
- The state of the toolbar (hidden or shown)
- Whether vendor names are substituted for addresses

Note
- Settings that you save as your default configuration are available to you from session to session.

To restore default settings

1 In Control Panel, double-click the Network Monitor Agent icon.

2 Click the Restore Default button.

To start Network Monitor from the command line
- Type **start netmon**

This command takes the following switches:
- /REMOTE *remotename*. Starts Network Monitor with a connection to the Network Monitor Agent that you specify.
- /NET *number*. Starts Network Monitor with a connection to the network number that you specify. This option enables you to use Network Monitor on any of the segments to which you are physically connected. This option does not enable you to connect to an instance of the Network Monitor Agent.
- /CAPTUREFILTER *path*. Starts Network Monitor with a specific capture filter loaded.
- /DISPLAYFILTER *path*. Use this switch to start Network Monitor with a specific display filter loaded.
- /BUFFERSIZE *number.* Starts Network Monitor with the buffersize preset to the number of bytes that you specify.
- /QUICKFILTER *type address.* When you use this option, Network Monitor begins capturing as soon as it is started and filters on the address that you have specified.
- /AUTOSTART. Use this switch if you want Network Monitor to begin capturing immediately upon starting.
- /AUTOSTOP. Use this switch if you want Network Monitor automatically to stop capturing when the capture buffer is full.

To set Capture and Display passwords

1 In Control Panel, double-click on the Monitoring Agent icon.

2 In the Configure Network Monitoring Agent dialog box, click Change Password.

3 Choose one or more of the following options:
▪   If you've previously set a Capture password, and you want to change it, type the previous password in the Old Capture Password box, and then, under Capture Password, type the new password.
▪   If you have not previously set a Capture password, then under Capture Password, type a Capture password.
▪   If you want some users to have permission only to open capture files, then under Display Password, type a Display password.
▪   If you do not want to set password protection, click No password.
▪   If you do not set a password, any computer can connect to the Network Monitor Agent on your computer and use it to capture from the network. If you are running a full installation of Network Monitor and do not set a password, any user with physical access to your computer can use it to capture statistics, compromising the security of your network.
▪   A Capture password allows the user both to capture statistics from the network and to display captured data.
▪   A Display password allows the user only to open previously saved capture (.CAP) files.

Note
▪   If a Windows NT computer is running a full installation of Network Monitor, the Capture and Display passwords that you set apply both to the full installation and to the Network Monitor Agent on that computer.

To edit an address in an address database

1 On the Capture or Display menu, click Addresses.

2 Select the Address that you want to edit, and then click the Edit button.

3 To associate the displayed address with a new address type, select the address type from the Address Type list, and then type in the new address. When you associate a name with a new address type, its association with the previous address type is lost.

4 To change the friendly name associated with the address, type the name in the Name box.

5 To associate a comment with the address, type the comment in the Comment box.

Note

▪   Changes that you make to an address are reflected when you include the edited address in a capture or display filter.

Open File

Use this button to open a file.

Save File

Use this button to save a file.

Display Filter

Use this button to display the Display Filter dialog box, which you can use to specify criteria for the type of data you want to display.

Protocol == Any

Use this line in the Expression Editor window to determine what protocols will be displayed. Double-click on this line to display the Expression dialog box, which you can use to add or remove protocols, addresses, and protocol properties from your display filter. By default, Network Monitor displays every captured protocol that Network Monitor supports.

Any <-> Any

Double-click on this line to display the Expression dialog box, which you can use to determine which computers, traffic directions, protocols, and protocol properties will be displayed in the Frame Viewer window.

Unless you edit the **Any <-> Any** line, all of the captured data sent in any direction (<->) on your network among any computers (ANY) will be displayed.

Expression...

Click on this button to display the Expression dialog box, which you can use to change the display of computer addresses, protocols, protocol properties, and traffic directions shown in the Frame Viewer window.

If a filter operator (AND, OR, or NOT) is selected, the caption of this button is "Operator". You can choose the Operator button to change the displayed operator.

And

Click this to place another AND tab in the decision tree displayed in the Display Filter window.

Or

Click this to place an OR tab in the decision tree displayed in the Display Filter window.

Not

Click this to place a NOT tab in the decision tree displayed in the Display Filter window.

Operator

Click this to display the Expression dialog box, which you can use to change the expressions that appear in the Display Filter window.

Line

After selecting a line in the Decision Tree, click this button to delete that line.

Branch

After selecting a branch in the Decision Tree, click this button to delete that branch.

All

To delete everything that appears in the decision tree, click this button.

Save...

Click this to save the Display Filter that you have designed. By doing so, you can avoid creating a filter from scratch the next time you need it.

Load ...

Click this to load a previously designed Display Filter.

Help

Click this to display Network Monitor context-sensitive Help.

Cancel

Click this to exit the Display Filter dialog box.

OK

Click this to activate the filter that you have designed.

SAP/ETYPE

This line lists the protocols that are currently enabled. If you want to alter this list, double-click on this line.

Any <--> Any

This is the default setting in the Address Pairs section of the Capture Filter dialog box. This line indicates that Network Monitor will capture all frames sent among all addresses. To alter this line and to specify specific computer addresses, double-click on the (Address Pairs) line.

Pattern Matches

Use this line to specify the patterns that you want to capture. To edit this line to specify a pattern, double-click on it.

Address

Click this to add a computer address from the Network Monitor address database.

Pattern

This button is active only when the Pattern Matches line is selected and displays the Pattern Match dialog box. Use this dialog to specify the patterns that you want Network Monitor to capture.

OR

Click this to add an OR tab to the expression tree.

NOT

Click this to add a NOT tab to the expression tree. When you add a NOT tab to the expression tree, your capture filter does not capture the line that follows the tab.

Line

This button is active only when a line in the expression tree is selected. Click this button to edit the contents of the selected line.

Line

This button is active only when a line in the expression tree is selected. Click this button to delete the selected line.

Save

Click this to display the Save Capture Filter dialog box, which you can use to save the filter that you have designed.

Load

Click this to display the Load Capture Filter dialog box, which you can use to load a previously designed capture filter into the Capture Filter dialog box.

Help

Click this to display Network Monitor Help on the Capture Filter dialog box.

Cancel

Click this to exit the Capture Filter dialog box without implementing any of the decisions that you have placed in the expression tree.

OK

Click this to implement the decision statements that currently appear in the expression tree.

Protocol Parsers Dialog Box

Use the Protocol Parsers dialog box to enable or disable the <u>parsers</u> that read and interpret data that has been transmitted using various protocols. When you disable a parser, Network Monitor does not capture data transmitted in the associated protocol until you re-enable it.

Use the Protocol Parsers dialog box to set the following options:

- <u>Enabled Protocol Parsers</u>
- <u>Disabled Protocol Parsers</u>
- <u>Save As Default</u>

Enabled Protocol Parsers

This box displays all of the parsers that are currently enabled. By default, all Network Monitor protocols are initially enabled.

Disabled Protocol Parsers

This box displays all of the parsers that are loaded into the \PARSERS subdirectory, but that are not enabled. If a parser appears in this box, you are currently unable to capture data sent in the associated protocol.

Save As Default

Check this box if you want the parsers that appear in the Enabled Protocol Parsers box to represent your default configuration. If you clear this box, Network Monitor will enable all parsers in the \PARSERS subdirectory.

Capture Filter Dialog Box

Displays the capture filter underline decision tree and allows you to specify the underline frames you want to capture. This dialog box includes the following controls, which allow you to make changes to the decision tree:

SAP/ETYPE

(Address Pairs)

(Pattern Matches)

Add Section

Edit Section

Delete Section

Load button

Save button

SAP/ETYPE

This line lists the protocols that Network Monitor is currently configured to capture. To edit this line, double-click on it.

(Address Pairs)

The line that appears beneath this heading lists the computer address pairs from which Network Monitor is currently configured to capture information.

(Pattern Matches)

The line that appears beneath this heading lists the patterns that the current filter is configured to capture.

Add Section

- Click the Address button to display the Address Expression dialog box, which you can use to specify the address pairs between which you want to capture data.
- Click the Pattern button to display the Pattern Match dialog box, which you can use to specify that you want to capture only those frames containing a specific pattern of ASCII or Hexadecimal data.
- Click the **OR** button to add an **OR** branch to the decision tree. This option applies only to pattern matches.
- Click the **NOT** button to add a **NOT** branch to the decision tree or to negate a branch of the tree. This option applies only to pattern matches.

Edit Section

Click the Line button in this section to alter the currently highlighted line.

Delete Section

Click the Line button in this section to delete the currently highlighted line.

Load

Click this to display the Load Capture Filter dialog box, which you can use to replace the current capture filter with a capture filter that has previously been saved to a file.

Save

Click this to display the Save Capture Filter dialog box, which you can use to save the current capture filter as a file. Later, to use this capture filter again, you can use the Load button to open this file.

Address Database Dialog Box

Use the Address Database dialog box to add, delete, or edit addresses in an <u>address database</u>. You can also use this dialog box to save the current address database or load a different one.

