



DeviceNet Network Analyzer

User Guide

Document Edition: 2.0

Document #: 717-0025

Document Edition: 2.0

Date: August 7, 2007

This document applies to the DeviceNet Network Analyzer software application.

Copyright ©2007 Woodhead Software & Electronics, Division of Woodhead Canada Limited

This document and its contents are the proprietary and confidential property of Woodhead Industries Inc. and/or its subsidiaries and may not be used or disclosed to others without the express prior written consent of Woodhead Industries Inc. and/or its subsidiaries.

SST is a trademark of Woodhead Software & Electronics. All other trade names are trademarks or registered trademarks of their respective companies.

At Woodhead, we strive to ensure accuracy in our documentation. However, due to rapidly evolving products, software or hardware changes occasionally may not be reflected in our documents. If you notice any inaccuracies, please contact us (see Appendix A of this document).

**Written and designed at Woodhead Software & Electronics, 50 Northland Road,
Waterloo, Ontario, Canada N2V 1N3.**

Hardcopies are not controlled.

Contents

Preface	v
Purpose of this Guide	vi
Conventions	vi
Style.....	vi
Terminology	vii
Special Notation	vii
 Overview	 9
1.1 Main Features	10
1.2 Guidelines for Use	11
1.3 System Requirements	12
1.3.1 Software License	12
 Working Environment	 13
2.1 General Overview	14
2.2 Menu Bar and Toolbar	17
 Using the Network Analyzer	 21
3.1 Specifying the Card Name and Network Baud Rate	22
3.2 Using Message Filters	24
3.2.1 Filtering Based on Specific Messages.....	25
3.2.2 Filtering Based on Mask/Match Criteria.....	27
3.2.3 Loading and Saving Filter Profiles.....	30
3.3 Using the Trigger Filter	31
3.4 Using the Capture Filter	32

3.4.1 Defining the Capture Filter	32
3.4.2 Toggling the Capture Filter	32
3.5 Capturing Network Data.....	33
3.5.1 Toggling Between Hexadecimal and Decimal.....	34
3.5.2 Setting the Display Mode to CAN	34
3.5.3 Setting the Display Mode to DeviceNet.....	34
3.6 Using the View Filter	35
3.6.1 Defining the View Filter	35
3.6.2 Toggling the View Filter	35
3.6.3 Removing Messages from the View Filter.....	36
3.7 Finding a Message in the View	37
3.7.1 Finding a Specific Message.....	37
3.7.2 Finding the Trigger Point.....	38
3.8 Saving and Exporting Captured Messages	39
3.8.1 Saving to a Capture File.....	40
3.8.2 Saving the View to a Capture File	40
3.8.3 Exporting the View to a Text File.....	41
Troubleshooting.....	45
4.1 Required Software Components.....	46
Warranty and Support.....	47
A.1 Warranty	48
A.2 Technical Support.....	48
A.2.1 Getting Help	49
Index.....	51

Preface

Preface Sections:

- Purpose of this Guide
- Conventions

Purpose of this Guide

This guide contains technical and product-related information on the DeviceNet Network Analyzer software application.

The DeviceNet Network Analyzer captures individual CAN messages on a CAN or DeviceNet network and allows them to be viewed and analyzed.

Conventions

This guide uses stylistic conventions, special terms, and special notation to help enhance your understanding.

Style

The following stylistic conventions are used throughout this guide:

Bold	indicates field names, button names, tab names, executable files, command names, and options or selections
<i>Italics</i>	indicates keywords (indexed) or instances of new terms and/or specialized words that need emphasis
CAPS	indicates a specific key selection, such as ENTER, TAB, CTRL, ALT, DELETE
Code Font	indicates command line entries or text that you'd type into a field
<u>Underlining</u>	indicates a hyperlink
“>” delimiter	indicates how to navigate through a hierarchy of menu selections/options
“0x”	indicates a hexadecimal value

Terminology

The following special terms are used throughout this guide:

Console The software tool used to configure the DeviceNet network for a Woodhead DeviceNet interface card.

Network Analyzer The DeviceNet Network Analyzer software application.

Special Notation

The following special notations are used throughout this guide:



Note

A note provides additional information, emphasizes a point, or gives a tip for easier operation. Notes are accompanied by the symbol shown, and follow the text to which they refer.

1

Overview

Chapter Sections:

- Main Features
- Guidelines for Use
- System Requirements

1.1 Main Features

The Network Analyzer is used with a Woodhead DeviceNet interface card to capture network activity. It can perform the following functions:

- Captures individual CAN messages on a CAN or DeviceNet network using the 11-bit identifier, as defined in the CAN specification, version 2.0, part A.



Note

The capturing of Remote Frames is not supported.

- Allows you to define a Trigger Filter to specify when the capture should begin, based on specific messages, communications between a client and server, or mask/match criteria. The filter will trigger when these criteria are met or not met for a certain period of time.
- Allows you to define the number of messages to capture prior to the trigger point, and the number of messages or time to capture following it.
- Allows you to define a Capture Filter to specify what should be captured, based on specific messages, communications between a client and server, or mask/match criteria.
- Allows captured messages to be displayed and analyzed.
- Displays the timestamp, MAC ID, message group, message ID, data values, and a description of the message type associated with a DeviceNet message.
- Allows the captured messages to be post-filtered, based on specific messages, communications between a client and server, or mask/match criteria.
- Allows you to search for a specific message in the list of captured messages.
- Saves the captured messages to a capture file, or a comma-delimited or fixed-column-width text file.
- Can capture up to 100 million messages over a period of up to 46 days.

1.2 Guidelines for Use

The Network Analyzer performs two main functions:

- Captures CAN messages on a CAN/DeviceNet network based on filtering criteria and a trigger point (both of which are optional).
- Displays captured network messages and allows them to be filtered.

Using the Network Analyzer typically involves the following sequence of events:

1. Select the name of the card and the network baud rate to be used for the capture.
2. Create a Trigger Filter to define the trigger point (if one will be used during the capture).
3. Specify the Capture Filter (optional).
4. Start the capture, using one of the available methods.
5. Stop the capture (or wait until the capture terminates, if using the trigger point).
6. View the CAN messages in the list of captured messages.
7. Filter the displayed messages to further refine them.
8. Save the filtered list to a file.

1.3 System Requirements

The Network Analyzer is designed to work with the DN3 family of interface cards. It is used in conjunction with the hardware driver DLL and an application module that provides basic access to the CAN network.



Note

When used within the Network Analyzer, capture files should always be located on the hard drive. Avoid opening capture files that are stored on removable media, as performance may be impaired. Do not open capture files that are stored on floppy disks.

1.3.1 Software License

The Network Analyzer is licensed through the use of a hardware key (dongle). The key should be attached to the USB or parallel port of the computer. If you receive a message saying that no dongle was detected on the port, or that the dongle is not licensed, check that you have a dongle connected to the computer and that it is licensed for use with the DeviceNet Network Analyzer.

