

# **LonScanner™ Protocol Analyzer User's Guide**



Echelon, LNS, LonTalk, LONWORKS, i.LON, LONMARK, NodeBuilder, Neuron and the Echelon logo are registered trademarks of Echelon Corporation. LonMaker and LonScanner are trademarks of Echelon Corporation.

Other brand and product names are trademarks or registered trademarks of their respective holders.

Neuron Chips and other OEM Products were not designed for use in equipment or systems which involve danger to human health or safety or a risk of property damage and Echelon assumes no responsibility or liability for use of the Neuron Chips in such applications.

Parts manufactured by vendors other than Echelon and referenced in this document have been described for illustrative purposes only, and may not have been tested by Echelon. It is the responsibility of the customer to determine the suitability of these parts for each application.

ECHELON MAKES AND YOU RECEIVE NO WARRANTIES OR CONDITIONS, EXPRESS, IMPLIED, STATUTORY OR IN ANY COMMUNICATION WITH YOU, AND ECHELON SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Echelon Corporation.

Printed in the United States of America.  
Copyright © 1994 – 2005 Echelon Corporation.

Echelon Corporation  
[www.echelon.com](http://www.echelon.com)

---

## Welcome

You can use the LonScanner™ Protocol Analyzer to monitor, analyze, and diagnose the behavior of installed LONWORKS® networks. The LonScanner Protocol Analyzer connects to IP-852 (ANSI/CEA-852), LONWORKS/IP, and native ANSI/CEA709.1 (EN14908) channels, collects packets from those channels, and records information from the packets into log files. You can use the log files to inspect and interpret the collected packets.

You can monitor up to 10 channels at once with the protocol analyzer. You can view the logs created for each channel, called active logs, while the protocol analyzer is monitoring the channel and collecting packets, and you can take advantage of the filtering and statistical features the tool provides to make sure it gathers the information you want to see.

---

## Purpose

The *LonScanner Protocol Analyzer User's Guide* describes how to use the LonScanner Protocol Analyzer to monitor, analyze, and diagnose IP-852 (ANSI/CEA-852), LONWORKS/IP, and native ANSI/CEA709.1 (EN14908) channels, and how to interpret the data that the protocol analyzer collects.

---

## Related Documentation

The *Introduction to the LONWORKS System* document provides an introduction to the LONWORKS platform. You can view this document by clicking the Windows Start menu, opening the Echelon LonScanner Protocol Analyzer program folder, and then clicking **Introduction to LonWorks**.

---

## Software Requirements

To install and use the LonScanner software, your computer must meet the following minimum requirements:

- Intel® Pentium® III 800MHz processor
- 128MB RAM
- Windows XP, Windows Server 2003, or Windows 2000
- 10MB of available hard-disk space
- 800x600 screen resolution

---

## Table of Contents

Welcome .....	i
Purpose .....	i
Related Documentation .....	i
Software Requirements .....	i
Table of Contents .....	i

<b>Introduction .....</b>	<b>1</b>
Introduction .....	2
New Features .....	2
Using LonScanner with LNS Turbo Edition .....	3
Installing the LonScanner Software .....	4
Activating the LonScanner Software .....	5
Transferring a LonScanner Activation .....	6
Viewing Activation Status .....	8
Using the LonScanner Protocol Analyzer .....	8
Monitoring a Network Channel .....	9
Opening an Existing Packet Log .....	9
Log Files Overview .....	10
Using the LonScanner Menus, Toolbar, and Status Bar .....	11
LonScanner Menus .....	11
LonScanner Toolbar .....	12
LonScanner Status Bar .....	14
Document Roadmap .....	14
<b>Logging Data .....</b>	<b>17</b>
Configuring the LonScanner Protocol Analyzer .....	18
Setting Logging Preferences .....	18
Filtering Packets .....	19
Configuring the Global and Device Filters .....	20
Importing Filter Settings From a Channel .....	23
Saving Filter Settings For Later Use .....	23
Setting the Capture and Monitor Modes .....	23
Viewing Channel Statistics and Trend Graphs .....	24
Viewing Bandwidth Utilization by Packet Types .....	25
Viewing Bandwidth Utilization History .....	26
Viewing Error Rate History .....	27
Viewing General Statistics .....	27
Setting Statistics Options .....	28
Using Names .....	32
Importing Names .....	33
Importing Names from an LNS Database .....	33
Importing Names from a Local Names File .....	36
Importing Names from a Channel .....	37
Creating and Customizing Names .....	38
Creating Group Names .....	38
Creating Device Names .....	39
Creating Message Code Names .....	40
Creating Domain Names .....	41
Managing Names Files .....	42
<b>Analyzing Packet Log Details .....</b>	<b>45</b>
Searching For Packet Log Entries .....	46
Searching By String .....	46
Searching By Log Number .....	47
Bookmarking Packet Log Entries .....	47
Formatting the Packet Log .....	49
Selecting Data Fields .....	49
Formatting Data Field Columns .....	50
Color-Coding the Packet Log .....	51
Printing Log Files .....	52

Exporting Log Files.....	53
<b>Example Logs .....</b>	<b>55</b>
Example Packet Logs.....	56
Channel Without Assigned Names.....	56
Channel with Names Imported from LNS Database .....	57
<b>Network Interfaces.....</b>	<b>61</b>
Network Interfaces Overview.....	62
i.LON 100 Internet Server.....	63
i.LON 600 LONWORKS/IP Server.....	64
PCC-10 and PCLTA-20/21 .....	64
<b>LonScanner Software License Agreement .....</b>	<b>67</b>



# 1

## Introduction

This chapter introduces the LonScanner Protocol Analyzer. It describes how to install and activate the LonScanner software, and how to get started with the protocol analyzer. This chapter also provides a roadmap you can follow when reading this document and learning how to use the protocol analyzer.

---

## Introduction

You can use the LonScanner Protocol Analyzer to monitor, analyze, and diagnose the behavior of installed LONWORKS networks. The LonScanner Protocol Analyzer connects to IP-852 (ANSI/CEA-852), LONWORKS/IP, and native ANSI/CEA709.1 (EN14908) channels, collects packets from those channels, and records information from the packets into log files. You can use the log files to inspect and interpret the collected packets.

You can monitor up to 10 channels at once with the protocol analyzer. You can view the logs created for each channel, called active logs, while the protocol analyzer is monitoring the channel and collecting packets, and you can take advantage of the filtering and statistical features the tool provides to make sure it gathers the information you want to see.

IP-852 (ANSI/CEA-852) and LONWORKS/IP channels are both referred to as *IP-852 channels* in this user's guide. Native ANSI/CEA-709.1 (EN14908) channels such as TP/FT-10 and PL-20 are referred to as *709.1 channels* in this user's guide.

---

## New Features

Release 3 of the LonScanner Protocol Analyzer supports all the features of the Echelon LonManager Protocol Analyzer. It also includes the following new features:

- Runs on Windows XP, Windows 2003 Server, and Windows 2000.
- Supports all Echelon layer 2 and IP-852 network interfaces, including the U10 USB Network Interface, U20 USB Network Interface, PCC-10, PCLTA-20, PCLTA-21, *i.LON*<sup>®</sup> 100 Internet Server, and *i.LON* 600 LONWORKS/IP Server. A separately licensed LNS<sup>®</sup> Turbo runtime is required for use with IP-852 channels.
- Provides enhanced statistical views of the network, including bandwidth utilization and packet type statistics.
- Allows monitoring of up to 10 separate channels at once.
- Allows network interface sharing if an LNS Turbo Edition Server is installed.
- Provides integrated packet detail display.
- Supports the ANSI/CEA-709.1-B protocol extended command set (ECS).
- Formats network variable values using formats defined in LONMARK<sup>®</sup> resource files.
- Imports device and network variable names from an LNS network database.



---

## Using LonScanner with LNS Turbo Edition

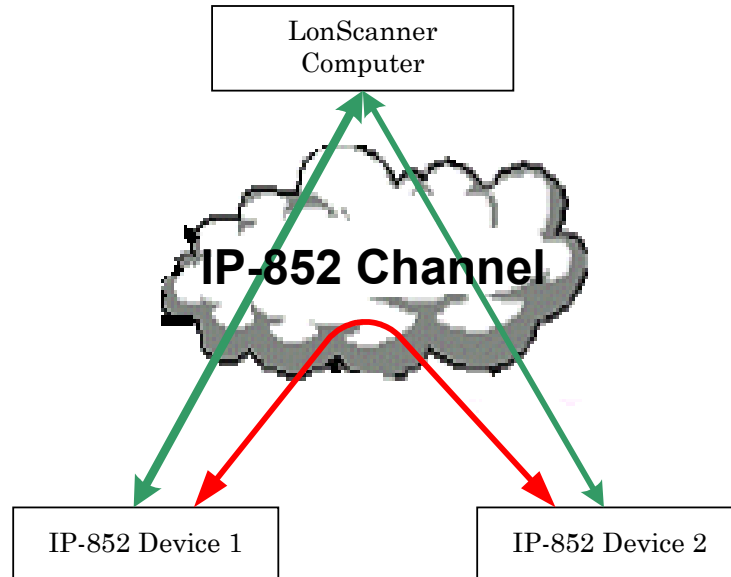
If you plan to use LonScanner Professional Edition with 709.1 channels, you do not require an LNS Turbo Edition Server. However, when used with the protocol analyzer, an LNS Turbo Edition Server provides several additional features.