The Address List on this dialog displays the following information about each computer: a friendly name; the 12-digit <u>hexadecimal</u> network <u>address</u>; the address type (for example, MAC or IP); the name of the vendor who created the network card; and a comment or additional information.

The following options are available in this dialog box:

<u>Add</u>

<u>Edit</u>

<u>Delete</u>

<u>Load</u>

<u>Save</u>

Add

Displays the Address Information dialog box, which you can use to add a new computer address to the Address Database.

Edit

Displays the Address Information dialog box, which you can use to edit the currently selected computer address. You can display this dialog box also by double-clicking on any address that appears in the Address Database dialog box.

Delete

Deletes the currently selected computer address from the Address Database.

Load

Displays the Open Address File dialog box, which you can use to load a different address database in place of the one currently displayed. Unless you explicitly save changes you have made to the currently displayed database, changes made to the Address List during a session will be lost when you load a new address database or when you exit Network Monitor.

Save

Displays the Save Addresses As dialog box, which you can use to save the currently displayed address database to a file. Unless you explicitly save the changes that you make to the current database, these changes will be lost when you load a new address database or when you exit Network Monitor.

Transmit Frames Dialog Box

Use the Transmit Frames dialog box to transmit onto the network one or more <u>frames</u> from the capture file displayed in the Frame Viewer window. The Transmit Frames dialog box includes the following controls:

<u>All Frames button</u>

<u>Selected Frames button</u>

<u>Use Filter</u>

<u>Send Entire Range Once button</u>

<u>Send Entire Range Multiple Times button</u>

<u>Use Time Interval on Frame button</u>

<u>Set Time Interval Between Frames button</u>

All Frames

Select this button to send frames from the entire range of the capture file. You can select All Frames or Selected
Frames, but not both. You can send the entire range either filtered or unfiltered.

Selected Frames

Enables you to send a range of frames that you specify. You can select All Frames or Selected Frames, but not both. You can send the selected range either filtered or unfiltered.
- In the From box, specify the number of the first frame in the range you want to send.
- In the To box, specify the number of the last frame in the range you want to send.

Use Filter

Select this box to apply the current Display filter settings to the capture file before transmitting any frames.

Send Entire Range Once

Select this button to transmit all the frames only once. You can select Send Entire Range Once or Send Entire Range Multiple Times, but not both.

Send Entire Range Multiple Times

Select this button to transmit all the frames multiple times to enable the Send and Delay text boxes, which you can use to specify the following options:

- In the Send __ Times (cycles) box, specify the number of times that you want to transmit the specified range of frames onto the network.
- In the Delay __ mSec Between Cycles box, specify the amount of time (in milliseconds) you want to transpire between each send.

Use Time Interval on Frame button

Sends frames at the time intervals that were recorded during capture.

Set Time Interval Between Frames button

Enables the Time (msec) Between Frames box, which you can use to specify the time delta on the frames that you are transmitting.

Other Network Monitor Installations Dialog Box

Use the Other Network Monitor Installations dialog box to identify other computers on your <u>local area network</u> that are using Network Monitor to monitor the network. This feature enables you to:

- Protect the integrity of your network.
- Avoid the use of unlicensed installations of Network Monitor on your network.

This dialog box contains the following features:
- <u>Machine Name</u>
- <u>User Name</u>
- <u>Current State</u>
- <u>Adapter Address</u>
- <u>Version</u>
- <u>License Number</u>
- <u>Total Installed</u>
- <u>Total Running</u>
- <u>Total Capturing</u>
- <u>Refresh List</u>
- <u>Add Names to Address Database</u>

Machine Name

Identifies the name of the computer on which Network Monitor is installed. This category is filled in only if your Address Database contains information on this computer.

User Name

Displays the user name associated with the Machine Name. This category is filled in only if your Address Database contains information on this computer.

Company Name

Identifies the company that owns the license to the Network Monitor installation. This category is filled in only if your Address Database contains information on this computer.

Current State

This column identifies the current state of the Network Monitor installation on the remote computer. There are four possible states:

- Driver installed: The Network Monitor driver is installed, but Network Monitor is not currently running on the remote computer.
- Running: Network Monitor is running on the remote computer but is not currently capturing data.
- Capturing: Network Monitor is capturing data on the network.
- Transmitting: Network Monitor is transmitting frames onto the network.

Adapter Address

This column identifies the network adapter card address of the computer on which Network Monitor is installed. This column is filled in for any installation that Network Monitor detects.

Version

Identifies the applications version number. This column is filled in for any installation that Network Monitor detects.

License Number

Identifies the license number of the Network Monitor installation. If you detect two installations of Network Monitor that have the same license number, a license violation has occurred.

Refresh List

Use this button to browse the network again to determine the location and states of Network Monitor installations on your network. This button enables you to update regularly the statistics displayed in the Other Network Monitor Installations dialog box.

Total Installed

Identifies the total number of Network Monitor installations on your network.

Total Running

Identifies the total number of currently running Network Monitor installations on your network.

Add Names to Address Database

Select this option to add the names displayed in this dialog box to the default address database (Default.adr).

Total Capturing

Identifies the total number of Network Monitor installations on your network that are currently capturing data.

Print Dialog Box (Advanced)

The Advanced button expands the Print dialog box to include the following controls:

- [Print Frame Summary Lines](#)
- [Print Protocol Details](#)
- [Indent Levels](#)
- [Indent Spaces per Level](#)
- [Print Same as View](#)
- [Expand All Levels](#)
- [Print Hex Data](#)
- [Lines of Hex Data to Print](#)
- [Apply Display Filter](#)
- [Edit Filter](#)
- [Add Page Breaks](#)

Note

- If you use the Print To File option in the Print dialog box, the original frame numbers associated with the frames are preserved, even if the frames are filtered. If you save the filtered frames to a capture file (.CAP), the original numbering on the frames is lost; the frames in a capture file always begin with 1.

Print Frame Summary Lines

Select this box to print the information that appears in the Summary pane of the Frame Viewer window.

Print Protocol Details

Select this box to print the information that appears in the Details pane of the Frame Viewer window.

Indent Levels

Select this button to indent each successive protocol level.

Indent Spaces per Level

In this box, specify the number of spaces that you want to indent each level of detail.

Print Same as View

Select this box to print a document that reflects exactly the structure of the Frame Viewer window.

Expand All Levels

Select this box to print a document that contains an expanded view of all of the protocols listed in the Detail Pane of the Frame Viewer window.

Print Hex Data

Select this box to print the data that appears in the Hex Pane of the Frame Viewer window.

Lines of Hex Data to Print

In this box specify a number of lines of hexadecimal data that you want to print.

Apply Display Filter

Select this box to apply a display filter to the data you want to print.

Add Page Breaks

Select this checkbox to add page breaks to the printed material.

Edit Filter

Click this if you want to edit your display filter before applying it to the data that you want to print.

Print Dialog Box

Use the Print dialog box to specify basic printer options. The Print dialog box contains the following options:

- Output to
- Setup Print
- Edit Fonts
- Print Range
- Advanced

Advanced

Expands the Print dialog box to include advanced printer options.

Output to

Use the buttons in this group box to specify where you want to direct output.
- To direct output to a printer, select the Printer button.
- To direct output to a file, select the File button, and then specify the file to which you want to direct output.

Setup Print

Displays the Print Setup dialog box, which you can use to change printers and printer settings.

Edit Fonts

Displays the Font dialog box, which you can use to specify the font to use in printed output. It has no effect on output to a text file.

Print Range

Use the buttons in this group box to specify which frames you want to print.
- To print all of the displayed frames, select the All button.
- To print only a portion of the displayed frames, select the Frame button, and then specify the range of frames that you want to print in the From/To boxes. By default, these boxes reflect the total number of frames in the capture.

Add Section

Use the buttons in this group box to add expressions to the decision tree.

- The Address button allows you to specify address pairs.
- The Pattern button allows you to specify an ASCII or hexadecimal pattern.
- The Or button allows you to add an Or branch to the decision tree.
- The Not button allows you to add a Not branch to the decision tree or to negate a branch of the tree.

Edit Section

Click the Line button to edit a line that you have selected in the decision tree.

Delete Section

Click the Line button to edit a line that you have selected in the decision tree.

Load

Press this button to display the Load Capture Filter dialog box, which you can use to load a pre-designed filter into the Capture Filter dialog box.

Save

Press this button to display the Save Capture Filter, which you can use to save the filter you have designed as a .CAP file.

Load Capture Filter Dialog Box

Use this dialog box to load a previously saved capture file into the Capture Filter. This dialog box contains the following controls:
- File Name
- List File of Type
- Directories
- Drives
- Network

File Name

Specify a filename in the File Name text box. Or select a name from the attached drop-down list box.

List File of Type

From this drop-down list, select the extension of the files that you want to load. Files in the currently selected directory that have this extension appear in the File Name list box. The default file type for Network Monitor is .CF.

Directories

Double-click on the directory that contains the capture filter file that you want to load.

Drives

Select the drive that contains the capture filter file that you want to load.

Station 1

In this column, select the first address in the address pair. This can be the originating or the destination address, depending on the arrow that you select in the Direction list.