2

Working Environment

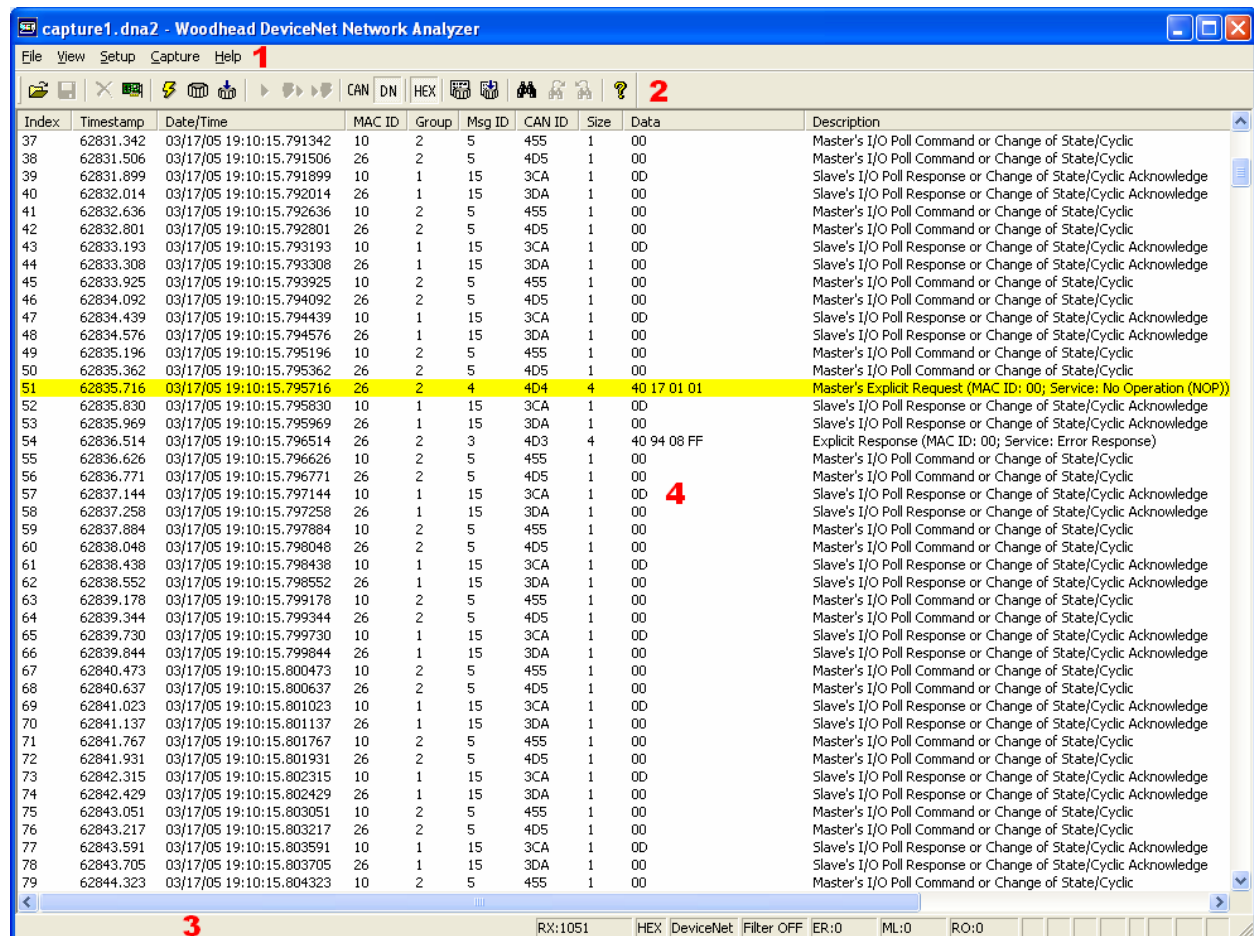
Chapter Sections:

- General Overview
- Menu Bar and Toolbar

2.1 General Overview

The Network Analyzer working environment is a stand-alone application, consisting of a user interface containing four different regions, as indicated below.

Figure 2.1-1: Network Analyzer Working Environment



Region 1: Menu Bar

The Menu Bar contains all of the Network Analyzer commands. When a command is highlighted, a brief description is displayed.

Region 2: Toolbar

The Toolbar contains iconic representations of many Network Analyzer commands. When the mouse is on top of an icon, a brief description of the command is displayed.

Region 3: Status Bar

The Status Bar displays the description of any Menu or Toolbar item that the mouse is on top of, as well as numerous status indicators. A description of each indicator is provided below.

Table 2.1-1: Status Bar Indicators

Indicator Name	Description	Host Interface Memory Block Offset
General		
RX:	The number of messages in the capture. The message count increments while a capture is taking place. Only messages that pass the Capture Filter (if enabled) or the trigger point message increment the message count.	
HEX/DEC	The state of the View Data as Hex command is displayed in this field as either "HEX" or "DEC".	
CAN/DeviceNet	The state of the display mode is displayed in this field as either "CAN" or "DeviceNet".	
Filter ON/Filter OFF	The state of the View Filter is displayed in this field as either "Filter ON" or "Filter OFF".	
CAN Counters		
ER:	CAN communication error counter. Incremented when a CAN frame error is detected.	0x38
ML:	CAN lost messages counter. Incremented when a CAN message is received before the previous message is placed into the receive queue.	0x3A
RO:	CAN receive queue overrun counter. Incremented when a CAN message is lost due to a full receive queue.	0x3C
Bus Status		
BP	Bus Power Detect – zero if no bus power. Indicates the presence or absence of network power. This flag is clear if the physical bus interface is not powered.	0x30 – bit 0x0200
ER	CAN Bus Error – CAN communication error. This flag is set each time a CAN communication error is detected. An excessive number of errors indicates a faulty physical media component (cable, connector, etc.) or excessive noise from external sources (check cable routing and shield connection).	0x30 – bit 0x0100
ML	Message Lost – CAN controller/receive ISR. This flag is set when a message is received from the bus while the previous message is still in the receive buffer. A lost message indicates a lower-layer application error (in the kernel interrupt handler).	0x30 – bit 0x80
RO	Receive Buffer Overrun – host application too slow emptying receive queue. This flag is set when messages are received from the bus faster than the application can process them. An overrun receive buffer indicates an upper-layer application error (in the application module).	0x30 – bit 0x40

Indicator Name	Description	Host Interface Memory Block Offset
A	Network Activity Detected – messages received or transmitted. This flag is set when any message is transmitted or received.	0x30 – bit 0x08
BO	Bus Off – this node has been disconnected due to excessive errors. This flag is set when an excessive number of communication errors are detected and the CAN chip automatically goes offline. This flag is cleared when the CAN interface is reinitialized. A bus off condition indicates a serious communication fault, such as an incorrect baud rate or physical layer error (short, open, etc.). To recover from a bus off condition, the application can issue the following command sequence: stop scan, offline, online, start scan.	0x30 – bit 0x04
BW	Bus Warning – this node is experiencing a large number of errors. This flag is set when an abnormal number of communication errors are detected and the CAN chip stops transmitting error frames. This flag is cleared when the error count returns to normal levels or the CAN interface is reinitialized. A bus warning indicates a potentially serious communication fault, such as an out-of-tolerance baud rate or physical layer error (electrical noise, signal attenuation, intermittent connection, etc.).	0x30 – bit 0x02
OL	Online – CAN interface has been initialized and is ready to communicate.	0x30 – bit 0x01






Region 4: List of Captured Messages











The list of captured messages is in the middle portion of the application window. This area displays the captured messages immediately following a capture or after loading a capture file. The fields displayed include index, timestamp, date/time, CAN ID, data size in bytes, and data values. When displaying the messages in DeviceNet mode, the MAC ID, message group, message ID, and message type will also be shown. The trigger point (first message that is allowed by the Trigger Filter), if applicable, is highlighted in yellow. After a successful search, the found message is highlighted in green. The list of captured messages can also be filtered, based on specific messages, communications between a client and server, or mask/match criteria.





2.2 Menu Bar and Toolbar

The Menu Bar contains all of the Network Analyzer commands, and the Toolbar contains icons for many of the Menu commands. A description of each command is provided below.