The first is the importing of device and network variable names from an LNS network database. This feature is described in Chapter 2 of this document. The second is network interface sharing. If you have LNS Turbo Edition Server installed, you can use the protocol analyzer and the LonMaker™ Integration Tool (or any custom LNS application) at the same time with the same network interface, as long as the network interface is a PCC-10, a PCLTA-20/21, an *i*.LON 100 Internet Server, an *i*.LON 600 LONWORKS/IP Server or a USB Network Interface.

You can also run the protocol analyzer and the LonMaker tool (or any custom LNS application) at the same time with the same network interface on a computer with an LNS 3 Server, as long as you are using an *i*.LON 100 Internet Server or an *i*.LON 600 LONWORKS/IP Server as the network interface. In addition, you can import device and network variable names from your LNS database if you have an LNS 3 Server.

Another key feature provided by LNS Turbo Edition is the monitoring of IP-852 channels. With an LNS Turbo Edition Server installed, you can use the protocol analyzer to monitor IP-852 channels, as well as 709.1 channels. When using the LNS Turbo IP-852 interface, there is one key difference from 709.1 channels. The layer 2 interface of every device on a 709.1 channel receives every packet on the channel. Echelon's IP-852 devices and routers do not automatically forward packets to every other device and router on the channel. Instead, they selectively forward packets directly to the intended destination devices and routers on the channel. As a result, the protocol analyzer will not receive packets that are sent on an IP-852 channel from one device or router to another if the source or destination device is not the computer running the protocol analyzer.

Figure 1.1 demonstrates this. In Figure 1.1, the protocol analyzer is monitoring an IP-852 channel containing two devices named "IP-852 Device 1" and "IP-852 Device 2." The protocol analyzer will only receive packets sent between the IP-852 devices and the LonScanner computer (the network paths displayed in green). The protocol analyzer will not receive packets sent between IP Device 1 and IP Device 2 (the network path displayed in red).



**Figure 1.1** Using LonScanner to Monitor an IP-852 Channel

---

## Installing the LonScanner Software

To install the LonScanner software, follow these steps:

1. Insert the Echelon LonScanner Protocol Analyzer CD into a CD-ROM drive. If the installation does not automatically start after a few seconds, start the program manually. You can start the installation by clicking the Windows **Start** button, clicking **Run**, browsing to the setup application, and then clicking **Open**. The main LonScanner installation window opens.
2. Click **Install Products** to continue. The Install Products window opens.
3. Click **LonScanner Protocol Analyzer** to continue. The Welcome window opens.
4. Click **Next** to continue. The License Agreement window opens.
5. Read the terms of the LonScanner software license agreement, and click **I Accept the Terms in the License Agreement** if you agree to the license agreement. The User window opens.  
**NOTE:** The LonScanner software license is included in this document in Appendix B, *LonScanner Software License Agreement*.
6. Fill in your user name, organization and serial number, and click **Next** to continue.
7. If the LONWORKS path has not been set for your computer, a dialog will open prompting you to choose this path. You can change this setting as long as you have not previously installed any other Echelon or LONMARK software. Click **OK** to select the path.
8. On the next dialog, click **Install** to begin the installation. When the installation has completed, a dialog appears to notify you.

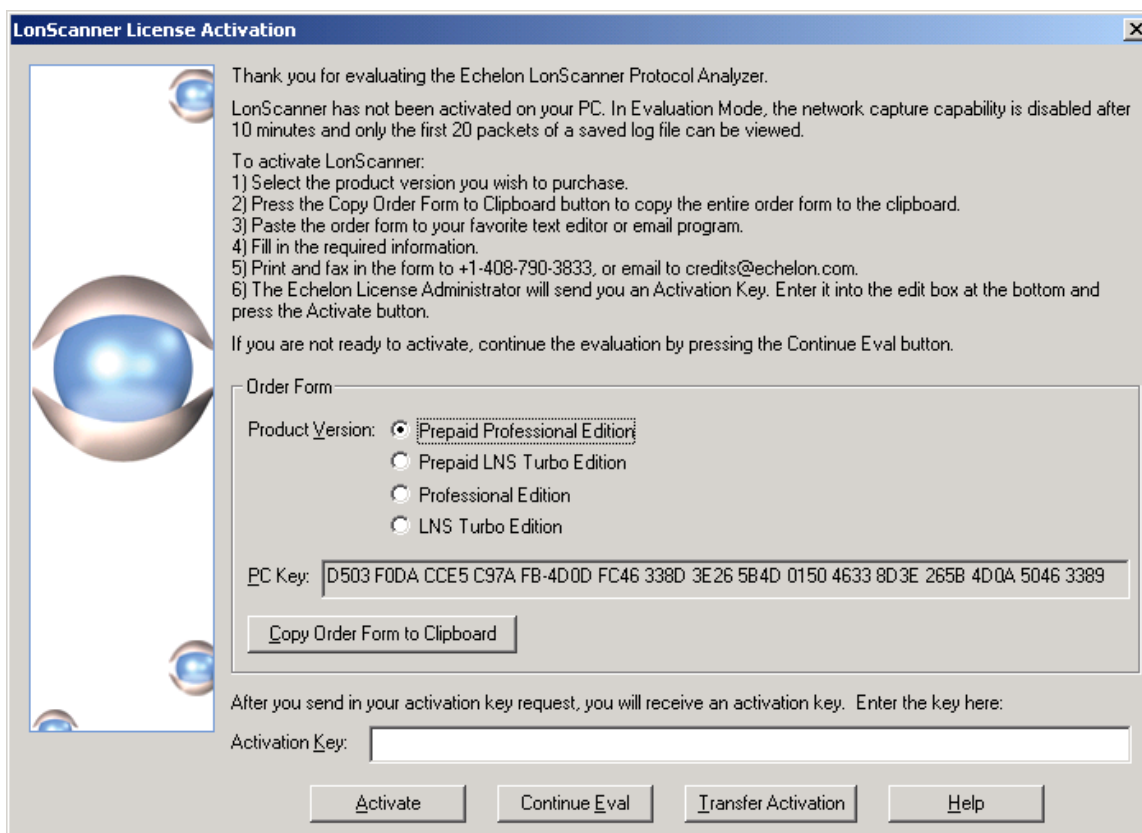
**NOTE:** You can also choose to install Adobe Acrobat Reader, the NodeBuilder<sup>®</sup> Resource Editor, and the PCC-10/PCLTA 10/20/21 Drivers software from the Install Products dialog mentioned in steps 2 and 3.

You can use the NodeBuilder Resource Editor to browse the network variable types available on your computer when configuring device names with the protocol analyzer, as described in Chapter 2 of this document. The installation provides the option to install the PCC-10/PCLTA 10/20/21 Drivers software in case you are using a PCC-10, PCLTA-10, PCLTA-20, or PCLTA-21 as your network interface, and do not have current driver software installed. Drivers for the *i*.LON 100 Internet Server, *i*.LON 600 LONWORKS/IP Server, and the U10 and U20 USB Network Interfaces are included with the main LonScanner software installation.

---

## Activating the LonScanner Software

After a successful installation, the protocol analyzer will run in demonstration mode until you activate it. When operating in demonstration mode, the following dialog appears each time you start the protocol analyzer:



**Figure 1.2** LonScanner License Activation Dialog

To continue running in demonstration mode, click **Continue Eval**. When operating in demonstration mode, the protocol analyzer does not display every captured packet and displays only the first 20 packets of a saved or imported log file.

If you choose to operate in demonstration mode, the LonScanner License Activation dialog will appear every time you open the protocol analyzer. You can also access the LonScanner License Activation dialog and activate the LonScanner software while running in demonstration mode by selecting **Activate Product** from the **Help** menu, and then clicking **Activate**.

To activate the protocol analyzer from the LonScanner License Activation Dialog, select a product version from the list. Select **Prepaid Professional Edition** if you previously paid for a Model 33110-301 LonScanner Professional Edition with prepaid key. Select **Prepaid LNS Turbo Edition** if you previously paid for a Model 33110-302 LonScanner LNS Turbo Edition with prepaid key. You will have to supply the serial number supplied with your prepaid edition to order either of the prepaid editions. Select **LNS Turbo Edition** if you have an LNS Turbo Edition Server installed on your computer, and you do not have a prepaid key. Select **Professional Edition** if you do not have an LNS Turbo Edition Server installed on your computer, and you do not have a prepaid key. If you select **Professional Edition** or **Prepaid Professional Edition**, you can still use the protocol analyzer with an LNS 3 Server as described in the *Using LonScanner with LNS Turbo Edition* section on page 3.

When you have selected a product version, click **Copy Order Form to Clipboard**. Paste the order form that is copied to an email message or text editor document, and then email or fax the request to Echelon, using the email address or fax number on the form. Echelon will process the request and send you an activation key. Enter the activation key in the **Activation Key** box, and then click **Activate** to activate the software. Following this, you will have access to all LonScanner features.