Network

If your capture filter file resides on a network drive, click the Network button. The Connect Network Drive dialog box appears, and allows you to make or select a network connection and to load your filter from the network drive that you specify.

Address Expression Dialog Box

The Address Expression dialog box allows you to create a new <u>address</u> expression to be added to the Address Pairs section of the current capture filter.

This dialog box allows you to specify the following options:
- <u>Include</u>
- <u>Exclude</u>
- <u>Station 1</u>
- <u>Station 2</u>
- <u>Direction</u>
- <u>Edit Addresses</u>

Exclude

Select this option to exclude the currently specified address pair from the capture filter decision tree.

Edit Addresses

Displays the Address Database dialog box, which you can use to modify the current address database.

Direction

From this list, select an arrow to indicate the direction of the traffic that you want to include or exclude from the capture filter decision tree.
- Select the single arrow to specify that you want to include in your expression only traffic traveling in the direction that the arrow points between Station 1 and Station 2.
- Select the double arrow to include in your expression traffic traveling in both directions between Station 1 and Station 2.

Station 2

In this column, select the second address in the address pair. This can be the originating or the destination address, depending on the arrow that you select in the Direction list.

Include

Select this option to include the current address pair in the capture filter decision tree.

Capture Trigger Dialog Box

Use the Capture Trigger dialog box to specify an event that will act as a trigger, as well as the action that will result from this event. This dialog box includes the following features:

- Trigger on
- Pattern
- Buffer Space
- Trigger Action

Trigger on

Use this area to specify the conditions that induce the trigger action. By default, no trigger is set. The following options are available:

- Select Pattern Match to perform the trigger action when a specified Hexadecimal or ASCII pattern match occurs.
- Select Buffer Space to perform the trigger action when a Capture has filled a specified percentage of the capture buffer.
- If you select Pattern Match Then Buffer Space, Network Monitor begins monitoring buffer space after the specified pattern is encounter and then performs the trigger action when both specified conditions exist.
- If you select Buffer Space Then Pattern Match, Network Monitor begins monitoring for the specified pattern when a capture has filled a specified percentage of the capture buffer, then performs the trigger action when both specified conditions exist.

Pattern

If your trigger action includes a pattern match, use this section to specify the pattern. The following pattern characteristics are available:

- Use the Offset box to designate the number of hexadecimal bytes after the beginning of the frame to begin looking for the pattern. By default the pattern triggers only if the pattern occurs at the beginning of the frame.
- To start the search for the pattern at the beginning of the frame, select From Start Of Frame.
- To start the search for the pattern beyond the topology header, select From End Of Topology Header. The topology header is the section of a frame that is attached to a frame by the networking hardware. It includes information like the source and destination address of the frame, and does not include information from the frame's data field.
- In the Pattern box, specify the pattern that you want to initiate the trigger.
- Select the Hex or ASCII buttons to indicate whether the pattern you specified is hexadecimal or ASCII.

Buffer Space

In this section, specify how full the capture buffer should be before the trigger action is performed. For example, if you want to trigger action to occur when the capture buffer is three-quarters filled, select 75%.

Trigger Action

When the trigger criteria that you specify are met, the trigger that you specify occurs. The following are the available trigger results:

Select Stop Capture to stop the capture process.

Select No Action if you want the capture process to continue without interruption while a command executes.

Select Execute if you want to execute a command or an executable file when the trigger specifications are met.

- To start an executable file, type the path to the file.
- To use a command that represents an executable file (any of the NET commands, for example), simply type the command.
- To use a command that requires the command processor (COPY, for example), type CMD /K, and then type the command.
- If you select the Execute option, and you are capturing on a remote system, the program you specify is executed on the remote system. This event is invisible to the remote system's users.

Font Dialog Box

This dialog box allows you to change the fonts used to display or print captured frames. The Font dialog box has the following controls:

- <u>Font</u>
- <u>Style</u>
- <u>Size</u>
- <u>Save as Default</u>

Font

The Font list box lists available fonts. You may prefer a monospace font such as Courier or Fixed Sys rather than a proportional font such as MS Sans Serif. Depending on the configuration of your printer, some fonts may be unavailable for printing.

Style

From the Font Style list box you can select the variation of the chosen font that is easiest for you to read.

Size

From the Size list box you can select the type size that gives you the best combination of readability and data per screen. Other ways to fit data onto the screen include maximizing the window and rearranging columns.

Save As Default

The Save As Default check box lets you specify that the font setting you have specified be used every time you start Network Monitor.

Capture Buffer Settings Dialog Box

This dialog box contains the following controls:
- The Buffer Settings box. Use this box to specify the size of your capture buffer. The default size is 1.0 MB.
- The Frame Size box. Use this box to specify the number of bytes that you want Network Monitor to capture from each frame.

Note
- It is recommended that you set the buffer size to the amount of memory available on your system. If your buffer setting exceeds this amount, frames are dropped because of memory swapping.

Capture Filter SAPs and ETYPEs Dialog Box

Use this dialog box to specify the protocols that Network Monitor captures during the execution of your capture filter. The choices that you make in this dialog box are reflected in the line of the Capture filter decision tree that begins with SAP/ETYPE=.

This dialog box contains the following controls:
- Enabled Protocols
- Disabled Protocols
- Enable Button
- Disable Button
- Enable All Button
- Disable All Button

Enabled Protocols

This box lists all currently enabled controls. The Enabled box consists of four columns:
- Enabled Protocol. This list contains the names of all of the currently enabled protocols.
- Comment. This list contains a brief description of the protocol.
- Type. This list contains the protocol type (ETYPE or SAP).
- Values. This list contains the possible values for the enabled protocols.

Double-click on any line in this box to move the associated protocol to the Disabled box. You can also sort on any column in this box by double-clicking on the column head.

Disabled Protocols

Lists all currently disabled protocols. This list box has four columns:
- Disabled Protocol. This list contains the names of all of the currently enabled protocols.
- Comment. This list contains a brief description of the protocol.
- Type. This list contains the protocol type (ETYPE or SAP).
- Values. This list contains the possible values for the disabled protocols.

Double-click on any line in this box to move the associated protocol to the Enabled box. You can also sort on any column in this box by double-clicking on the column head.

Enable

Causes the protocols that you highlight in the Disabled box to be moved to the Enabled box.

Disable

Causes the protocols that you highlight in the Enabled list box to be moved to the Disabled list box.

Enable All

Causes all available protocols to be enabled.

Disable All

Causes all available protocols to be disabled.

Protocol Colors Dialog Box

This dialog box allows you to assign colors to protocols for easier viewing.

The Protocol Colors Dialog Box contains the following options:
- X
- Name
- Description
- Colors
- Select All
- Clear All
- Save as Default

The colors that you specify in this dialog box appear in the following locations:
- in the Summary pane to highlight frames using that protocol
- in the Detail pane to highlight the detail information pertaining to that protocol
- in the Hex pane to highlight the corresponding hexadecimal data

When you highlight a line in the Detail pane, the colors for that protocol are reversed: the color that is normally used for the background is used for the lettering and the color that is normally used for the lettering is used for the background.

Name

This box contains the name of the currently supported protocols. To select a protocol, point to the protocol with your mouse, and then press your primary mouse button.

Description

This box contains a description of the currently selected protocol.

Colors

This box contains three controls:
- Use the Foreground list to specify the color for the text of the protocol.
- Use the Background list to specify the color for the background of the text.

Select All

Click this to select all of the currently enabled protocols.

Clear All

Click this to unselect all of the currently selected protocols.

Save as Default

When you have finished specifying the colors that you want to use, select this checkbox to save your selections as your default configuration.

Pattern Match Dialog Box

Use this dialog box to specify that you want to capture only those frames having a specific pattern of hexadecimal or ASCII data. You can specify that the pattern start at the beginning of the frame or that it be a specified number of bytes (offset) into the frame. The Pattern Match dialog box includes the following controls:

- <u>Offset (in hex)</u>
- <u>From Start of Frame</u>
- <u>From End of Topology Header</u>
- <u>Pattern</u>
- <u>Hex</u>
- <u>ASCII</u>

From End of Topology Header

Measures your offset from the end of the topology header, which is the number of bytes attached to a frame on the physical layer. This header identifies the network type. For example, on an Ethernet network, the topology header consists of 14 bytes. In a TokenRing environment, the number of bytes varies.

From Start of Frame

Measures the offset you specified from the beginning of the frame.

Offset (in hex)

In this box, type the number of bytes from the beginning of the frame to look for the pattern. The way Network Monitor interprets this number depends upon whether you specify the From Start Of Frame or the From End Of Topology Header options.

Pattern

In this box, type the hexadecimal or ASCII pattern.

Hex

Select this radio button to have the pattern read as hexadecimal.

ASCII

Select this radio button to have the pattern read as ASCII.

Display Filter Dialog Box

The Display Filter allows you to limit your display to frames that have the characteristics that you specify. For example, you can specify the protocols, computer addresses, and protocol properties that you want to display in the Frame Viewer window. To set these options, make changes to the underlined decision tree that appears in this dialog box.

To change a logical operator (AND, OR, or NOT), click on it to cycle through the AND, OR, or NOT options.