Table 2.2-1: Menu/Toolbar Items

Menu/Toolbar Item Name	Icon	Description
File Menu		
Open... (Ctrl+O)		Open an existing capture file. Avoid opening capture files that are stored on removable media, as performance may be impaired. Do not open capture files that are stored on floppy disks. You can open older (.dna) capture files by specifying a file type of DeviceNet Network Analyzer 1.x Files in the Open dialog.
Close		Close the active capture.
Close Card and Network Connection		Close the card and network connection.
Save (Ctrl+S)		Save the active capture. Always save capture files to the hard drive. If you want to transfer the capture file to another location or to physical media, copy the file from the hard drive after saving it.
Save View As...		Save the messages that are currently being viewed to a capture file with a new name. You can save all messages or only the range of messages selected. Always save capture files to the hard drive. If you want to transfer the capture file to another location or to physical media, copy the file from the hard drive after saving it.
Export View to Text File...		Export the messages that are currently being viewed to a comma-delimited or fixed-column-width text file. You can save all messages or only the range of messages selected. You can also specify the field types to include, the time and index options, and the MAC ID, message ID, CAN ID, and data format.
MRU list (4 entries)		Open a capture file listed in the recent files list.
Exit		Quit the application. If you have not saved the active capture, you will be prompted to save it before exiting.
View Menu		
Toolbar		Show or hide the toolbar.
Status Bar		Show or hide the status bar.
CAN		Set the display mode to CAN. This mode displays the list of captured messages in a format that conforms to a CAN network, showing only the raw data. It also disables the DeviceNet-specific trigger, capture, and view filtering options.
DeviceNet		Set the display mode to DeviceNet. This mode displays the list of captured messages in a format that conforms to a DeviceNet network, showing the raw data, DeviceNet MAC ID, message group, and message ID, as well as the message type. It also enables the DeviceNet-specific trigger, capture, and view filtering options.

Menu/Toolbar Item Name	Icon	Description
Set Dec/Hex Mode for Columns...		Select whether to view column values in hexadecimal as opposed to decimal. You can specify how the values should be displayed for each of the MAC ID, Msg ID, CAN ID, and Data columns.
View Data as Hex		View data values in hexadecimal as opposed to decimal.
Setup View Filter...		Define the filter to use when displaying the list of captured messages. You can set up this item to filter based on specific messages or mask/match criteria.
Enable View Filter		Toggle whether or not to use the View Filter when displaying the list of captured messages.
Select CAN ID in View Filter		Select all messages in the View Filter that have the same CAN ID as the selection in the view. One or more messages can be selected. You can also access this command by right-clicking on a message.
Remove CAN ID from View Filter		Remove all messages from the View Filter that have the same CAN ID as the selection in the view. One or more messages can be selected. You can also access this command by right-clicking on a message.
Select Message Type in View Filter		Select all messages in the View Filter that have the same predefined DeviceNet message type as the selection in the view. One or more messages can be selected. You can also access this command by right-clicking on a message.
Remove Message Type from View Filter		Remove all messages from the View Filter that have the same predefined DeviceNet message type as the selection in the view. One or more messages can be selected. You can also access this command by right-clicking on a message.
Find... (Alt+F3)		Find a message in the list of captured messages based on CAN ID, or DeviceNet MAC ID, message group, and message ID. The most recently found message is highlighted in green in the view.
Find Next (F3)		Find the next occurrence of a captured message that meets the criteria previously specified during a search.
Find Previous (Shift+F3)		Find the previous occurrence of a captured message that meets the criteria previously specified during a search.
Go To Trigger Point (Ctrl+G)		Find the trigger point in the list of captured messages.
Always On Top		Toggle whether or not the application window is always topmost.
Setup Menu		
Card and Network...		Define the card and network baud rate settings to be used during the capture, and connect to the card.
Trigger Filter...		Define the filter to use when determining the key trigger message used to start or stop a capture upon detecting a specific message. You can set up this item to filter based on specific messages or mask/match criteria, triggering either when the filter criteria are met, or when they are not met for a certain period of time. You can also specify the number of messages to capture prior to the trigger point, and the number of messages or time to capture following it.
Capture Filter...		Define the filter to use when pre-screening messages during network data captures. You can set up this item to filter based on specific messages or mask/match criteria.
Capture Menu		
Enable Capture Filter		Toggle whether or not to use the Capture Filter when capturing network data.

Menu/Toolbar Item Name	Icon	Description
Start		Put the physical connection online and start capturing messages. The Trigger Filter is not used.
From Trigger Point		Put the physical connection online and start capturing messages at the trigger point. The number of messages specified in the Trigger Filter will be captured following the trigger point. If specified in the filter, a certain number of messages prior to the trigger point may also be captured.
To Trigger Point		Put the physical connection online and start capturing messages immediately, but only until the trigger point. The number of messages specified in the filter will be captured following the trigger point.
Help Menu		
About DeviceNet Network Analyzer		Display the product version number and copyright information.

3

Using the Network Analyzer

Chapter Sections:

- Specifying the Card Name and Network Baud Rate
- Using Message Filters
- Using the Trigger Filter
- Using the Capture Filter
- Capturing Network Data
- Using the View Filter
- Finding a Message in the View
- Saving and Exporting Captured Messages

3.1 Specifying the Card Name and Network Baud Rate

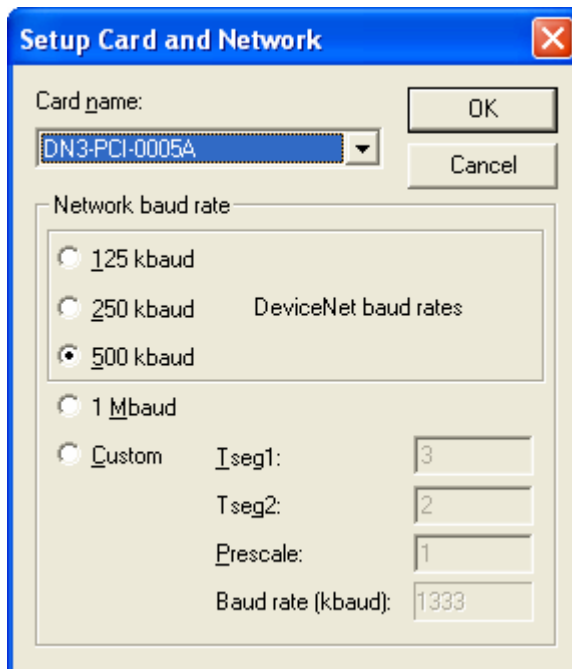
Before capturing network data, you need to select which DeviceNet card will establish the connection, as well as the network baud rate settings for the capture. The Network Analyzer will then go online with the card and allow you to start and stop capturing message traffic.

To define the card and network settings, follow these steps:

1. Select the **Setup Card and Network** command via the Menu or Toolbar:

 **Setup > Card and Network...** The Setup Card and Network dialog is displayed.

Figure 3.1-1: Setup Card and Network Dialog



2. Select a card name.
3. Select a baud rate. For a DeviceNet network, use a baud rate of 125, 250, or 500 kbaud. For a CAN network, you can also select a baud rate of 1 Mbaud or a custom baud rate. For custom baud rates, enter the Tseg1 interval (3 – 16), Tseg2 interval (2 – 8), and baud rate prescaler (1 – 64). The custom baud rate will be calculated and shown within the dialog.

4. Click **OK** to accept the card and network settings. The Network Analyzer connects to the selected card. Typically this results in the BP (Bus Power Detect) status bar indicator being set.



Note

If you start the capture and immediately begin receiving a large number of CAN bus errors (as indicated by the “ER:” status bar indicator), or the ER and BW status bar indicators are set, you should verify that you have selected the correct baud rate for your network.