---

## *Transferring a LonScanner Activation*

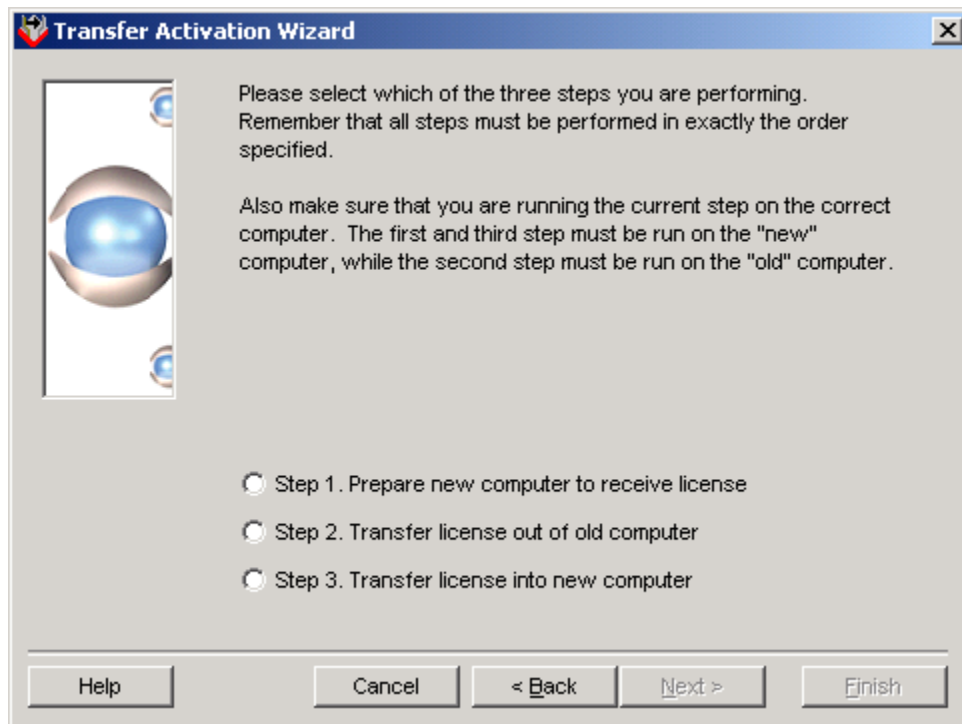
You can transfer your LonScanner activation to another computer. This will deactivate the protocol analyzer on your original computer, and then activate it on the new computer. To transfer activation, follow these steps:

1. Select **Activate Product** from the **Help** menu, and then click **Transfer Activation**. The window shown in Figure 1.3 opens.



**Figure 1.3** LonScanner Transfer Activation Wizard

2. Click **Next** to continue. The window shown in Figure 1.4 opens.



**Figure 1.4** LonScanner Transfer Activation Wizard Main Window

3. There are three steps you need to perform from this window. Steps one and three must be performed on the computer that initially contains the activation being transferred. The LonScanner software on this computer will no longer be activated once the transfer is complete. Step two must be performed on the computer that is to be activated. Consult the online help for more details on these steps.

---

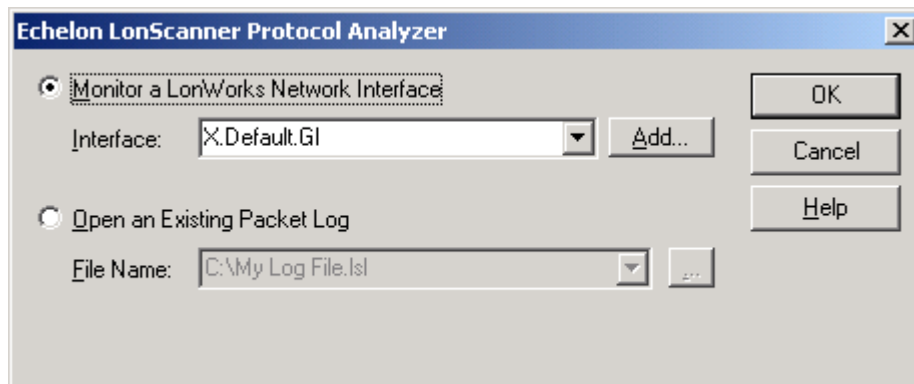
## Viewing Activation Status

You can access information about your LonScanner software at any time by selecting **About LonScanner Protocol Analyzer** from the **Help** menu. This opens a window displaying the version number and activation key of your LonScanner software. You can access additional activation information by selecting **Activate Product** from the **Help** menu, and then clicking **Display Activation Status**.

---

## Using the LonScanner Protocol Analyzer

Once you have installed the LonScanner software, you can begin monitoring IP-852 and 709.1 channels with the protocol analyzer and analyzing the data it collects. To start the protocol analyzer, select **Programs>Echelon LonScanner Protocol Analyzer>LonScanner Protocol Analyzer** from the Windows **Start** menu. If you have not yet activated the software, the LonScanner License Activation dialog shown in Figure 1.2 will open. Following that, the dialog shown in Figure 1.5 opens:



**Figure 1.5** Start-Up Dialog

You have two options to choose from:

- **Monitor a LONWORKS Network Interface.** Select this option to begin monitoring an IP-852 or 709.1 channel via a local or remote LONWORKS network interface. For more information, see the *Monitoring a Network Channel* section below.
- **Open an Existing Packet Log.** Select this option to view a packet log saved from a previous monitoring session. For more information, see *Opening an Existing Packet Log* on page 9.

## Monitoring a Network Channel

To monitor an IP-852 or 709.1 channel, follow these steps:

1. Select **Monitor a LonWorks Network Interface** on the Start-up dialog shown in Figure 1.5, and then select the network interface you plan to use from the **Interface** box.

If you are using an *i.LON* 100 Internet Server or an *i.LON* 600 LONWORKS/IP Server as your network interface, you will need to configure it with the LONWORKS Interfaces application in the Windows Control Panel before using it with the protocol analyzer. To access the application, click **Add** from the Start-up dialog. Consult the online help for instructions on how to use the application.

For special instructions you may need to follow when using network interfaces such as the *i.LON* 100 Internet Server, the *i.LON* 600 LONWORKS/IP Server, the PCC-10 and the PCLTA-20/21, see Appendix A, *Network Interfaces*.

2. Click **OK** to begin monitoring the selected channel. The main LonScanner window opens. A log entry will be added to the Packet Log tab for each packet the protocol analyzer receives from the channel. For an overview of the Packet Log tab and the rest of the main LonScanner window, see *Log Files Overview* on page 10.
3. To save the log file for later use at any point, select **Save Log As** from the **File** menu. This opens a dialog you can use to save the log file. Following that, you can re-open the log file at any point, as described in the next section.
4. To monitor additional channels, select **New Connection** from the **File** menu, or click **New** on the LonScanner toolbar. You can monitor up to 10 channels at once with the protocol analyzer.

See Chapter 2, *Logging Data*, for a description of how to use the protocol analyzer to perform additional tasks such as filtering incoming data or controlling the packet log

## Opening an Existing Packet Log

To open a packet log saved from a previous LonScanner or LonManager Protocol Analyzer session, select **Open an Existing Packet Log** on the Start-up dialog shown in Figure 1.5, and then select the log you want to open from the File Name box. Alternatively, you can browse for a packet log using the **Browse** button. LonScanner log files use a *.lsl* extension, and LonManager log files use a *.pal* extension.

Once you have selected a file, click **OK**. This opens the main LonScanner window. The log you selected will be displayed in the Packet Log tab. For an overview of the Packet Log tab and the rest of the main LonScanner window, see the *Log Files Overview* section.

You can open additional packet logs after you have started the protocol analyzer by selecting **Open Log** from the **File** menu.

## Log Files Overview

Once you have begun monitoring a channel or opened a saved log file with the protocol analyzer, the main LonScanner window shown in Figure 1.6 opens.

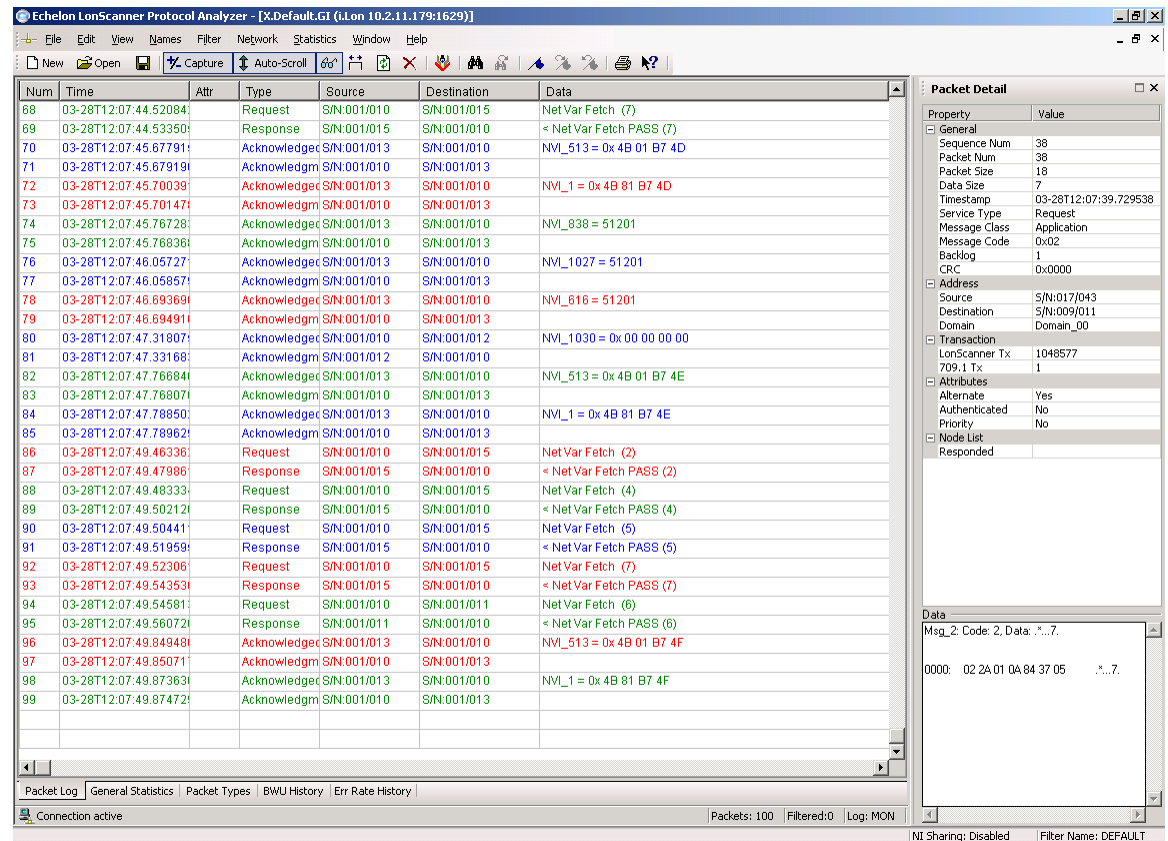


Figure 1.6 Main LonScanner Window

There are three main areas to the window shown in Figure 1.6:

- The Packet Log tab comprises the majority of the main LonScanner window. The Packet Log tab contains a series of log entries, one for each packet that the protocol analyzer has collected from the channel. The log entries are listed sequentially by order of the time each packet was received. Consult the online help for descriptions of the data fields listed for each packet.