In the Display Filter dialog box, you can specify the following options:
- Protocol == Any
- Any <-> Any
- Add Section
- Edit Section
- Delete Section
- Load button
- Save button

Note
- If an expression is selected, the Edit button's label changes to Expression, and you can click on this button to display the Expression dialog box. If an operator is selected, the Edit button's label changes to Operator, and you can click on this button to cycle through the AND, OR, or NOT options.

Add Section

Click the Expression button to display the Expression dialog box, which you can use to specify the computer address pairs, protocols, and protocol properties that you want to display.

- Click the AND button to add an AND tab to the currently selected branch of the decision tree.
- Click the OR button to add an OR branch to the decision tree.
- Click the NOT button to add a NOT branch to the decision tree or to negate a branch of the tree.

Edit Section

After selecting a line in the decision tree, click this button to display the Expression dialog box. This dialog box allows you to edit the selected line.

Delete Section

- Click the Line button in this section to delete the currently selected line of the decision tree.
- Click the Branch button in this section to delete the currently selected branch of the decision tree.
- Click the All button in this section to delete the entire decision tree.

Load

Click this to display the Load Display Filter dialog box, which you can use to load a Capture filter that has previously been saved to a file, in place of the current Display filter.

Save

Click this to display the Save Display Filter dialog box, which you can use to save as a .DF file the filter configuration that currently appears in the decision tree.

Protocol = Any

This line reflects the protocols that you want to display. To modify this line:

- Select the line, and then click the Expression button in the Edit group box.
- Or, double-click on the line.

Either of these actions displays the Expression dialog box, in which you can specify the addresses, protocols, or protocol properties that you want to display.

Any <-> Any

This line reflects the computer address pairs that you want to display. To modify this line:
- Select the line, and then click the Expression button in the Edit group box.
- Or, double-click on the line.

Either of these actions displays the Expression dialog box, which you can use to specify the addresses, protocols, or protocol properties that you want to display.

Expression Editor Dialog Box

Use the Expression Editor dialog box to:
- Write or edit an expression that will appear in a display filter's <u>decision tree</u>.
- Search a frame in the Frame Viewer window on the basis of criteria that you provide.

The main categories for which you can specify options are represented by tabs. This dialog box contains the following sections:
- <u>Expression</u>
- <u>Address</u>
- <u>Protocol</u>
- <u>Property</u>

Expression

The Expression box appears regardless of which tab you have selected.

This box shows the expression line that you want to locate or to add to a display filter's decision tree. It changes as you select items in other areas of the dialog box. You cannot edit this text box directly.

Address

Use this tab to specify the address you want to find or to add an Address expression to the decision tree. This tab category displays in the Station 1 and Station 2 boxes all of the addresses contained in the currently loaded address database. For each address, the friendly name, type of address, hexadecimal address, and associated comments are included.

Use this category to specify the following options:
- In the Station 1 and Station 2 boxes, select the computer addresses between which you want to monitor traffic, or that you want to locate.
- In the Direction box, select the arrow that indicates the traffic direction that you want to monitor or locate. For example, to identify traffic that travels from Computer 1 to Computer 2, select Computer 1's name, then the --> symbol, then Computer 2's name.
- Click the Edit Addresses button to edit the currently selected address.

Note
- You should specify Broadcast, Multicast, and Functional only as destination addresses.

Protocol

Use the Protocol category to specify the protocols that you want to find in the Frame Viewer window or to add a display filter decision tree.

If you are attempting to locate a frame, Network Monitor will search for the protocols that appear in the Enabled Protocols list box, and will not attempt to locate protocols listed in the Disabled protocols list box. If you are designing a display filter, protocols listed in the Enabled Protocols list box will be added to the filter decision tree.

After selecting one of the protocols in the Enabled Protocols or Disabled Protocols boxes, specify one of the following options:

- Click the Disable button to move the selected protocol to the Disabled Protocols list box.
- Click the Enable button to move the selected protocol to the Enabled Protocols list box.
- Click the Disable All button to move all protocols to the Disabled Protocols list box.
- Click the Enable All button to move all protocols to the Enabled Protocols list box.

Property

Use the Property category to specify which protocol properties you want to find or to display in the display filter decision tree.

- The Property category consists of the following options:
- Protocol Property. If a plus (+) sign appears next to a protocol name, the protocol is not expanded. To expand it, double-click on the plus sign, and then select one of the displayed properties.
- Relation. The relational operators in this box specify the connection between the Protocol Property and its possible values.
- Value: Displays the possible values to which the highlighted property is compared.
- The Hex and Decimal radio buttons, when displayed, allow you to specify whether the number in the Value text box is displayed in hexadecimal or decimal.

Note

- For certain properties, the Hex Offset text box appears. This text box allows you to specify how many hex digits from the beginning of the frame to look for the specified property.

Save Dialog Box

Use this dialog box to:
- Save captured data in a file that can be viewed in Network Monitor at a later time. (To save the data to a text file, print to a file.)
- Save a filter that you have designed or edited.
- Save an address database.

This dialog box allows you to specify the following options:
- File Name
- Comment
- List Files of Type
- Directories
- Drives
- Network
- Filtered
- Range

File Name

Either type the filename in the File Name text box, or select a name from the attached drop-down list box.

Comment

Type any comment that will help you identify the file.

List Files of Type

Specify the two- or three-letter file extension (the file type) of the files that you want to see in the drop-down list box under File Name. These are the default filename extensions:

- For capture files: .CAP
- For capture filters: .CF
- For display Filters: .DF
- For address database files: .ADR

Directories

If you want to save the file to a different directory than is listed under Directories, either select a different directory from the attached drop-down list box, or include the complete path in the File Name text box.

Drives

From the list of drives to which you are connected, select the drive to which you want to save the file.

Network

Displays the Connect Network Drive dialog box, which you can use to make a network connection without leaving Network Monitor.

Range

Use the Range boxes to specify the numerical range of the frames you want to save to a capture file (.CAP).

This option is available only if you are saving a capture file. It does not appear when you save a filter or an address database.

- When a range of frames is saved to a capture file, the numbers associated with the frames are changed; in a capture file, frame numbers always begin with 1, regardless of the number associated with the original frame. Similarly, if you apply a display filter, then save the filtered frames, the frame numbers in the capture file begin with 1. If, on the other hand, you use the Print To File option in the Print dialog box, the original frame numbers associated with the frames are preserved.

Filtered

Use the Filtered checkbox to apply the current Display filter to the data as the data is saved. When you use this option, the saved frames are renumbered so that no gaps appear in the sequence.

This option is available only when you are saving a capture file. It does not appear when you save a filter or an address database.

Display Options Dialog Box

Use the Display Options dialog box to specify the time delta and the protocols that you want to appear in the Summary pane of the Frame Viewer window.

This dialog box contains the following options:

- Time
- Summary Protocol

Time

Options that you specify in the Time box determine the time that appears in the Time column of the Summary pane. The following options are available:

- Time of day. If you select this option, Network Monitor displays the system time at which the frame was captured.
- Seconds from beginning of capture. If you select this option, Network Monitor displays, in milliseconds, the time that elapsed between the beginning of the capture and the capture of the frame.
- Seconds from previous frame. If you select this option, Network Monitor displays, in milliseconds, the time that elapsed between the capture of a frame and the capture of the frame that precedes it. (Note that the last captured frame may or may not be displayed in the current filtered view.)

Summary Protocol

The protocol summary information in the Description column of the Summary pane can show any one of the following:

- Last protocol in frame. Displays information on the last protocol that appears in the captured frame.
- Auto (based on protocols in display filter). Displays information on the protocol that is probably most interesting to you, based on decision statements in the current display filter.

Go To Dialog Box

This dialog box allows you to go to a specific frame in the currently displayed capture file.

The second field in the status bar of the Frame Viewer window lists the number of the frame that is currently highlighted, followed by a / and the total number of frames in the current capture file.

In the Frame Number box, specify the number of the frame that you want to highlight.

Open File Dialog Box

Use the Open File dialog box to:
- Open a .CAP file for viewing in the Frame Viewer window.
- Open a .CF file in the Capture Filter dialog box.
- Load a .DF file in the Display Filter dialog box.
- Load a .ADR database in the Open Address File dialog box.
- Select an executable or command file to run when capture trigger specifications are met.

This dialog box allows you to specify the following options:
- File Name
- List Files of Type
- Directories
- Drives
- Network

File Name

Type the filename in the File Name text box. Or, select a name from the attached drop-down list box.

List Files of Type

Specify the three-letter file extension (the file type) of the files that you want to see in the drop-down list box under File Name. The default file type for Network Monitor capture files is .CAP.

Directories

If the file is in a different directory than is listed under Directories, select a different directory from the attached drop-down list box or include the complete path in the File Name text box.

Drives

Select a different drive from the attached drop-down list box or include the complete path, including the drive letter, in the File Name text box.

Network

The Network button opens the standard Connect Network Drive dialog box, allowing you to make a network connection without leaving Network Monitor.