To close the card and network connection when it is no longer required, select the **Close Connection** command via the Menu or Toolbar:



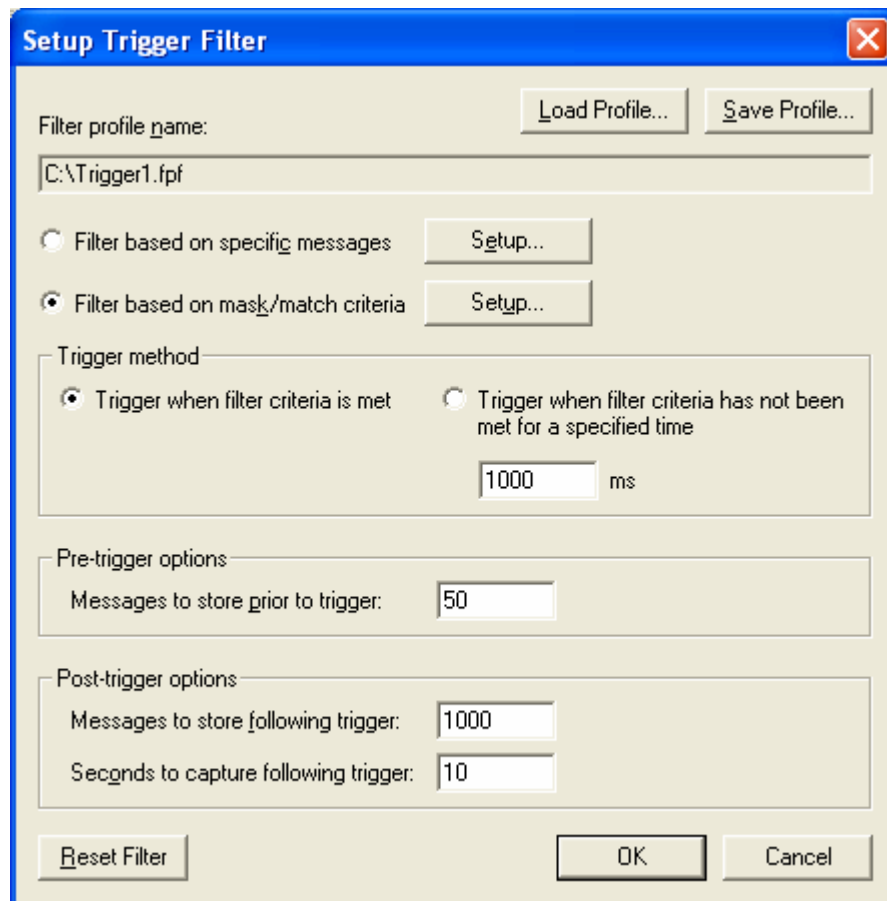
File > Close Card and Network Connection

3.2 Using Message Filters

This section applies to the three different types of Network Analyzer filters ([trigger](#), [capture](#), and [view](#)). These filters will be described later in the chapter.

Selecting the **Setup Trigger Filter**, **Setup Capture Filter**, or **Setup View Filter** command will display the main filter setup dialog. From this dialog you can specify whether to filter based on specific messages or mask/match criteria. For the Trigger Filter, you can also specify the trigger method and the pre- and post-trigger options. You are also able to load and save filter profiles and reset the filter to a default state.

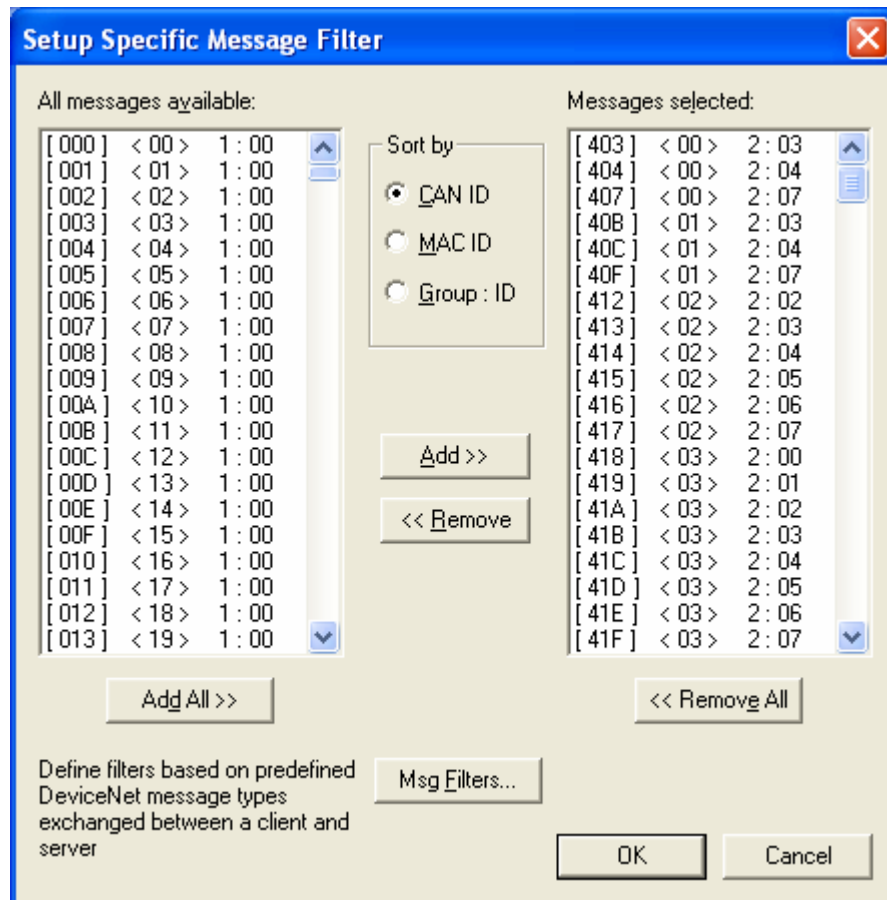
Figure 3.2-1: Setup Filter Dialog



3.2.1 Filtering Based on Specific Messages

In the main Setup Filter dialog, click **Setup**. The Setup Specific Message Filter dialog is displayed.

Figure 3.2.1-1: Setup Specific Message Filter



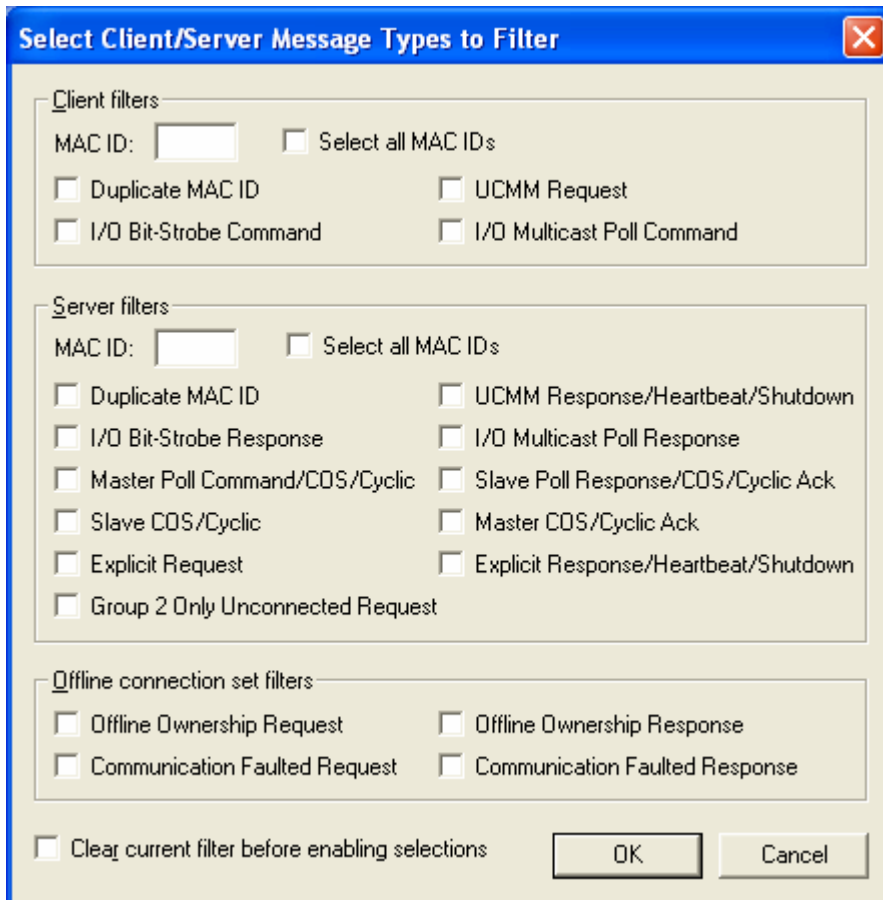
This dialog allows you to select and remove specific messages that will be included in the list of allowed messages. Only messages that appear in the **Messages selected** list on the right will pass through the filter; all others will be ignored.