When you are actively monitoring a channel, you can also select the General Statistics, Packet Types, Bandwidth Utilization History, and Error Rate History tabs at the bottom of the window to view statistics collected from the channel during your log session. For more information on these tabs, and for information regarding how you can configure the protocol analyzer's behavior during an active log session, see Chapter 2, *Logging Data*.

- The Packet Detail pane to the right of the Packet Log tab lists detailed information about the packet currently selected in the Packet Log. Click a packet in the Packet Log to select it and view its details in the Packet



Detail pane. Consult the online help for descriptions of the data fields listed for each packet in the Packet Detail pane.

- The menus and toolbar above the Packet Log tab and Packet Detail pane allow you to determine how the protocol analyzer will collect data from the channel, and to organize and analyze the data once it has been collected. For an overview of the features provided by each menu, consult the next section, *Using the LonScanner Menus, Toolbar, and Status Bar*.

---

## *Using the LonScanner Menus, Toolbar, and Status Bar*

This section provides a brief introduction to the features you can access using the LonScanner menus and toolbar. These features are described in more detail later in the following chapters, and in the LonScanner online help.

### **LonScanner Menus**

Table 1.1 lists the LonScanner menus, and describes the functionality provided by each menu. For detailed descriptions of each menu option, see Chapters 2 and 3 of this document, and the LonScanner online help.

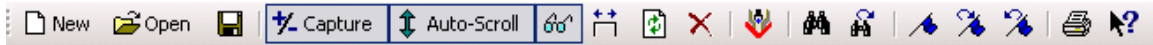
**Table 1.1** LonScanner Menus

<b>Menu</b>	<b>Description</b>
File Menu	Use the File menu to open new connections to local and remote channels, and to open pre-existing log files. You can also use the File menu to print and export log files, and to set the general logging preferences that affect how the protocol analyzer will create and manage log files.
Edit Menu	Use the Edit menu to search through log files, and to bookmark specified log entries as being of interest.
View Menu	Use the View menu to format how the data in the Packet Log will be displayed. This includes selecting which data fields will be displayed in the Packet Log for each log entry, how each data field will be formatted, and what color and font will be used to display each log entry. You can also use the View menu to hide or display the LonScanner toolbar, status bar and Packet Detail pane.
Names Menu	Use the Names menu to import or edit device and network variable names for the channel you are monitoring.
Filter Menu	Use the Filter menu to create and activate LonScanner filters, which you can use to select which packets the protocol analyzer will record into a log file, and which ones it won't record.

Menu	Description
Network Menu	When you are actively monitoring a channel with the protocol analyzer, you can use the Network menu to enable and disable capture mode and monitor mode, and to clear all data from the currently selected log.
Statistics Menu	When you are actively monitoring a channel with the protocol analyzer, you can use the Statistics menu to configure how the protocol analyzer will gather and display network statistics.
Window Menu	Use the Window menu to arrange the log files and windows you have open.
Help Menu	Use the Help menu to access information regarding the version and activation status of the LonScanner software you are using, and to access the LonScanner online help. You can also access the LonScanner Transfer Activation Wizard from this menu.

## LonScanner Toolbar


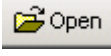

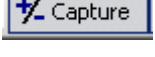
The LonScanner toolbar provides quick access to commonly used menu options. The LonScanner toolbar is shown in Figure 1.7.
















**Figure 1.7** LonScanner Toolbar

You can click a button on the toolbar to use the feature provided by that button. Table 1.2 lists the buttons, and describes the features each one provides access to.

**Table 1.2** LonScanner Toolbar Buttons

Button	Description
	Opens a new connection to a channel and starts a new Packet Log.
	Opens an existing log file.
	Saves the log file currently displayed in the Packet Log tab.
	Enables or disables the recording of packets into the current log file when LonScanner is actively monitoring a channel.

Button	Description
	Enables or disables automatic scrolling to the most recently collected packets in the Packet Log tab when you are actively monitoring a channel and recording packets into a log file.
	Enables or disables automatic refreshing of the Packet Log tab when you are actively monitoring a channel and recording packets into a log file. When disabled, you will have to manually refresh the Packet Log by clicking the Refresh button, or by selecting <b>Refresh Display</b> from the <b>View</b> menu, to see the most recently collected packets in the Packet Log tab.
	Adjusts the column widths of the Packet Log tab so that as much of the data stored in each column as possible will be displayed on the screen.
	Refreshes the information shown in the Packet Log and Statistics tabs when you are actively monitoring a channel and recording packets into a log file.
	Clears all data from the log file currently shown in the Packet Log tab.
	Starts the LNS Names Import Wizard, which you can use to import device and network variable names from an LNS database.
	Finds an occurrence of a string in the Packet Log tab.
	Finds the next occurrence of a string in the Packet Log tab.
	Creates a bookmark. You can use bookmarks to mark certain log entries as being of interest.
	Scrolls the Packet Log tab to the next bookmarked packet.
	Scrolls the Packet Log tab to the previous bookmarked packet.
	Prints the log file currently displayed in the Packet Log tab.

Button	Description
	Provides context-sensitive online help. After clicking the button, click an area of the LonScanner window for information on how that part of the software works.

## LonScanner Status Bar

The Status Bar is at the bottom of the LonScanner Protocol Analyzer window. It provides the following information:

- A status message that provides a brief description of the currently selected menu items and buttons.
- The total number of packets recorded into log file.
- The number of packets that have been filtered.
- The logging state of the currently selected active log.
- Whether or not network interface sharing is enabled or disabled. For more information on network interface sharing, see Chapter 1 of the *LonScanner Protocol Analyzer User's Guide*.

---

## Document Roadmap

The remaining chapters of this document describe other tasks you can perform when monitoring channels and reading log files with the protocol analyzer. These chapters are summarized below:

- Chapter 2, *Logging Data*. This chapter describes how to configure the protocol analyzer's behavior while it collects packets from an IP-852 or 709.1 channel. This begins with a discussion of how to set general logging preferences, and how to use LonScanner filters to determine what packets the protocol analyzer will record into log files, and what packets it will ignore. This is followed by a discussion of other features you can use while actively monitoring a channel, such as how to view the channel statistics compiled by the protocol analyzer. Chapter 2 also describes how to import and edit device and network variable names.
- Chapter 3, *Analyzing Packet Log Details*, describes how you can organize and analyze the information stored in your log files. This begins with a discussion of how to search a log file for the log entry for a particular packet, and how to use bookmarks and color-coding features to mark packets of interest. This chapter also describes the Format menu, which you can use to determine the format of the various data fields that the protocol analyzer displays.
- Chapter 4, *Example Logs*, describes several example logs and demonstrates how you could search those logs for log entries for specific packets.

Appendix A, *Network Interfaces*, describes the network interfaces you can use to connect to an IP-852 or 709.1 channel with the protocol analyzer, and lists any special guidelines to follow when using a particular network interface.



# 2

## Logging Data

This chapter describes how you can log packets with the protocol analyzer, and how you can view statistics related to those packets. The first part of this chapter describes how you can configure the behavior of the protocol analyzer while it monitors a channel and collects packets. This includes topics such as setting logging preferences, using the Capture and Auto-Scroll features, and filtering packets.

The second part of this chapter describes how to access statistics that are available when you monitor a channel with the protocol analyzer. This includes data related to bandwidth utilization, the types of packets traveling on the network, and other network statistics.

This chapter also describes how you can use names to identify the devices and network variables on the channel you are monitoring.