Address Information Dialog Box

The Address Information dialog box allows you to edit individual address entries or add a new entry.
- Use the Type list to associate an address type with a displayed address. For example, if an name is associated with an Ethernet address, and you want to associate it with an IP address, select IP from this list, then type the IP address in the Address box. When you associate a name with a new address type, its association with the previous address type is lost.
- The Address box contains the hexadecimal address by which the computer is known to the network.
- The Name box contains a friendly name, such as the computer name.
- The Comment box contains additional information. For example, you might enter the type of CPU or network card, or mention some problem the computer has exhibited.
- Use the Permanent Name check box to use the text in the Name box as the computer's name in the local address database.

The Graph Pane

The Graph pane provides a graphical representation of the total capture statistics for the current capture. By default, this pane appears in the upper-left corner of the Capture window.

The Graph pane displays the following statistics:
- % Network Utilization
- Frames Per Second
- Bytes Per Second
- Broadcasts Per Second
- Multicasts Per Second

The Station Statistics Pane

The Station Statistics Pane displays the statistics on a workstation's activity on a network. By default, this pane appears at the bottom of the Capture window:

The Station Statistics Pane displays the following statistics:
- Network Address
- Frames Sent
- Frames Rcvd
- Bytes Sent
- Bytes Received
- Directed Frames Sent
- Multicasts Sent
- Broadcasts Sent
- Network Monitor reflects station statistics only on the first 128 unique addresses that it detects. To gather statistics on a specific workstation, design a capture filter.

The Session Statistics Pane

A session designates the period of time during which two computers are connected and exchange information. The Session Statistics pane displays statistics on a per-session basis, identifying both participants in a conversation, and how much information has passed in either direction between them:

This pane consists of the following components:
- Network Address 1
- 1-->2
- 2-->1
- Network Address 2
- Network Monitor reflects session statistics only on the first 128 unique sessions that it detects. To examine a particular session, design a capture filter.

The Total Statistics Pane

The Total Statistics pane of the Capture window consists of panels that provide an overall view of the activity on your network. By default this pane appears in the upper-right corner of the Capture window:

The following list explains the information contained in these four panels:
- Network Statistics
- Captured Statistics
- Per Second Statistics
- Network Card (MAC) Statistics
- Network Card (MAC) Error Statistics

The Summary Pane

The summary pane of the Frame Viewer window, displays a list of the frames that were captured in the order in which they were captured. This pane displays the following information:

- Frame Number
- Time
- SRC MAC Address
- Dst MAC Address
- Protocol
- Description
- Src Other Addr
- Dst Other Addr
- Type Other Addr

The Detail Pane

The Detail pane displays information about the frame that is currently selected in the Summary pane, including details about the frame itself and about the protocols that were used to send it.

You can expand or collapse the levels of detail that appear in this pane. If a plus sign (+) appears next to a line, you can expand the line by double-clicking on it. When a line is expanded, a minus (-) sign appears next to it, and you can collapse the line by double-clicking on it.

The Detail pane consists of the following sections:
- Frame
- Protocol

The Hex Pane

This pane consists of two sections:

- The hex section displays the hexadecimal contents of the frame.
- The ASCII section displays an alphabetical representation of the frame's hexadecimal contents.

As you select a line in the Detail pane, the section of the frame that the line represents is automatically selected in both sections of the Hex pane.

% Network Utilization

This bar displays dynamically the percentage of your network's available resources that are being used.

Frames Per Second

Displays the number of frames-per-second that are being transmitted over your network.

Bytes Per Second

Displays the number of bytes-per-second that are being transmitted over your network.

Broadcasts Per Second

Displays the number of broadcasts-per-second that are being transmitted over your network.

Multicasts Per Second

Displays the number of multicasts-per-second that are being transmitted over your network.

Network Address 1

This column displays the network address of one of the participants in a network session.

1 --> 2

This column displays the number of frames sent from the address listed in the Network Address 1 column to the address listed in Network Address 2.

2 <-- 1

This column displays the number of frames sent from the address listed in the Network Address 2 column to the address listed in Network Address 1.

Network Address 2

This column displays the network address of one of the participants in a network session.

Network Address

Identifies the network address from which frames were captured. To sort this column, double-click on the column head.

Frames Sent

Identifies the number of frames sent from the address listed in the Network Address column.

Bytes Sent

Identifies the number of bytes sent by the address listed in the Network Address column.

Bytes Received

Identifies the number of bytes received by the address listed in the Network Address column.

Directed Frames Sent

Identifies the number of non-broadcast and non-multicast frames transferred over the network from the associated address.

Multicasts Sent

Identifies the number of times the address listed in the Network Address column has sent frames to a subset of computers on the network.

Broadcasts Sent

Identifies the number of times the address listed in the Network Address column has sent frames to all the computers on the network.

Network Statistics

Displays the total amount of traffic that has occurred on the network since the current capture began. These statistics include:

- The total number of frames sent over the network.
- The total number of broadcasts sent to the network.
- The total number of multicasts sent to the network.
- The total number of bytes sent to the network.
- The total number of frames dropped.
- The Network Status. On an EtherNet network, this entry will always be Normal. On a Token Ring network, this entry reflects the status of the ring.

Capture Statistics

Displays total statistics on the current capture. The statistics include:

- The total number of frames captured.
- The total number of frames in the capture buffer.
- The total number of bytes captured.
- The total number of bytes in the buffer.
- The percentage of allotted buffer space that is in use.
- The number of frames dropped by Network Monitor.

Per Second Statistics

Displays statistical averages of current activity and continually updates this average to reflect current per-second activity. The statistics in this panel include all frames, including frames that were excluded by a capture filter. The following are components of the Per Second Statistics panel:

- The average frames per second detected since capturing began.
- The average bytes per second detected since capturing began.
- The average broadcast messages per second detected since capturing began.
- The average multicast messages per second detected since capturing began.
- The percentage of network utilization. This statistic is based on an average of the percentage of network utilization since capturing began.
- These statistics are not supported on all network adapter cards. If a statistic is unsupported for your network adapter card, the statistic label is replaced with Unsupported.

Network Card (MAC) Statistics

The Network Card (MAC) statistics reflect the average activity detected by your network adapter card since the beginning of the current capture. The statistics in this pane reflect all the network activity that your network adapter card is able to receive, including:

- The total number of frames detected by the network adapter card.
- The total number of broadcast frames detected by the network adapter card.
- The total number of multicast frames detected by the network adapter card.
- The total number of bytes detected by the network adapter card.
- These statistics are not supported on all network adapter cards. If a statistic is unsupported for you network adapter card, the statistic label is replaced with Unsupported.

The Network Card (MAC) Error Statistics Panel

The Network Card (MAC) error statistics reflect errors that have occurred in relation to your network adapter card since the capture began, including:

- The number of errors that occurred because the cyclical redundancy check (CRC) did not match the actual bytes received.
- The number of frames detected by the network card but dropped because you lack buffer space.
- The number of frames detected by the network card but dropped because of hardware constraints.

Frame Number

Displays the number of the frame, beginning with 1, in the order in which it was captured.

Time

The time at which the frame was captured. This column can display one of three possible values, depending on the display options that you specify.

- The absolute system time at which the frame was captured
- The time that the frame was captured in relation to the beginning of the capture. This value is expressed in milliseconds
- The time that the frame was captured in relation to the capture of the frame that precedes it. This value is specified in milliseconds.

SRC MAC Address

The network address of the computer that sent the frame.

Dst MAC Address

The network address of the computer to which the frame was sent.

Protocol

The protocol that was used to send the frame.

Description

A brief description of the frame's contents.

Frame

Displays the base frame properties for the selected frame. These include:
- The date and time at which the frame was captured
- The time (in milliseconds) that elapsed between the capture of the current frame and the capture of the frame that precedes it
- The frame's number in the sequence of total frames captured
- The length of the frame in bytes
- The amount of the frame that was captured

The number of bytes remaining. For the Frame field, this number usually equals the total number of bytes in the frame.

Protocol

The protocol section of the Detail pane consists of all information below the end of the Frame section. The length of the section varies, depending on the number of protocols that were used to send the frame. The protocols are displayed from the lowest-level protocol to the highest.

- As you select a line in this pane, the raw representation of this line, displayed in the Hex pane, is automatically selected.

Frames Rcvd

Identifies the number of frames received by the address listed in the Network Address column.

Network Information Dialog Box

This dialog box displays information about your current network configuration. Use this dialog:
- To find information on this configuration
- To connect to an instance of the Network Monitoring Agent on a remote computer
- To specify the network onto which you want to transmit frames

This dialog box contains the following options:
- Number
- Node Name
- Connect State
- Type
- Current Address
- Card Description
- Link Speed
- Permanent Address
- Connect
- Disconnect
- Suspend

Net number

The number of the network connection.

Node name

The name of the network connection. Usually, this is LOCAL or REMOTE. If you are connected to the Network Monitoring Agent on a remote computer, this column displays the name of the agent on the remote computer.

Connect State

Displays the state of the network connection. These are Connected or Disconnected.

Type

Displays the type of network (for example, Ethernet) to which you are connected.

Link Speed

The bits per second (bps) that you can transfer over the network.