The two message lists in the dialog can be sorted by CAN ID, MAC ID, or by message group and message ID, depending on the selection in the **Sort by** group.

Multiple messages can be highlighted in either list by holding down Ctrl or Shift while selecting. The CTRL key allows you to select an additional message in the list, and the SHIFT key is used to select a range of messages.

The **Msg Filters** button is used to define filters that are based on the predefined DeviceNet message types exchanged between a client and server, and is only available when in DeviceNet display mode. Clicking **Msg Filters** displays the following dialog.

Figure 3.2.1-2: Select Client/Server Message Types to Filter



The Select Client/Server Message Types to Filter dialog allows you to select specific messages that will be included in the list of allowed messages that make up the filter. Only those messages that are in this list will pass through the filter; all other messages will be ignored.

There are three different filter types that can be added: client, server, and offline connection set. For the client and server filters, a MAC ID must be entered that is associated with the selected message type(s). If a message type is to be included for all MAC IDs, click the **Select all MAC IDs** check box in the Client filters and/or Server filters section. For additional information on each message type, please refer to the DeviceNet specification.

The **Clear current filter before enabling selections** check box can be used to specify whether to add the selected message types to the existing list of allowed messages for the filter, or to remove all existing messages from the list of allowed messages prior to adding the message types.

Clicking **OK** adds the selected message types for the specified MAC IDs to the list of allowed messages that make up the filter. The Messages selected list in the Setup Specific Message Filter dialog will be updated to include the messages that correspond to the selected message types.

To add additional message types to the list of allowed messages, reopen the Select Client/Server Message Types to Filter dialog using the **Msg Filters** button, select the types to include and their associated MAC IDs, and then click **OK**.

3.2.2 Filtering Based on Mask/Match Criteria

To filter based on Mask/Match criteria, follow these steps:

1. In the main Setup Filter dialog, click **Setup**. The Setup Mask/Match Filter dialog is displayed.

Figure 3.2.2-1: Setup Mask/Match Filter

Setup Mask/Match Filter

CAN messages		DeviceNet messages			
CAN ID (000 - 7EF):		MAC ID (00 - 3F):	Msg Group (0 - 3):	Msg ID (00 - 3F):	
000	Mask	FF	0	00	Mask
000	Match	0A	0	00	Match
<input type="checkbox"/> Enable filter		<input checked="" type="checkbox"/> Enable filter	<input type="checkbox"/> Enable filter	<input type="checkbox"/> Enable filter	<input type="checkbox"/> Enable filter

Message data values

1	2	3	4	5	6	7	8	(00 - FF)	
00	FF	00	00	00	00	00	00	00	Mask
00	17	00	00	00	00	00	00	00	Match
<input checked="" type="checkbox"/> Enable filter									

All mask/match values in this dialog should be entered using hex format.

OK Cancel

This dialog allows you to define the filter based on specific mask/match criteria. Messages that don't pass the filter will be ignored.

2. Enable one or more mask/match filters. Two different types can be enabled: one associated with the CAN ID, and the other with data values. Both filters can be used simultaneously. Also, in DeviceNet display mode, the CAN ID can be filtered by specifying mask/match criteria for the MAC ID, message group, and message ID.



Note

You can only define either the CAN ID filter or one or more of the MAC ID, message group, and message ID filters.

3. Specify a mask and match value for each enabled filter. All mask/match values should be entered using hexadecimal format (you don't have to prefix the value with "0x" or postfix it with "h").

If a bit in the mask is set, the corresponding bit in the CAN ID (or MAC ID, message group, and/or message ID) or data value must match the corresponding bit in the match value. Therefore, only those bits in the mask that are set are used when comparing the match value with the message or data values. A bit in the mask that is cleared indicates a "don't care" condition, and is ignored when comparing the match value. A message that meets the criteria of the mask/match filters will pass the filter.

The following is an example of how to specify the mask/match criteria for the CAN ID filter:

Mask	798	111 1001 1000	
Match	1E9	<u>001 1110 1001</u>	
Accepted		001 1xx0 1xxx	where 'x' indicates a bit that will be ignored



Note

When specifying a filter, a mask of 0 indicates that all bits will be ignored. This can be useful when defining the mask/match filter for message data values. For any bytes that don't need to be included in the filter, simply leave the mask set to 0.

To define the filter to match only one value, use a mask that has all bits set (for example, FFF). This tells the filter to compare all bits in the CAN ID (or MAC ID, message group, and/or message ID) or data value with the match value.

4. When you are finished setting the filters, click **OK**.

3.2.3 Loading and Saving Filter Profiles

Your filter settings can be stored in a file, referred to as a filter profile. These files are given a file extension of “.fpf”. A filter profile can be used with any of the three different types of filters (trigger, capture, and view). The settings associated with the pre- and post-trigger options will only be used if the profile is loaded for a Trigger Filter.

- To save a filter profile, click **Save Profile**. The standard Save As dialog is displayed, allowing you to select the location and file name for the profile.
- To load a profile, click **Load Profile**, which opens the file and associates the filter options with the currently open filter. The standard Open dialog is displayed, allowing you to select the profile you want to load.

The profile name will be displayed in the main filter setup dialog following the save or load.


- If you make any changes to the filter, the profile name will be prefixed with an asterisk to indicate that it has been modified. This does not alter the actual file. To update the file, you will need to save the profile again.

When you exit the Network Analyzer and restart the application, the profiles that were last used for each of the three filters will be loaded automatically.

3.3 Using the Trigger Filter

This feature allows you to specify trigger criteria, which are used to determine the key trigger message used to start or stop a capture when a specific message is detected.

To define the Trigger Filter, follow these steps:

1. Select the **Setup Trigger Filter** command via the Menu or Toolbar:
 **Setup > Trigger Filter...** The main filter dialog is displayed, allowing you to specify whether to filter based on specific messages or mask/match criteria. You can also load and save filter profiles for each filter, and reset the filter. Refer to Section 3.2, [Using Message Filters](#), for details relevant to all Network Analyzer filters.
2. Select whether you want to trigger when the filter criteria are met, or when the filter criteria have not been met for a certain period of time. If you are triggering when the criteria have not been met for a specified time, enter the number of milliseconds. The maximum value is 300,000.
3. Enter the number of messages to capture prior to the trigger point. If you don't want any messages to be captured beforehand, enter 0. The maximum value is 1000.

If the Capture Filter is enabled, the specified number of messages that pass it will be stored.



Note

You may capture fewer messages than specified if the trigger point occurs before the specified number of messages have been captured.

4. Enter the number of messages to capture and the number of seconds for capturing after a trigger point. If you don't want any messages to be captured after this point, enter 0 in either field. The maximum number of messages is 99,999,999, and the maximum number of seconds is 4,000,000.


After a trigger point, messages will be captured until the specified number of messages has been reached or the specified number of seconds has elapsed, whichever occurs first. Note that the capture may end earlier due to the restrictions on the number of messages or capture duration. You can capture up to 100 million messages over a period of up to 46 days.

3.4 Using the Capture Filter

This feature is used when pre-screening messages during network data captures.