---

## Configuring the LonScanner Protocol Analyzer

This section describes how you can configure the behavior of the protocol analyzer while it monitors a channel. This includes the following topics:

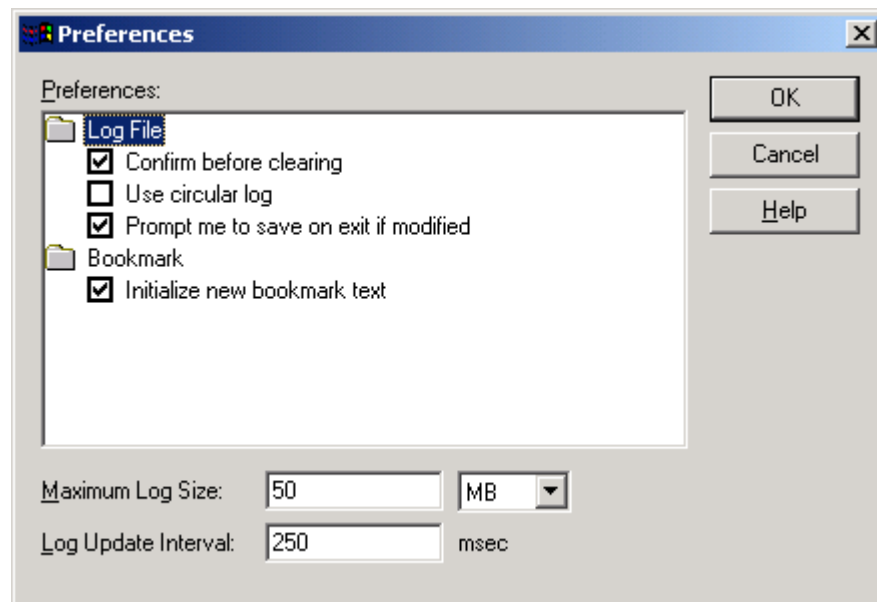
- *Setting Logging Preferences.* This section describes how you can use the LonScanner Preferences dialog to control how the protocol analyzer collects and record packets from a channel.
- *Filtering Packets.* You can use filters to select which packet types will be recorded into the log file. This section describes how to create, configure and activate filters.
- *Setting the Capture and Monitor Modes.* When actively monitoring a channel with the protocol analyzer, the Capture and Monitor modes determine whether the packets collected from the channel will be recorded into the log file, and whether the protocol analyzer should automatically refresh the Packet Log display as data is added to the log. This section describes how to enable these features.

---

## Setting Logging Preferences

You can use the LonScanner Preferences dialog to determine how the protocol analyzer will collect and display data during a monitoring session. To do so, follow these steps:

1. From the **File** menu, select **Preferences**. The dialog shown in Figure 2.1 opens.



**Figure 2.1** LonScanner Preferences Dialog

2. Configure the fields on the LonScanner Preferences Dialog. Consult the dialog's online help for detailed descriptions of these fields.

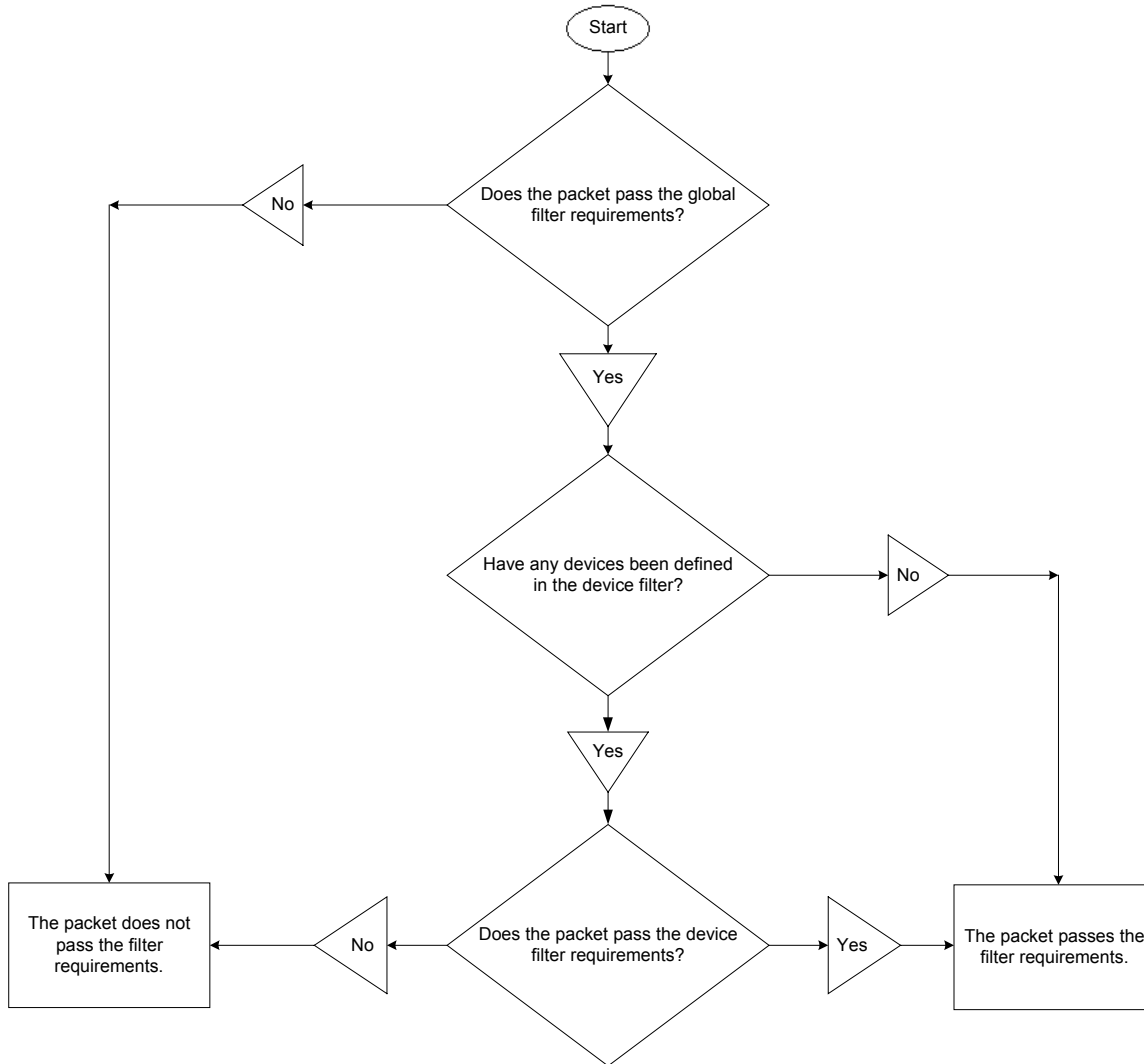


3. Click **OK** to save your changes.

---

## Filtering Packets

You can use filters to select the types of packets that will be recorded into the log file. You can use two types of filters—a *global filter* that applies to all packets, and a *device filter* that applies to packets sent to and from specific devices on the network. When the protocol analyzer receives a packet from the channel, it uses the global and device filter to determine if the packet passes the filter requirements. Figure 2.2 shows the steps it follows to do so:



**Figure 2.2** Filtering Packets

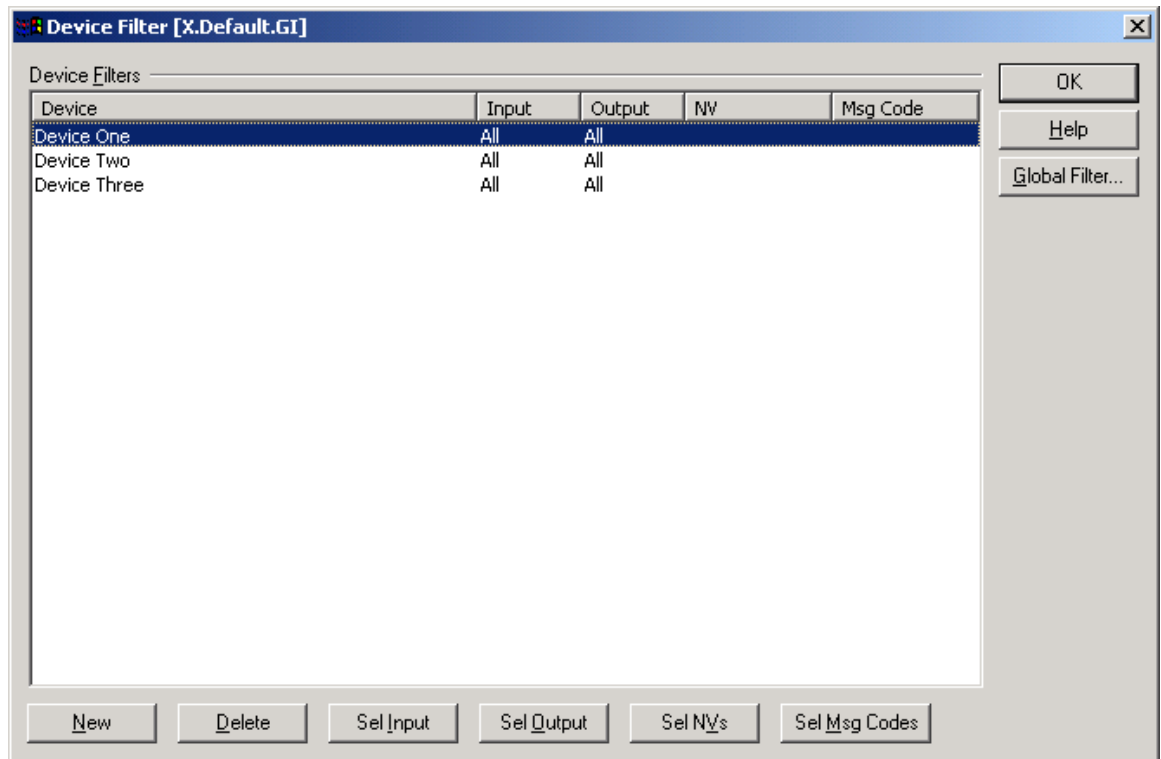
The following sections describe how to initially configure the global and device filters. As you review this section, you should be aware that each time you modify the filter settings for a channel, the protocol analyzer automatically saves those settings. As a result, every time you connect to a channel, the protocol analyzer will use the filter settings defined for the channel the last time it was used.