Permanent Address

The address of your network adapter card. This is the address assigned by the card's manufacturer.

Current Address

The current address of your network adapter card. Unless the permanent address of the card has been overridden, this listing is identical to the address in the Permanent Address column.

Welcome to Network Monitor Dialog Box

Use this dialog box to enter the password that gives you access to Network Monitor.

If you do not know your password, see your administrator or the person who installed Network Monitor.

Connect

Click this to display the Connect to Network Monitoring Agent dialog box, which you can use to connect to the Network Monitor agent on a remote Windows NT workstation.

- If you are already connected to the Network Monitor Agent on a remote workstation, this button does not appear.

Suspend

If you are connected to the Network Monitor Agent on a remote Windows NT workstation, you can use this button to suspend the connection. You cannot suspend a connection until you have started capturing on the remote site. If you are connected to the Agent over an expensive line (for example, a modem link to a long-distance site) or an unreliable connection, you should select this option as soon as you begin capturing on the remote site. This ensures that if the connection is lost, the remote agent continues to capture.

No network drivers found

This message appears under the following circumstances:
- An error occurred in setup. Rerun setup.
- Network software has not yet been installed on your system. Install this software, and then rerun setup.
- You installed Network Monitor on a Windows NT workstation, but were not logged on as an administrator. Log on under your administrative account.

X

Use this column to specify the protocols to which the current color selection will apply. Click in the column next to a protocol, and an X appears next to the protocol name.

Src Other Addr

Displays the IP or IPX/XNS address associated with the address displayed in the Src MAC Addr column.

Dst Other Addr

Displays the IP or IP/XNS address associated with the address displayed in the Src MAC Addr column.

Type Other Addr

Displays the address type of the addresses displayed in the Src Other Addr and Dst Other Addr columns.

Card Description

Displays the descriptive comment that a user has associated with the network adapter card on the remote system. To associate such a comment with the card on your system, use the Network Monitoring Agent in the Control Panel.

Not

When you add a NOT expression to the decision tree, all expressions in the branch beneath the expression are excluded from the filter.

Disconnect

Click this to disconnect from the Network Monitor Agent.

- If you are not connected to an instance of the Network Monitor Agent, this button does not appear.

Label Window Dialog Box

Use the Label Window dialog box to change the default text that appears in the title bar of a Frame Viewer window.

In the Description box, type the window's new label.

Network Monitor Guide to Books on Networking

Black, Uyless D. *Computer networks: protocols, standards, and interfaces.* Englewood Cliffs, NJ: Prentice Hall, 1987.

Black, Uyless D. *Data link protocols.* Englewood Cliffs, N.J. : PTR Prentice Hall, 1993.

Comer, Douglas *Internetworking with TCP/IP Vol I-III.* Englewood Cliffs, NJ: Prentice Hall, 1991.

Davies, Donald Watts., Barber, D.L.A., Price, W.L., and Solomonides, C.M. *Computer networks and their protocols.* Chichester, UK; New York: John Wiley & Sons, 1979.

Edwards, T. C. *Fiber-optic Systems: Network Applications.* Chichester, West Sussex England, New York: Wiley, 1989.

Hailpern, Brent., and Owicki, Susan S. *Verifying network protocols using temporal logic.* Stanford, CA: Stanford University, 1980.

Haugdahl, Scott J. *Inside NetBIOS 3rd Edition.* Minneapolis, MN: Architecture Technology Corporation, 1990.

Held, Gilbert. *Internetworking LANs and WANs : concepts, techniques, and methods.* Chichester; New York : Wiley, 1993.

Holzmann, Gerard J., and American Telephone and Telegraph. *Design and Validation of Computer Protocols.* Englewood Cliffs, NJ: Prentice Hall, 1991.

Holzmann, Gerard J. "*The analysis of message passing systems: An algebra for protocol validation.*" A Report for Bell Telephone Laboratories, Inc. Murray Hill: Bell Laboratories, 1981.

Hordeski, Michael F. *Microcomputer LANS: network design and implementation.* Blue Ridge Summit, PA: Tab Professional and Reference Books, 1987.

Hunt, Craig. *TCP/IP network administration.* Sebastopol, CA: Oreilly & Associates, NC, 1992.

Kumar, Akhil., Rabinovich, Michael., and Sinha, Rakesh K. "*A performance study of a new grid protocol and general grid structures for replicated data.*" Report for the University of Washington. Department of Computer Science and Engineering. Seattle, WA: University of Washington. Department of Computer Science and Engineering, 1993.

Ladner, Richard., LaMarca, Anthony., and Tempero, Ewan. "*Counting protocols for reliable end-to-end transmission.*" Report for the University of Washington. Department of Computer Science and Engineering. Seattle, WA: University of Washington. Department of Computer Science and Engineering, 1992.

Lindgren, Bo. *Illustrated ISDN : a painless primer to principles and protocols.* Kalmar, Sweden: INFOTRANS, 1989.

Martin, James. *Local Area Networks: Architectures and Implementations.* Englewood Cliffs, NJ: Prentice Hall, 1989.

Miller, Mark. *LAN Protocol Handbook*. Redwood City, CA: M&T Publishing, 1990.

Miller, Mark. *LAN Troubleshooting Handbook.* San Mateo, CA: M&T Books, 1989.

Miller, Mark. *Troubleshooting TCP/IP*. San Mateo, CA: M&T Books, 1992.

Nance, Barry. *Introduction to networking.* Carmel, IN : Que Corp., 1992.

Poltrock, Steven E., and Nasr, Maria G. "*Protocol Analysis: a tool for analyzing human-computer interactions.*" Report for Microelectronic & Computer Technology Research Corporation. Austin, TX: MCC, 1989.

Quarterman, John S. *Network substrata : a survey of common higher level network protocols.* Santa Clara, CA ; UniForum, 1990.

Schatt, Stanley. *Understanding network management: strategies and solutions.* Blue Ridge Summit, PA: Windcrest/McGraw-Hill, 1993.

Schwaderer, David W. *C Programmer's Guide to NetBIOS.* Carmel, IN: Howard W. Sams & Co., 1988.

Schwartz, Mischa. *Telecommunication networks : protocols, modeling, and analysis.* Reading, MA : Addison-Wesley Pub. Co, 1988.

Sidhu, Gursharan S., Andrews, Richard F., Oppenheimer, Alan B., and Apple Computers, Inc. *Inside AppleTalk,*

Second Edition.   Reading, MA : Addison-Wesley Publishing Company, Inc., 1990.

Spragins, John D., Hammond, Joseph L., and Pawlikowski, Krzysztof.   *Telecommunications: protocols and design.*   Reading, MA : Addison-Wesley Pub. Co., 1991.

Tanenbaum.   *Computer Networks.*   Englewood Cliffs, NJ: Prentice Hall, 1989.

Thekkath, Chandramohan A., Voelker, Geoff., and Wolman, Alec.   "*Implementing network protocols at user level.*"   A Report for the University of Washington. Department of Computer Science and Engineering.   Seattle, WA: University of Washington.   Department of Computer Science and Engineering, 1993.

Tobagi, Fouad A.   "*Carrier Sense Multiple Access with Message-based Priority Functions.*"   Report prepared for the Stanford University Computer Systems Laboratory. Stanford University, 1980.

VanderSluis, Kurt., and Amr, Eissa.   *Troubleshooting Macintosh Networks.*   New York, NY : M&T Books, 1993.

Wolman, Alec., Thekkath, Chandramohan A., and Voelker, Geoff.   "*Latency analysis of TCP on an ATM network.*"   Report for the University of Washington, Department of Computer Sciences and Engineering.   Seattle, WA: University of Washington. Department of Computer Science and Engineering, 1993.

Zeines, Ben.   *Introduction to network analysis.*   Englewood Cliffs, NJ: Prentice Hall, 1967.

Network Monitor Guide to Reports on Networking

Atwood, Michael E., and Jeffries, Robin. "*Studies in Plan Construction I: Analysis of an Extended Protocol.*" Report for Science Applications, Inc. Englewood, CO: Science Applications, Inc., 1980.

Holzmann, Gerard J. "*The analysis of message passing systems: An algebra for protocol validation.*" A Report for Bell Telephone Laboratories, Inc. Murray Hill: Bell Laboratories, 1981.

Kumar, Akhil., Rabinovich, Michael., and Sinha, Rakesh K. "*A performance study of a new grid protocol and general grid structures for replicated data.*" Report for the University of Washington. Department of Computer Science and Engineering. Seattle, WA: University of Washington. Department of Computer Science and Engineering, 1993.

Ladner, Richard., LaMarca, Anthony., and Tempero, Ewan. "*Counting protocols for reliable end-to-end transmission.*" Report for the University of Washington. Department of Computer Science and Engineering. Seattle, WA: University of Washington. Department of Computer Science and Engineering, 1992.

Poltrock, Steven E., and Nasr, Maria G. "*Protocol Analysis: a tool for analyzing human-computer interactions.*" Report for Microelectronic & Computer Technology Research Corporation. Austin, TX: MCC, 1989.