3.4.1 Defining the Capture Filter

To define the Capture Filter, select the **Setup Capture Filter** command, via the Menu or Toolbar:

 **Setup > Capture Filter...** The main filter dialog is displayed, allowing you to specify whether to filter based on specific messages or mask/match criteria. You can also load and save filter profiles for each filter, and reset the filter. Refer to Section 3.2, [Using Message Filters](#), for details relevant to all Network Analyzer filters.

3.4.2 Toggling the Capture Filter

To toggle the Capture Filter, use the **Enable Capture Filter** command, via the Menu or Toolbar:






 **Capture > Enable Capture Filter.**

3.5 Capturing Network Data

Once you have selected the card and network baud rate, and created a Trigger Filter and/or Capture Filter (optional), you can begin capturing network data.

The capture can be started in three different ways. When combined with the pre- and post-trigger options, this results in five different capture methods, as outlined in the following table.

Table 3.5-1: Methods for Capturing Network Data

Command/Method Name	Icon	Description
Start Capture (pre-trigger options ignored; post-trigger options ignored)		The capture starts immediately, without a trigger point. The capture ends when you manually stop the capture, or the restrictions on the number of messages or duration of the capture have been exceeded.
Capture from Trigger Point (pre-trigger options set to 0; post-trigger options specified for the number of messages to store and/or the number of seconds to capture following the trigger point)		The capture starts when a trigger point occurs. The capture ends when the specified number of messages has been captured or the specified number of seconds has elapsed after a trigger point, whichever occurs first. The capture also will end if you manually stop the capture, or the restrictions on the number of messages or duration of the capture have been exceeded.
Capture from Trigger Point (pre-trigger options specified for the number of messages to store prior to the trigger point; post-trigger options specified for the number of messages to store and/or the number of seconds to capture following the trigger point)		The capture starts just before a trigger point occurs. The capture ends when the specified number of messages has been captured or the specified number of seconds has elapsed after a trigger point, whichever occurs first. The capture also will end if you manually stop the capture, or the restrictions on the number of messages or duration of the capture have been exceeded.
Capture to Trigger Point (pre-trigger options ignored; post-trigger options set to 0)		The capture starts immediately. It ends when a trigger point occurs.
Capture to Trigger Point (pre-trigger options ignored; post-trigger options specified for the number of messages to store and/or the number of seconds to capture following the trigger point)		The capture starts immediately. It ends when the specified number of messages has been captured or the specified number of seconds has elapsed after a trigger point, whichever occurs first. The capture will also end if you manually stop the capture, or the restrictions on the number of messages or duration of the capture have been exceeded.

If you have set any post-trigger options, the capture stops when the specified number of messages has been captured or the specified number of seconds has elapsed after a trigger point, whichever occurs first. You can also stop the capture by pressing the **Stop** button.

If the restrictions on the number of messages or capture duration have been exceeded, the capture may end earlier than expected. You can capture up to 100 million messages over a period of up to 46 days.

The “RX:” counter on the status bar will increment as messages are stored. The Status Bar also provides the status of the CAN counters and bus (refer to Table 2.1-1). Once the capture is complete, the total number of stored messages will be indicated.

The list of captured messages displays the messages immediately following a capture, or after loading a capture file. The fields displayed include index, timestamp, date/time, CAN ID, data size in bytes, and data values. When displaying the messages in DeviceNet mode, the MAC ID, message group, message ID, and message type are also shown. The trigger point (first message that is allowed by the Trigger Filter) is highlighted in yellow.

The timestamp represents the time, in milliseconds, assigned to a message when it arrives in the receive queue. The date/time represents the system time when a message occurs, as calculated from the timestamp. The timestamp resolution is one microsecond.

3.5.1 Toggling Between Hexadecimal and Decimal

To toggle between hexadecimal and decimal values, use the **View > Set Dec/Hex Mode for Columns** command via the Menu, or the **View Data as Hex** command, via the Menu or Toolbar:

 **View > View Data as Hex**

3.5.2 Setting the Display Mode to CAN

To set the display mode to CAN, which only shows the raw data, use the **Display CAN** command, via the Menu or Toolbar:

 **View > CAN**

3.5.3 Setting the Display Mode to DeviceNet

To set the display mode to DeviceNet, which shows the raw data, DeviceNet MAC ID, message group, message ID and message type, use the **Display DeviceNet** command, via the Menu or Toolbar:


 **View > DeviceNet**

3.6 Using the View Filter

This feature allows you to filter messages after they've been captured.

3.6.1 Defining the View Filter


To define the View Filter, use the **Setup View Filter** command, via the Menu or Toolbar:

 **View > Setup View Filter...** The main filter dialog is displayed, allowing you to specify whether to filter based on specific messages or mask/match criteria. You can also load and save profiles for each filter, and reset the filter. Refer to Section 3.2, [Using Message Filters](#), for details relevant to all Network Analyzer filters.

If you redefine the View Filter while it's in use (i.e., the list of captured messages is being filtered), you will be asked if you want to apply the new settings to the current view. Click **Yes** to apply the new settings immediately.

3.6.2 Toggling the View Filter

To toggle the View Filter, use the **Enable View Filter** command, via the Menu or Toolbar:

 **View > Enable View Filter**

3.6.3 Removing Messages from the View Filter

To quickly select or remove one or more messages from the View Filter, use the **Select/Remove CAN ID** and **Select/Remove Message Type** commands. These commands are available via the View menu, or by right-clicking on a captured message. The following table describes the available commands:

Table 3.6-1: Commands for Selecting/Removing Messages in the View Filter

Menu Command Name	Description
Select CAN ID in View Filter	Select all messages in the View Filter that have the same CAN ID as the selection in the view. One or more messages can be selected.
Remove CAN ID from View Filter	Remove all messages from the View Filter that have the same CAN ID as the selection in the view. One or more messages can be selected.
Select Message Type in View Filter	Select all messages in the View Filter that have the same predefined DeviceNet message type as the selection in the view. One or more messages can be selected.
Remove Message Type from View Filter	Remove all messages from the View Filter that have the same predefined DeviceNet message type as the selection in the view. One or more messages can be selected.

3.7 Finding a Message in the View

The Network Analyzer provides a means to search for a specific message within the list of captured messages, or to quickly reposition the view to display the trigger point, if one exists.

3.7.1 Finding a Specific Message

To find a specific message, use the **Find** command via the Menu or Toolbar:


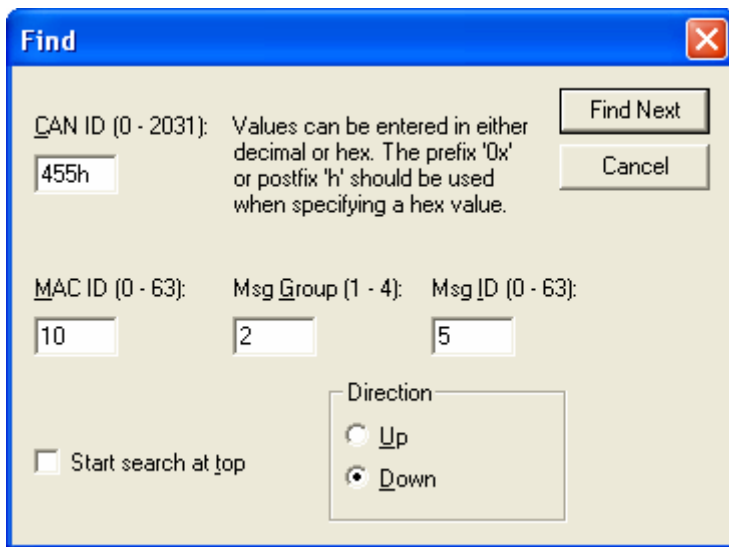
 **View > Find...** A dialog is displayed, allowing you to specify the CAN ID, or the MAC ID, message group, and message ID.