**NOTE:** If desired, you can also filter packets with a custom filter file. To create and use a custom filter file, you will need to modify the code found in the `lscustomfilter.cpp` file in the `Example Custom Filter` subdirectory of your LonScanner installation directory. For details on this, consult the Knowledge Base on Echelon's website at [www.echelon.com](http://www.echelon.com).

## Configuring the Global and Device Filters

To configure the device filter and the global filter, follow these steps:

1. From the **Filter** menu, select **Edit Filters**. The dialog shown in Figure 2.3 opens.



**Figure 2.3** Device Filter Dialog

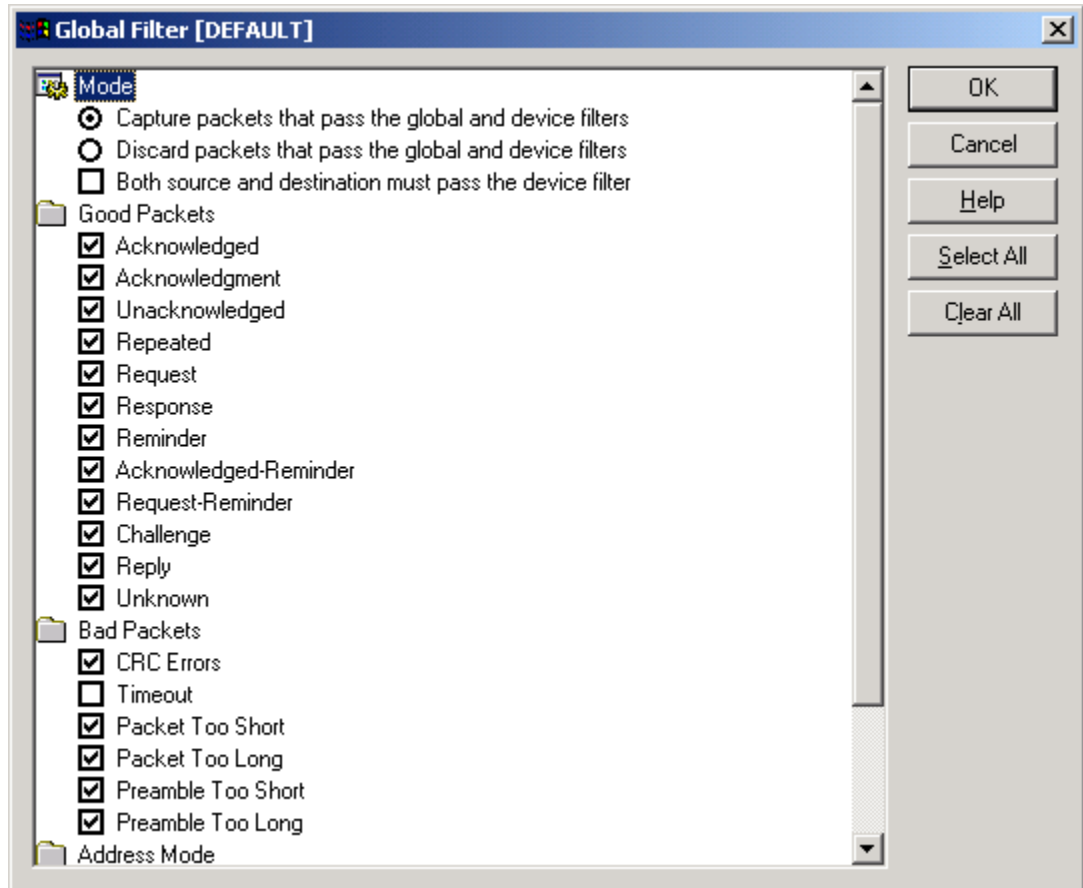
2. To filter packets addressed to or from a specific device, click **New**. The **Select a Device to Add** dialog opens, which lists all the devices defined in the current names file. Select the device you want to add to the filter, and then click **Add**. For more information on names files, see *Using Names* on page 32.

You will return to the Device Filter dialog shown in Figure 2.3, and the newly added device will be listed in the Device list on the dialog.

3. If you added a device to the filter in the previous step, all packets addressed to or from the device will pass the device filter by default. You can refine whether you want all packets or network variable packets addressed to the device, and whether or not you want all packets or network variable packets sent by the device, to pass the device filter. To refine the filter, edit the filter configuration for the device that you just added by selecting it in the Device Filters list, and then clicking any of the five buttons at the bottom of the

Device Filter dialog. These buttons are listed and described below. Consult the online help for more detailed instructions on each of them.

- Click **Delete** to remove the selected device from the device filter.
  - Click **Sel Input** to open the Input Mode dialog. You can use this dialog to specify whether or not packets sent to the selected device should pass the device filter requirements.
  - Click **Sel Input** to open the Output Mode dialog. You can use this dialog to specify whether or not packets sent from the selected device should pass the device filter requirements.
  - Click **Sel NVs** to open the **Select Network Variables** dialog. You can use this dialog to determine which network variable update messages sent to and from the selected device should pass the device filter requirements. You must define the network variable types in the current names file before adding them to the device filter. For more information on names files, see *Using Names* on page 32.
  - Click **Sel Msg Codes** to open the **Select Message Codes** dialog. You can use this dialog to determine which message codes sent to and from the selected device should pass the device filter. You must define the message codes in the current names file before adding them to the device filter. For more information on names files, see *Using Names* on page 32.
4. Repeat steps 2 and 3 until you add all the devices you want to the device filter. When doing so, remember that the filter settings you define for each device apply to that device only, and not to the other devices in the filter. You can bypass these steps if you do not want to filter packets based on their source or destination device.
  5. Configure the global filter settings for the filter file. Click **Global Filter**. The dialog shown in Figure 2.4 opens.



**Figure 2.4** Global Filter Dialog

6. Click **Capture Packets that Pass the Global and Device Filters** to record packets that pass the requirements of the global and device filters into the Packet Log. Click **Discard Packets that Pass the Global and Device Filters** to record packets that don't pass the requirements into the Packet Log.
7. Select the **Both Source and Destination Must Pass the Device Filter** check box to check each packet against the filter settings for both the source device and the destination device. This allows you to filter traffic between a specified pair of devices.
8. Select which packet types should pass the global filter by selecting or clearing the appropriate check boxes. You can select all packet types by clicking **Select All**, and clear all packet types by clicking **Clear All**. For descriptions of each of the packets types listed on the Global Filter dialog, consult the online help.
9. Click **OK** to save your changes. This returns you to the Device Filter dialog shown in Figure 2.3.
10. Click **OK**. The protocol analyzer will now use the updated filter configuration to filter all incoming packets. You can edit the configuration of the filter file again later by selecting **Edit Filters** from the **Filter** menu, and repeating steps 2 through 10.

You can select **Set to Defaults** from the **Filter** menu at any time to revert the filter back to the default filter settings.

## Importing Filter Settings From a Channel

As noted earlier in this section, the protocol analyzer automatically saves the filter settings you define for a channel each time they are modified. So when you modify the filter settings for a channel, the protocol analyzer will use those settings the next time you connect to the channel.

You can import the filter settings for a given channel into another channel. This may be useful if you are using multiple network interfaces to monitor a channel or group of channel, and want them all to use the same filter settings. To do so, follow these steps:

1. Select **Import From Channel** from the **Filter** menu. A window opens, reminding you that this will overwrite any filter settings defined for the channel before the import was performed.
2. Click **Yes** to continue. A dialog opens, allowing you to select the network interface you are using to connect to the channel containing the filter settings you want to import.
3. Select the network interface from the **Interface** box, or click **Add** to add a new network interface, and then click **OK**.

A window will open to inform you when the filter settings have been imported. Click **Yes** to continue. The protocol analyzer will then use the imported filter settings.

## Saving Filter Settings For Later Use

You can save the global and device filter settings you create into a filter file so that you can return to those settings later, without having to reconfigure the filter and undo any subsequent changes later. To save the current global and device filter settings into a filter file, select **Save Copy** from the **Filter** menu.

Once you have saved a filter file, you can create or import new filter settings as described in the previous sections, and then restore the saved filter settings at any point. To restore your saved filter settings later, select **Import From Filter File** from the **Filter** menu, and then open your saved filter file. The protocol analyzer will then use the filter settings defined in the saved filter file. Note that these settings will overwrite any filter settings defined for the channel before the import was performed.

You can save any number of filter files, and import them at any given time. You may find this more convenient than continually editing the same filter file, or continually create new filter files from scratch.

---

## *Setting the Capture and Monitor Modes*

You can use the Capture and Monitor modes to control whether or not the packets collected from the channel are recorded into the log file, whether or not

the Packet Log tab is refreshed as packets are received, and whether or not the Packet Log tab is automatically scrolled to display incoming packets.

To record packets collected from the network into the current log file, click the Capture button on the LonScanner toolbar, or select **Capture Mode** from the **Network** menu.

To automatically update the Packet Log tab as packets are collected from the channel, click the Monitor button on the LonScanner toolbar or select **Monitor Mode** from the **Network** menu. When disabled, you will have to manually refresh the Packet Log tab whenever you want to see the most recently collected packets by clicking the Refresh button on the LonScanner toolbar, or by selecting **Refresh Display** from the **View** menu.