Thekkath, Chandramohan A., Voelker, Geoff., and Wolman, Alec. "*Implementing network protocols at user level.*" A Report for the University of Washington. Department of Computer Science and Engineering. Seattle, WA: University of Washington. Department of Computer Science and Engineering, 1993.

Tobagi, Fouad A. "*Carrier Sense Multiple Access with Message-based Priority Functions.*" Report prepared for the Stanford University Computer Systems Laboratory. Stanford University, 1980.

Wolman, Alec., Thekkath, Chandramohan A., and Voelker, Geoff. "*Latency analysis of TCP on an ATM network.*" Report for the University of Washington, Department of Computer Sciences and Engineering. Seattle, WA: University of Washington. Department of Computer Science and Engineering, 1993.

Microsoft Product Support Services

The core functionality of Network Monitor, described in Help, is supported by Microsoft Product Support Services. Network-dependent tasks, such as interpreting data that you capture from your network, are not supported.

The Network Monitor Agent is supported for Windows NT, but is unsupported on Windows 3.1 and Windows for Workgroups workstations.

Microsoft Network Monitor Help

Network Monitor is a component of Microsoft Systems Management Server (SMS) that enables you to detect and troubleshoot problems on LANs or on WANs running the Microsoft Remote Access Service (RAS). Network Monitor monitors the network *data stream*, which consists of all of the information transferred over a network at any given time.

Find Network Addresses From Name Dialog Box

This dialog box enables you to resolve network addresses (IP, IPX, Ethernet, token ring, or FDDI) for a specific computer name. You can also specify an address to resolve its registered friendly name.

This dialog box contains the following options:
- Name
- Local Machine Information
- Run Query
- Name
- Aliases
- Options
- Keep Names
- Addresses
- Edit Addresses

Name

Type the computer name whose network address you want to find.

Or, type an IP or IPX address to find its computer name.

Local Machine Information

Retrieves local network addresses for the computer on which you currently are running Network Monitor.

Network Monitor will try to detect your IP, IPX, and MAC addresses by querying the WinSock and NetBIOS services.

Run Query

Retrieves network addresses that belong to the computer name specified by <u>Name</u>.

Name

Displays the computer name for the computer name or network address specified in the first <u>Name</u> box.

Aliases

Displays any aliases for the computer name or network address specified in the first <u>Name</u> box.

Options

Opens the Options dialog box, where you can specify how to search for network addresses or a computer name.

Keep Names

Adds the found address (or updates the existing address with the new address information) to the local address database.

Addresses

Displays the network address(es) for the computer specified in the first <u>Name</u> box.

Select an address in this list to edit its name and comment for the local address database.

Edit Addresses

Opens the Address Information dialog box, where you can edit the selected computer name.

Options Dialog Box

This dialog box enables you to specify how to retrieve network addresses or a computer name. You can select which services to search and the order that services will be queried.

You can enable or disable services by selecting a service name in a list box and using the arrow buttons to move the service name. Or, you can double-click the service name.

Use the '+' and '-' buttons to promote/demote service names in a list box, in order to affect the order in which the services will be queried in a search.

The following services can be used to search for network addresses and computer names:

DNS (Domain Name Server)

Local ADR (address) Database

NetBIOS

SAP (Service Advertising Protocol)

SMS (Server Management System) Remote Database

Find Network Routers Dialog Box

The Find Network Routers dialog box enables you to determine which network addresses represent routers on your network. Network Monitor looks for devices that have a single FDDI or media access control (MAC) address but multiple protocol addresses if the network supports multiple protocols, and for the OSPF protocol, which specifically identifies routers.

This dialog box contains the following options:
- Test Protocols
- Minimum Duplicate Addresses
- Capture Buffer Size

Test Protocols

Select the protocols for which you want to search for routers:

{button ,PI(`',`IDC_ROUTER_TEST_SAP')}   SAP

{button ,PI(`',`IDC_ROUTER_TEST_BROWSER')}   BROWSER

{button ,PI(`',`IDC_ROUTER_TEST_RIPX')}   RIPX

{button ,PI(`',`IDC_ROUTER_TEST_IP')}   IP

{button ,PI(`',`IDC_ROUTER_TEST_OSPF')} OSPF

{button ,PI(`',`IDC_ROUTER_TEST_RIP')}   RIP

When you click OK, the dialog will disappear and the Capturing Router Data or Processing Capture dialog box will display (depending on the current state). The progress indicators display on top of this dialog box.

If no capture exists in the Network Monitor window, a new capture is started. This capture will stop when the buffer is full, or when you click Proceed to Search Capture.

SAP

The NetWare Service Advertising Protocol.

At regular intervals, individual devices (including printers and PCs) will broadcast a General Service Response frame. In the response, the device describes 'services' available through that address. For a printer or a PC, there is only one service available. A router will report a larger number of services.

Find Network Routers keeps track of the number of services available through a given network address. Addresses with more than one service are reported.

BROWSER

Microsoft advertising protocol.

Devices broadcast BROWSER host announcements, which contain the device's name. Depending on the network configuration, the broadcasts will include NetBIOS, IPX, and IP frames. The IPX and IP frames will have their own address types, but all three will have the same service name and MAC address. Routers re-broadcast the announcements, without altering the name and IP or IPX address.

Find Network Routers monitors BROWSER announcements and stores the names associated with a physical address. Routers will usually have a large number of names associated in this way.

RIPX

NetWare's Routing Information Protocol.

A RIPX response frame contains a list of 'networks enumerated'; each network has a number.

Find Network Routers records the network numbers at each physical address.

IP

The Internet Protocol.

Find Network Routers keeps track of IP addresses and physical addresses. Routers will have more than one IP address.

Note that Ethernet 'multihome cards' can have **two** IP addresses, but only one physical address. Set the Minimum Duplicate Addresses option to eliminate multihome devices.

OSPF

The Open Shortest Path First TCP/IP Internet routing protocol.

Find Network Routers looks for OSPF 'Hello' messages, used to start communication between routers. Only routers use these OSPF messages.

RIP

The Internet Routing Information Protocol.

If Find Network Routers detects any RIP response frame, the device may be a router. Some networks are not configured to emit RIP response frames.

Minimum Duplicate Addresses

Specifies the minimum number of protocol addresses (or names in the case of BROWSER) per physical address. This number is used in all the protocol tests except RIP and OSPF.

Default value is 3, which eliminates multihome Ethernet cards. If you want to detect multihome cards, set this value to 2. (Multihome cards are **not** routers.)

Capture Buffer Size

Type the size of the capture buffer, in megabytes. (This setting is not available when you access the Find Network Routers dialog box from the Network Monitor Display window.) Default value is 2 MB.

A larger buffer size takes longer, but will be more likely to detect routers.

Certain test methods (SAP and BROWSER) are faster than others, usually requiring a smaller capture.

IP tests can be slow and should be run separately from other protocols. An IP-only capture will discard any frames that are not IP, and so have greater likelihood (for a given buffer size) of recognizing routers through this test.

Network Routers (*number* Found) Dialog Box

After a search for routers ends, the Network Routers dialog box displays the routers identified.

Each row of the list box contains a name, a physical address, and will have an entry under at least one of the test protocols.

- <u>Name</u>
- <u>Edit</u>
- <u>Delete</u>
- <u>Show Info</u>

Name

Displays the name Network Monitor assigned to the identified router (unless an existing name was marked as Permanent in the Address Edit dialog box), the name is formed from "Router" and the last six characters of the physical address.

Edit

Opens the Address Information dialog box, where you can edit the selected computer name and set the name as Permanent.

Delete

Removes the selected router from the list. If a listed computer is **not** a router, delete it from the list so that it is not added to the address database as such.

Show Info

Opens the Supplemental Router Information dialog box, which displays additional information about the selected router. This information will help you determine whether the specified computer is actually a router.

Permanent Name

Use the Permanent Name check box to use the text in the Name box as the computer's name in the local address database.

Supplemental Router Information Dialog Box

The Supplemental Router Information dialog box displays information about the selected router.

For the OSPF or RIP protocols, the existence of response frames is sufficient to recognize a computer as a router.

For the other protocols, information is accumulated:
- The IP test keeps track of all the IP addresses originating at one MAC address.
- The SAP test accumulates Service Names.
- The RIPX test has network numbers.
- BROWSER has name-address pairs.

The Supplemental Router Information dialog box displays this additional information to help you decide a router has been correctly identified.

You might also want to see what IP addresses were using the same MAC address, or the router ID assigned to an OSPF router.

This dialog box is not available when there is no supplemental information. This occurs only if a RIP identification is the only protocol for a listed router. If a protocol didn't trigger identification, that radio button will be disabled.

Protocol Distribution Dialog Box

The Protocol Distribution dialog box allows you to list information on the protocols gathered in a capture. Network Monitor displays how many frames each protocol was found in, how many bytes each protocol consumed, and the percentages for each. This enables you to determine how the network is being used, and what protocols on the network are consuming the most bandwidth.

This dialog box contains the following options:

Base List Upon

Select a method for compiling the protocol distribution list:
- Last Protocol in Frame
- First Effective Protocol in Frame
- All Protocols in Frame

Apply Current Display Filter

Select this check box to use the current display filter when calculating the protocol distribution.