Figure 3.7.1-1: Find Dialog




Note

Values within the dialog can be entered in either decimal or hexadecimal, by using the “0x” prefix or “h” postfix. If you enter a value for the CAN ID, the MAC ID, message group, and message ID fields will be updated automatically. Correspondingly, if you enter a value for the MAC ID, message group, or message ID, the CAN ID field will be updated automatically.

Check **Start search at top** if you want to begin the search at the beginning of the displayed list of captured messages. You can also specify the direction to be used when searching, either up or down.

Click **Find Next** to start the search. If a captured message that meets the search criteria is found in the view, the message will be highlighted in green.

To find the next occurrence of a captured message that meets the criteria previously specified during a search, use the **Find Next** command via the Menu or Toolbar:

 **View > Find Next**

To find the previous occurrence of a captured message that meets the search criteria previously specified, use the **Find Previous** command via the Menu or Toolbar:

 **View > Find Previous**

Following a successful search for the next or previous occurrence of a message in the displayed list of captured messages, the found message is highlighted in green.

3.7.2 Finding the Trigger Point

To find the trigger point in the list of captured messages, use the **View > Go To Trigger Point** command via the Menu, or press CTRL+G. The trigger point, if one exists, will immediately be visible in the view.

3.8 Saving and Exporting Captured Messages

There are three ways to save the captured messages:

1. By saving all of them to a capture file, which the Network Analyzer can later retrieve.
2. By saving the messages that are currently being viewed.
3. By exporting the messages that are currently being viewed to a text file.




Note

Always save capture files to the hard drive. If you want to transfer the capture file to another location or to physical media, copy it from the hard drive after saving it.

3.8.1 Saving to a Capture File

To save all of the messages in the active capture to a file, use the **Save** command, via the Menu or Toolbar:

 **File > Save**. The standard Save As dialog is displayed, allowing you to select the location and name for the capture file.

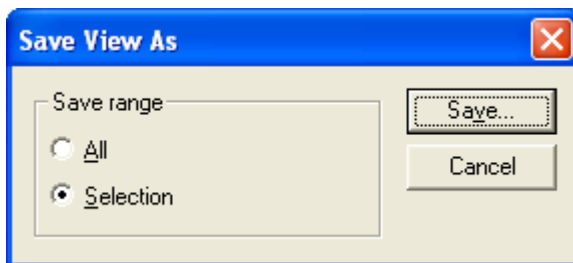
3.8.2 Saving the View to a Capture File

Before saving the view to a capture file, you can specify a range of messages by selecting a message in the list and then using the SHIFT key to select a second message, which will highlight the entire range of messages to be saved. Alternatively, you can use the CTRL key to select the second message in the list, in which case all messages from the first to the second selection will be included in the range.

To save the view to a capture file, follow these steps:

1. Select the **Save View As** command, via the menu: **File > Save View As...**
The Save View As dialog is displayed.

Figure 3.8.2-1: Save View As Dialog



2. Select the appropriate radio button and click **Save....** The standard Save As dialog is displayed, allowing you to select the location and name for the capture file.

3.8.3 Exporting the View to a Text File

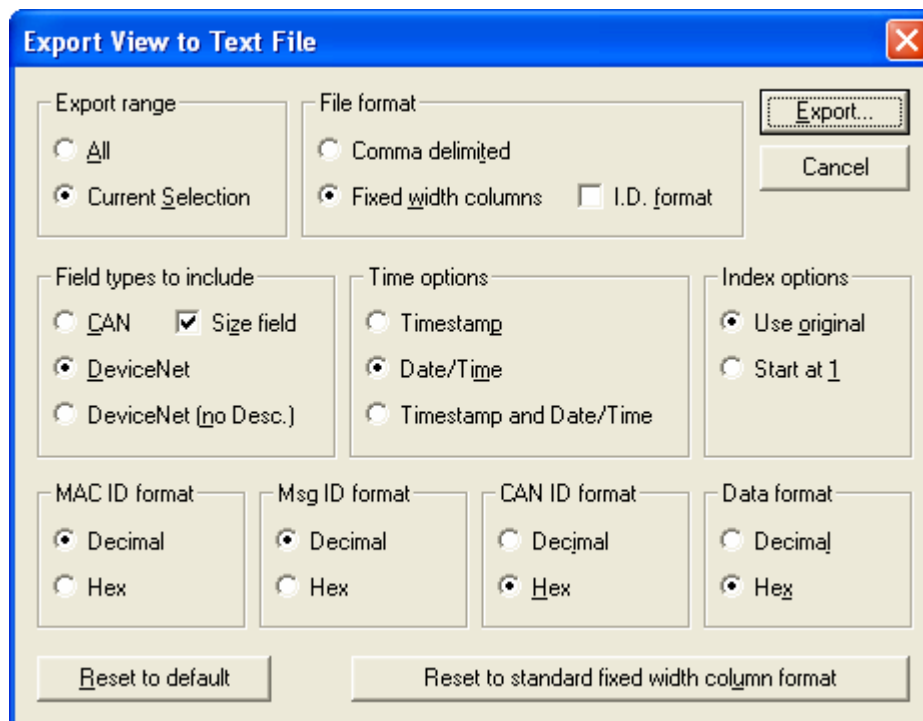
You can save the text file in comma-delimited or fixed-column-width format. You can also specify which fields should be included in the export, the time and index options, and whether the MAC ID, message ID, CAN ID, and data values should be formatted as decimal or hexadecimal.

Before exporting the view to a text file, you can specify a range of messages by selecting a message in the list and then using the SHIFT key to select a second message, which will highlight the entire range of messages to be exported. Alternatively, you can use the CTRL key to select the second message in the list, in which case all messages from the first to the second selection will be included in the range.

To export to a text file, follow these steps:

1. Select the **Export View to Text File** command, via the menu: **File > Export View to Text File...** The Export View to Text File dialog is displayed.

Figure 3.8.3-1: Export View to Text File



2. Select the appropriate Export range, either **All** or **Current Selection**. If a range of messages was selected in the list of captured messages prior to executing this command, then **Current Selection** will be selected by default. If a range of messages was not selected, then only **All** can be selected.
3. Specify whether the file should be formatted to use comma-delimited or fixed-width columns.
4. Select any other options you want to use for the export. The current set of options will be the same as the options that were used during the last successful export.

The following options are available:

- I.D. format:

If you're using fixed-width-column formatting, and you have not chosen to only include CAN field types, then you can choose to use the I.D. formatting style for the MAC ID, group, message ID, and CAN ID. If **I.D. format** is selected, the MAC ID, Group, Msg ID, and CAN ID columns will be replaced with a single column called I.D., formatted as <MAC ID>Group:Message ID [CAN ID]. For example, <26>2:03 [04D3]".

- Field types to include:

Selecting **CAN** will include only the CAN ID field in the export. Selecting **DeviceNet** will include the MAC ID, Group, Msg ID, CAN ID, and Description fields. Selecting **DeviceNet (no Desc.)** will include the MAC ID, Group, Msg ID, and CAN ID fields. If **DeviceNet** or **DeviceNet (no Desc.)** is selected, and you are using fixed width column formatting along with the I.D. format, then only a single column, called "I.D", will be exported (refer to the I.D. format option above).

Selecting **Size field** will include the Size field in the export, which is the number of bytes of data associated with each message.

- Time options:

Selecting **Timestamp** will include the Timestamp field in the export, which is the time, in milliseconds, assigned to each message when it arrived in the receive queue. Selecting **Date/Time** will include the Date/Time field in the export, which is the system time when each message occurred, as calculated from the timestamp. Selecting **Timestamp and Date/Time** will include both fields.