You can check the status bar to determine whether or not monitor mode and capture mode are enabled. For more information on the status bar, see *Using the LonScanner Menus, Toolbar, and Status Bar* on page 11.

To automatically scroll the Packet Log tab to the most recently collected packets, click the Auto-Scroll button on the LonScanner toolbar, or select **Auto-Scroll** from the **View** menu.

---

## Viewing Channel Statistics and Trend Graphs

You can view channel statistics and trend graphs when you are monitoring a channel to assess overall channel health at a specific point in time, or over a longer period of time. To view channel statistics or trend graphs, click the tabs at the bottom of the main LonScanner window. These tabs are introduced below, and described in more detail in the following sections. These tabs are not available if you are viewing a saved packet log.

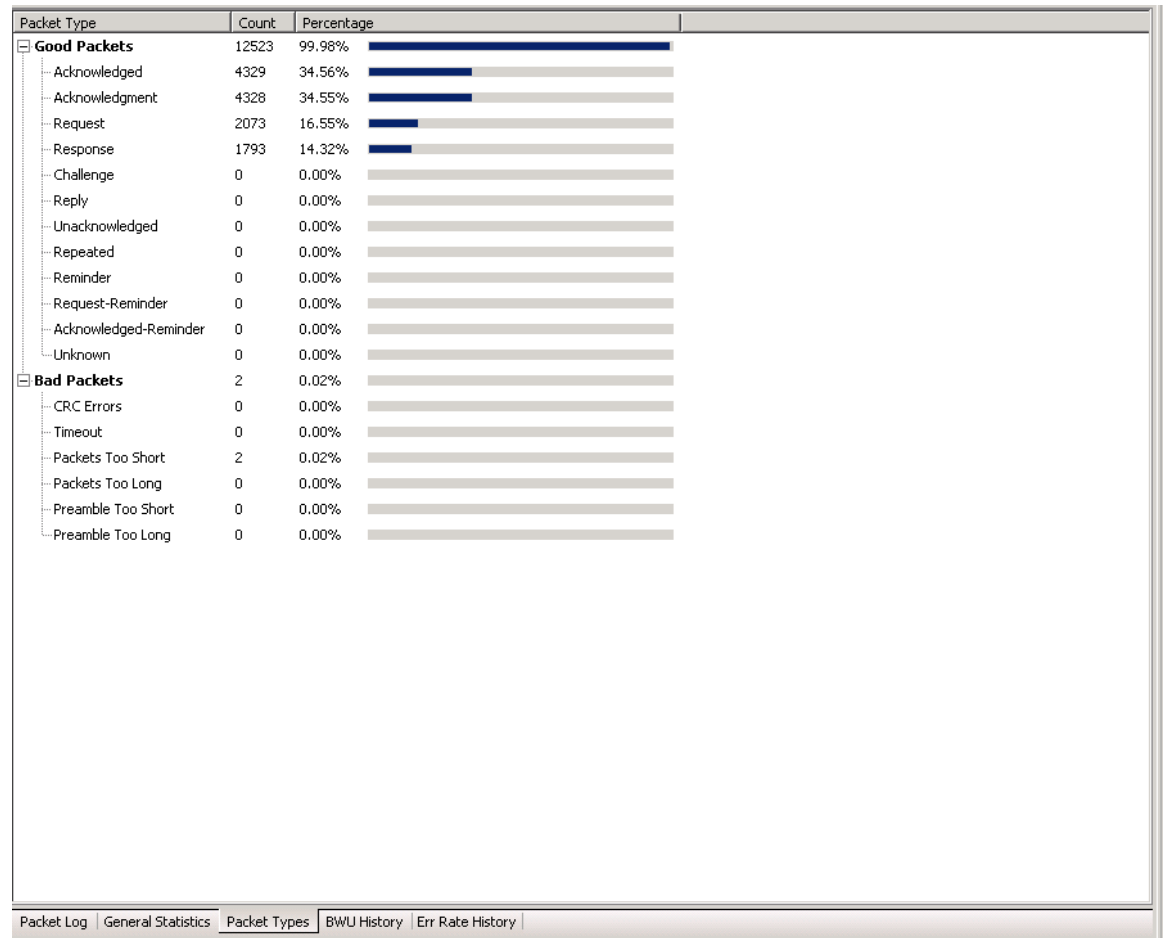
- **General Statistics.** Select the General Statistics tab to view channel statistics such as the total packets received during the log session, the average packet size received, and the number of packets received per second. The General Statistics tab also displays maximum and cumulative statistics, such as the maximum and average bandwidth utilization percentage and the maximum and average error rate during the session.
- **Packet Types.** Select the Packet Types tab to view a breakdown of the packet types collected from the monitored channel. For each packet type, the total number of packets of that type that has been collected from the monitored channel is listed, as well as the percentage of the total packet count that number makes up.
- **BWU (Bandwidth Utilization) History.** Select the BWU History tab to view a trend graph displaying the bandwidth utilization (by percentage) over time on the monitored channel.
- **Error Rate History.** Select the Err Rate History tab to view a trend graph displaying the percentage of invalid packets received from the monitored channel over time.

**NOTE:** The data displayed on the statistics tabs only accounts for packets recorded into the current log file. It does not account for packets that were discarded because they did not meet the current filter requirements.

## Viewing Bandwidth Utilization by Packet Types

Select the **Packet Types** tab to view a breakdown of the packet types collected from the monitored channel. The packet types are grouped as good (valid) and bad (invalid) packets. For each packet type, the total number of collected packets of that type is listed. The percentage of the total packet count that makes up is also listed. Consult the online help for descriptions of the packet types listed on the Packet Types tab.

Figure 2.5 shows a sample Packet Types tab.



**Figure 2.5** Packet Types Tab

In Figure 2.5, all the packets received during the current session have been valid packets. The protocol analyzer will adjust the packet count and percentage figures as more packets are received from the channel. You can control the rate at which the statistics on the display are updated by setting the general update interval with the statistics options tabs. For more information on this, see *Setting Statistics Options* on page 28.

---

## Viewing Bandwidth Utilization History

Select the **BWU History** tab to view a trend graph displaying the bandwidth utilization (by percentage) on the monitored channel. A well-designed network will not have any peaks in bandwidth utilization that are over 80%. Figure 2.6 shows a sample bandwidth utilization trend graph.



**Figure 2.6** Bandwidth Utilization History Tab

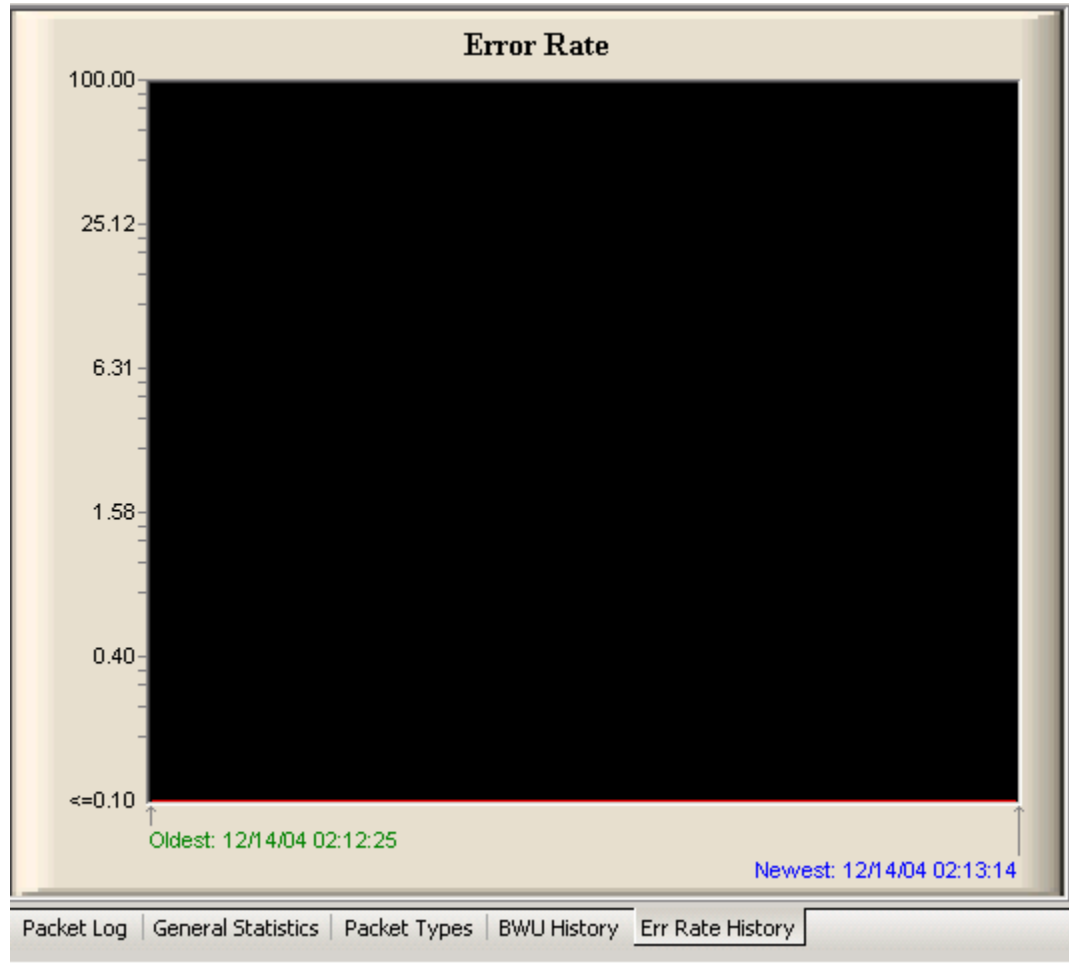
The sample shown in Figure 2.6 includes two timestamps. These are the times that the oldest and newest update points on the trend graph were recorded. You can set the rate at which this display will be updated, as well as the number of points that will be displayed on the chart, with the statistics options dialogs. For more information on this, see *Setting Statistics Options* on page 28.