If you do not select this option, the output will show data for all the frames in the capture, including those that have been filtered from the display.

Last Protocol in Frame

Collects data only for those protocols that were last in each frame. The last protocol in a frame claims the bytes for all protocols in the entire frame.

Use this option to determine where the frames in a capture are ending up, rather than the mechanism used to get them there.

First Effective Protocol in Frame

Collects data for only the first effective protocol in each frame. The first protocol in a frame claims the bytes for all protocols in the entire frame.

The first effective protocol is determined to be the protocol following SNAP or LLC (if there are any), or the last protocol found.

This option is useful for determining how frames get around on the network and for comparing IPX and IP percentages.

All Protocols in Frame

Collects data for each protocol in each frame. Each protocol in a frame is assigned the bytes it actually uses. For example, if IP hands off to TCP, which hands off NBT, all three protocols will get their byte counters incremented for that frame.

This option will list of all the protocols in a capture, how many bytes they consumed, and how many frames they were found in. Total Percentages will exceed 100% in this case, as the Frames and %Frames indicates how many frames this protocol was found in.

Protocol Distribution Report Dialog Box

The Protocol Distribution Report dialog box lists the information on the protocols gathered from the capture. It shows a breakdown of the protocols found (using the option specified in Base List Upon in the Protocol Distribution dialog box), how many frames each protocol was found in, how many bytes each protocol claimed, and percentages of each.

Find Top Users Dialog Box

The Find Top Users dialog box displays a list of the top users of the network in a capture to help you determine which users are causing the most network traffic, or where the network traffic is going.

Network Monitor searches each frame of a capture for the source and destination addresses, and it keeps a list of all the addresses, how many frames they appeared in, and how many bytes. Network Monitor displays the top senders and the top recipients of frames in the Top Users dialog box.

This dialog box contains the following options:

Amount of Users to Display

This value determines how many addresses to show in the report. Default value is 10. The maximum is 4095.

Base List Upon

Select a method for compiling the list of top users:
- Link Layer Addresses
- Mac Addresses

Apply Current Display Filter to List

Select this check box to use the current display filter when calculating the top users. If you do not select this is check box, the report will be based upon all the frames in the capture, including those that have been filtered from the display.

Link Layer Addresses

Select this option to base the list of top users upon the non-MAC addresses (such as IP, VINES_IP, IPX, and XNS) found in each frame—but MAC addresses will be used for frames with no non-MAC addresses. Use this option to show the actual top users (rather than routers).

Mac Addresses

Select this option to base the list on the MAC addresses of each frame. Note that if a frame crosses a router, the MAC address may be from the router rather than from the originator of the packet.

Top Users Dialog Box

The Top Users dialog box displays a list of the top senders and recipients based upon the source and destination addresses of each frame. It shows the amount of frames, bytes, and percentages of each address which was a source, along with similar information for the top destinations found in the capture.

This dialog box helps you determine who is using the network, or from which station a problem such as a broadcast storm may be coming.

Insert Comment Frame Dialog Box

The Insert Comment Frame dialog box allows you to insert a frame into a capture. With a comment frame, you can place comments and other information into a capture. The comment frame contains the Trail protocol, which includes statistics such as amount of frames and bandwidth consumed. These statistics are based on a block of frames bounded by the current comment frame and the next comment frame of the same type (or the end of the capture).

This dialog box contains the following options:

Frame Number

Specifies where to insert the comment frame in the capture. The inserted frame will be placed just before the frame number listed, and will push all the other frames down by one.

The maximum value is one more than the number of the last frame in the capture (up to 4095).

Enter in a Comment for this New Frame

The text you type in this box will be attached to the frame (using the protocol specified in the Type of Frame to Insert box).

Type of Frame To Insert

Specifies which parser will process the frame after the Trail protocol.

If you modify the \NETMON\PARSERS\TRAIL.INI file and map a parser to an integer, you can type that number in this field.

No Statistics

Select this check box to disable the generation of statistics for this comment frame. If you select this option, this frame will not be used to define a block for any other inserted comment frames (for statistics).

Apply Current Filter to Statistics

Select this check box to use the current display filter when calculating statistics.

If you do not select this option, the output will show data for all the frames in the capture, including those that have been filtered from the display.

To resolve network addresses

1. From the Tools menu, choose Resolve Addresses From Name.

   Or, right-click on an address in the Display window and choose Resolve Address *address*.

   The Find Network Addresses From Name dialog box appears.

2. In the Name box, type the computer name whose network address you want to find, or an IP/IPX address to find its computer name.

   The text you type is not case-sensitive, and it does not support wildcards.

3. Choose Run Query.

   Network Monitor retrieves the network address for the specified computer.

4. Choose Local Machine to obtain this data for the local computer.

5. Choose Options to specify how Network Monitor searches for network addresses or a computer name.

   You can select what services to include in the search, and the order in which they are to be queried.

6. Choose Keep Names to add the found address (or update an existing address with the new address information) to the local address database.

7. Choose Done when you have finished finding network addresses for computer names.

To find network routers

1. From the Tools menu, choose Find Routers.

   The Find Network Routers dialog box appears.

2. Make the following settings:

   Test Protocols

   Select the protocols for which you want to search for routers.

   Minimum Duplicate Addresses

   Type the number to be used in protocol tests. This number is used in all the protocol tests except RIP and OSPF.

   Capture Buffer Size

   Type the size of the capture buffer, in megabytes. (This setting is not available when you access the dialog box from the Network Monitor Display window.)

3. Choose OK to begin looking for network routers.

   The Capturing Router Data dialog box appears. Progress indicators appear on top of this dialog box.

   If no capture exists in the Network Monitor window, a new capture is started. This capture will stop when the buffer is full, or when you choose Proceed to Search Capture.

   After the capture terminates, Network Monitor examines the capture. When this search is complete, the Network Routers dialog box appears.

4. Use Edit and Delete to update the displayed routers.

   Choose Show Info to see supplemental information for the selected router.

5. Choose OK to add the displayed routers in the global address database.

To display protocol distribution

1. In the Network Monitor Display window, from the Tools menu, choose Protocol Distribution.

   The Protocol Distribution dialog box appears.

2. Select how you want to compile the protocol distribution list.

   Last Protocol in Frame

   Collects data only for those protocols that were last in each frame. The last protocol in a frame claims the bytes for all protocols in the entire frame.

   First Effective Protocol in Frame

   Collects data only the first effective protocol in each frame. The first protocol in a frame claims the bytes for all protocols in the entire frame.

   The first effective protocol is determined to be the protocol following SNAP or LLC (if there are any), or the last protocol found.

   This option is useful for determining how frames get around on the network and for comparing IPX and IP percentages.

   All Protocols in Frame

   Collects data for each protocol in each frame. Each protocol in a frame is assigned the bytes it actually uses.

   For example, if IP hands off to TCP, which hands off NBT, all three protocols will get their byte counters incremented for that frame.

3. Select the Apply Current Display Filter check box to use the current display filter when calculating the protocol distribution.

   If you do not select this option, the output will show data for all the frames in the capture, including those that have been filtered from the display.

4. Choose OK to create the report.

   The Protocol Distribution Report dialog box appears.

5. Choose OK when you are finished reviewing the report.

To find top users on the network

1. In the Network Monitor Display window, from the Tools menu, choose Find Top Users.

   The Find Top Users dialog box appears.

2. In the Amount of Users to Display box, type the number of top users you want Network Monitor to report.

3. Select how you want to compile the list of top users.

   Link Layer Addresses

   Bases the list on non-MAC addresses (such as IP, VINES_IP, IPX, and XNS) found in each frame — but MAC addresses will be used for frames with no non-MAC addresses. Use this option to show the actual top users (rather than routers).

   Mac Addresses

   Bases the list on the MAC addresses of each frame. Note that if a frame crosses a router, the MAC address may be from the router rather than from the originator of the packet.

4. Select the Apply Current Display Filter check box to use the current display filter when calculating the top users.

   If you do not select this option, the output will show data for all the frames in the capture, including those that have been filtered from the display.

5. Choose OK to create the report.

   Network Monitor calculates the top users and displays them in the TOP USERS dialog box.

6. Choose OK when you are finished reviewing the report.

To add a comment frame to a capture

1. In the Network Monitor Display window, from the Tools menu, choose Insert Comment Frame.

   You can also right-click on the frame, in the Frame Number column, where you want to insert a comment frame, and click Insert Comment on the pop-up menu.

   The Insert Comment Frame dialog box appears.

2. Type your comment in the Enter In A Comment For This New Frame box.

3. Select the Type of Frame to Insert to determine which parser will process the frame after the Trail protocol.

   If you modify the \NETMON\PARSERS\TRAIL.INI file and map a parser to an integer, you can type that number in this field.

4. Select the No Statistics check box if you want to disable the generation of statistics for this comment frame, and this comment frame will not be used to define a block for any other inserted comment frames.

5. Select the Apply Current Filter to Statistics check box to use the current display filter when calculating statistics.

   If you do not select this option, the output will show data for all the frames in the capture, including those that have been filtered from the display.

6. Choose OK to add the frame to the capture.