- **Index options:**
Selecting **Use original** will result in the exported Index values being the same as the Index field values in the list of captured messages view. Selecting **Start at 1** will set the Index value for the first exported message to 1 and then increment the Index for each message that follows by 1.
- **MAC ID format:**
Select **Decimal** or **Hex** to choose the display format for the MAC ID value in the exported text file.
- **Msg ID format:**
Select **Decimal** or **Hex** to choose the display format for the Msg ID value in the exported text file.
- **CAN ID format:**
Select **Decimal** or **Hex** to choose the display format for the CAN ID value in the exported text file.
- **Data format:**
Select **Decimal** or **Hex** to choose the display format for the Data value in the exported text file.
- **Default format:**
To restore the default set of options, click the **Reset to Default** button. The following is a sample of the “default” format, not including the DeviceNet Description field:

Index	Trig	Date/Time	MAC ID	Group	Msg ID	CAN ID	Size	Data
1		03/17/05 19:10:15.794439	10	1	15	3CA	1	0D
2		03/17/05 19:10:15.794576	26	1	15	3DA	1	00
3		03/17/05 19:10:15.795196	10	2	05	455	1	00
4		03/17/05 19:10:15.795362	26	2	05	4D5	1	00
5	!	03/17/05 19:10:15.795716	26	2	04	4D4	4	40 17 01 01
6		03/17/05 19:10:15.795830	10	1	15	3CA	1	0D
7		03/17/05 19:10:15.795969	26	1	15	3DA	1	00
8		03/17/05 19:10:15.796514	26	2	03	4D3	4	40 94 08 FF

- Standard fixed-width-column format:

To change the options to a standard fixed-width-column formatting style, similar to the format used by the previous-generation network capture tool, click the **Reset to standard fixed width column format** button. The following is a sample of the “standard fixed width column” format:

03-17-2007 19:10:15

Index	Trig	Timestamp (ms)	I.D.	Data
1		251383.359	<10>2:05	[0455] 00
2		251383.525	<26>2:05	[04D5] 00
3		251383.913	<10>1:15	[03CA] 0D
4		251384.027	<26>1:15	[03DA] 00
5	!	251998.034	<10>2:04	[0454] 40 17 01 01
6		251998.149	<10>1:15	[03CA] 0D
7		251998.262	<26>1:15	[03DA] 00
8		251998.662	<10>2:03	[0453] 40 94 08 FF



Note

Clicking **Reset to Default** or **Reset to standard fixed width column format** will also reset the file format selection to use fixed width columns.

5. Click **Export...** The standard Save As dialog is displayed, allowing you to select the location and name for the exported text file.

4

Troubleshooting

Chapter Sections:

- Required Software Components

4.1 Required Software Components

To function properly, the Network Analyzer depends on other software components. These are listed in the following table.

Table 4.1-1: Required Software Components

Name	Version # (or Higher)	Description
Can2a.ss3	2.05.4	Woodhead CAN2.0A module (located in the folder that SST modules get installed in, typically C:\Program Files\SST\DeviceNet DN3\Modules; Windows registry entries are associated with this module)
Dnerr32.dll	1.8.7.0	Woodhead DeviceNet Error DLL (installed as part of the DeviceNet driver)
Ssc2a32.dll	1.14.3.0	Woodhead CAN2.0A 32-bit DLL (installed as part of the DeviceNet driver)
Ssdn32.dll	3.7.4.0	Woodhead DeviceNet Hardware Driver DLL (installed as part of the DeviceNet driver)
Sx32w.dll	6.3.1.0	Rainbow Sentinel SuperPro Library DLL

A

Warranty and Support

Appendix Sections:

- Warranty
- Technical Support

A.1 Warranty

For software warranty information, refer to <http://www.mysst.com/warranty.asp>.

A.2 Technical Support

Please ensure that you have the following information readily available before calling for technical support:

- Software version
- Computer's make, model, CPU speed and hardware configuration (cards installed)
- Operating system type and version
- Details of the problem you are experiencing: application module type and version, target network, and circumstances that may have caused the problem

A.2.1 Getting Help

Technical support is available during regular business hours by telephone, fax or email from any Woodhead Software & Electronics office, or from <http://www.woodhead.com>. Documentation and software updates are also available on the Web site.

North America

Canada:

Tel: 1-519-725-5136

Fax: 1-519-725-1515

Email: WoodheadSupportNA@molex.com

Europe

France:

Tel: 33-(0)2-32-96-04-22

Fax: 33-(0)2-32-96-04-21

Email: WoodheadSupportEU@molex.com

Germany:

Tel: 49-711-782-374-22

Fax: 49-711-782-374-11

Email: WoodheadSupportEU@molex.com

Italy:

Tel: 39-010-595-4052

Fax: 39-010-595-6925

Email: WoodheadSupportEU@molex.com

Other countries:

Tel: 33-(0)2-32-96-04-23

Fax: 33-(0)2-32-96-04-21

Email: WoodheadSupportEU@molex.com

Asia-Pacific

Japan:

Tel: 81-3-5791-4621

Fax: 81-3-5791-4688

Email: WoodheadSupportAP@molex.com

Singapore:

Tel: 65-6261-6533

Fax: 65-6261-3588

Email: WoodheadSupportAP@molex.com

China:

Tel: 86-21-5835-9885

Fax: 86-21-5835-9980

Email: WoodheadSupportAP@molex.com

For the most current contact details, please visit <http://www.woodhead.com>.

Index

A

A indicator, 16

B

baud rate, specifying, 22

BO indicator, 16

BP indicator, 15

bus status indicators, 15

BW indicator, 16

C

CAN counters, 15

CAN/DeviceNet indicator, 15

capture file

 saving messages to, 40

 saving view to, 40

Capture Filter, using, 32

captured messages

 exporting, 39

 finding, 37

 list of, 16

 saving, 39

card name, specifying, 22

Console, defined, vii

conventions used in this guide

 special notation, vii

 special terms, vii

 style, vi

D

data capturing, 33

DeviceNet/CAN indicator, 15

E

ER indicator, 15

exporting captured messages, 39

exporting view to text file, 41

F

features, of Network Analyzer, 10

Filter ON/OFF indicator, 15

filters

 and data capturing, 33

 filtering specific messages, 25

 finding captured messages, 37

 loading and saving profiles, 30

 mask/match filtering, 27

 setting up, 24

 using Capture Filter, 32

- using Trigger Filter, 31
- using View Filter, 35, 37
- finding a captured message, 37
- finding the trigger point, 38

H

HEX/DEC indicator, 15

L

loading filter profiles, 30

M

- mask/match filtering, 27
- Menu Bar items, 17
- Menu Bar, location and function of, 14
- message filters, using, 24
- messages
 - finding, 37
 - finding trigger point, 38
 - saving to capture file, 40
- ML indicator, 15

N

Network Analyzer

- capabilities of, 10
- commands for, 17
- defined, vii
- function of, vi, 11
- general overview of, 14
- guidelines for use, 11
- software required for, 46
- system requirements for, 12
- technical support for, 48
- using, 22
- warranty for, 48

network baud rate, specifying, 22

network data, capturing, 33

note, defined, vii

O

OL indicator, 16

P

purpose of this guide, vi

R

RO indicator, 15

RX indicator, 15

S

- saving captured messages, 39
- saving filter profiles, 30
- saving messages to capture file, 40
- saving the view, 40
- software license, for Network Analyzer, 12
- software, for Network Analyzer, 46
- specific messages, filtering, 25
- Status Bar, location and function of, 15
- support, 48
- system requirements, for Network Analyzer, 12

T

Technical Support, 48

Toolbar items, 17

Toolbar, location and function of, 15

Trigger Filter

- function of, 10
- using, 31

trigger point, finding, 38

V

view

- exporting to text file, 41
- saving to capture file, 40

View Filter, using, 35, 37

W

warranty, 48