---

## Viewing Error Rate History

Select the **Err Rate History** tab to view a trend graph displaying the percentage of invalid packets received from the monitored channel. A well-designed network will not have any peaks in error rate of over 4%. Figure 2.7 shows a sample Error Rate History tab.



**Figure 2.7** Error Rate History Tab

In Figure 2.7, two timestamps are shown. These are the times that the oldest and newest update points on the trend graph were recorded. You can set the rate at which this display will be updated, as well as the number of points that will be displayed on the chart, with the statistics options tabs. For more information on this, see *Setting Statistics Options* on page 28.

---

## Viewing General Statistics

Select the **General Statistics** tab to view a variety of network statistics including the total number of packets collected during the current session, the average packet size, and the number of packets received per second. You can also view maximum and cumulative information, such as the maximum and average bandwidth utilization percentage and the maximum and average error rate

during the session. Consult the online help for descriptions of all of the data fields displayed on the General Statistics tab.

Figure 2.8 shows a sample General Statistics tab.

Name	Property
<b>Configuration</b>	
Update State	Update ON
Update Interval	2 sec(s)
<b>Time</b>	
Start Time	15:42:19.604
Previous Update Time	16:12:40.443
Update Time	16:12:42.446
<b>Snapshot Statistics</b>	
<b>Rate</b>	
Bandwidth Utilization	2.67%
Error Rate	0%
Packets Per Sec	5.99
Priority Packets Per Sec	0
Non-Priority Packets Per Sec	5.99
Filtered Packets Per Sec	0
Error Packets Per Sec	0
Average Packet Size	12.50 bytes
<b>Maximum</b>	
Max Bandwidth Utilization	5.94%
Max Error Rate	0%
Max Average Packet Size	18 bytes
Max Packets Per Sec	12.98
Max Priority Packets Per Sec	0
Max Non-Priority Packets Per Sec	12.98
Max Filtered Packets Per Sec	0
Max Error Packets Per Sec	0
<b>Cumulative Statistics</b>	
Elapsed Time	00:30:22.841
<b>Average</b>	
Bandwidth Utilization	2.67%
Error Rate	0%
Average Packet Size	12.88 bytes
Packets Per Sec	5.95
Priority Packets Per Sec	0
Non-Priority Packets Per Sec	5.95
Filtered Packets Per Sec	0
Error Packets Per Sec	0
<b>Total</b>	
Total Packets	10,843
Total Priority Packets	0

**Figure 2.8** General Statistics Tab

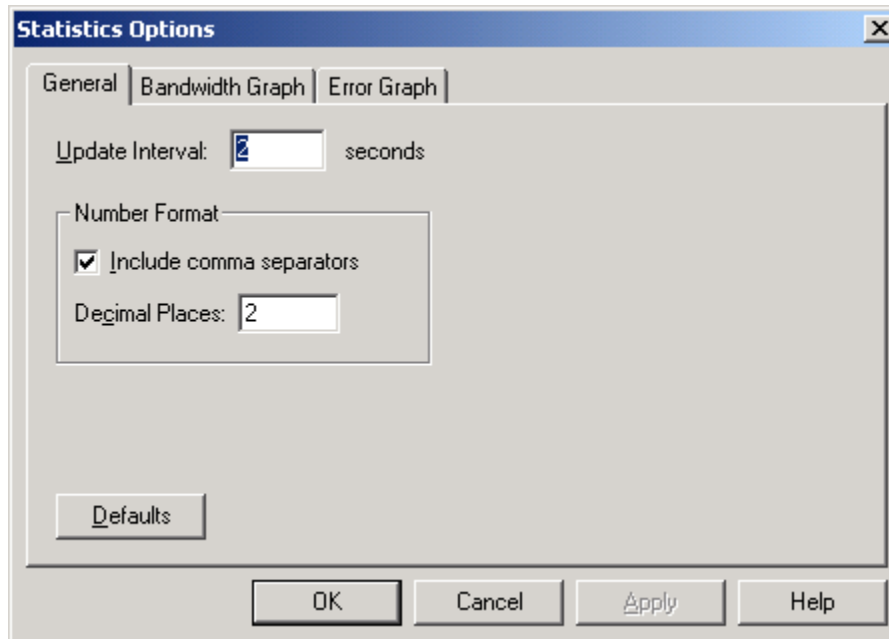
You can control the rate at which the statistics on the display are updated by setting the general update interval with the statistics options dialogs. For more information on this, see *Setting Statistics Options* on page 28.

---

## Setting Statistics Options

When using the statistics tabs, you can configure the statistics options, and you must select the channel type for the channel you are monitoring. This affects how the protocol analyzer will collect data from the network, and how that data will be displayed. To set the statistics options, follow these steps:

1. From the **Statistics** menu, select **Statistics Options**. The tab shown in Figure 2.9 opens.



**Figure 2.9** General Tab

2. Configure the settings on the General tab. These settings determine the interval at which the statistics display will be updated, and the format that will be used to display the statistics. Consult the online help for detailed descriptions of these fields.
3. Next, select the **Bandwidth Graph** tab.

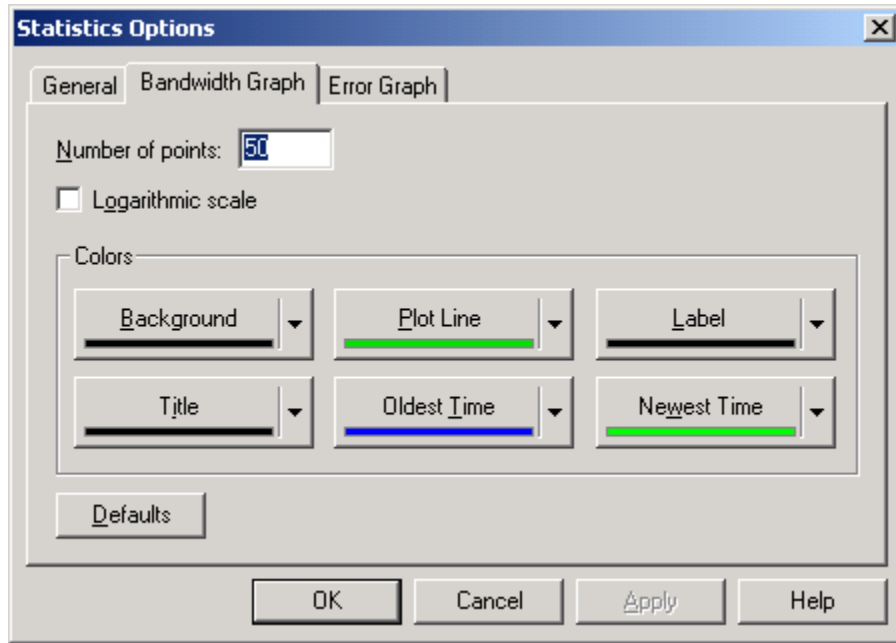


Figure 2.10 Bandwidth Graph Tab

4. Configure the settings on the Bandwidth Graph tab. These settings determine the number of historical points that will be displayed on the Bandwidth Utilization chart, whether or not logarithmic scaling should be used for the chart, and the colors that will be used to display the chart. Consult the online help for detailed descriptions of these fields.
5. Next, select the **Error Graph** tab.

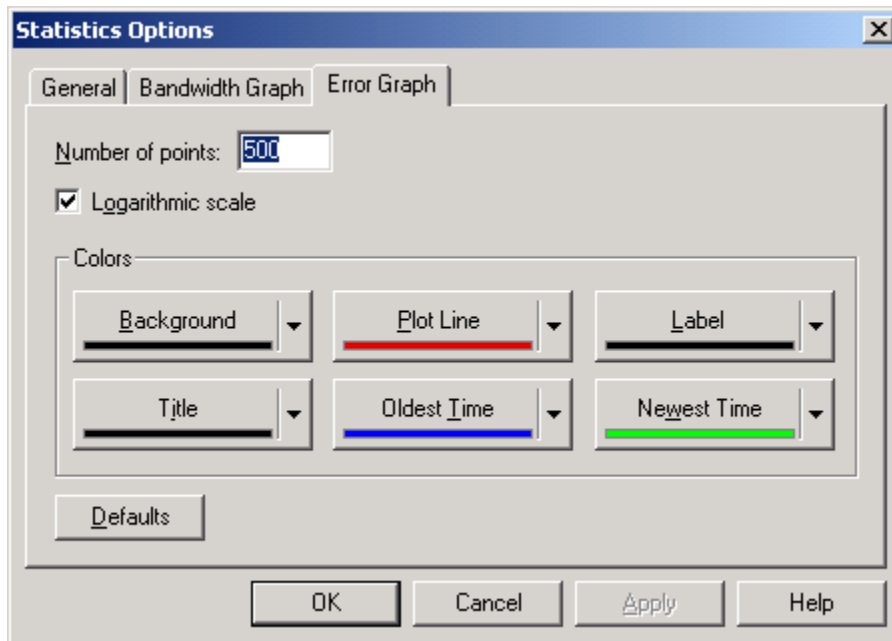
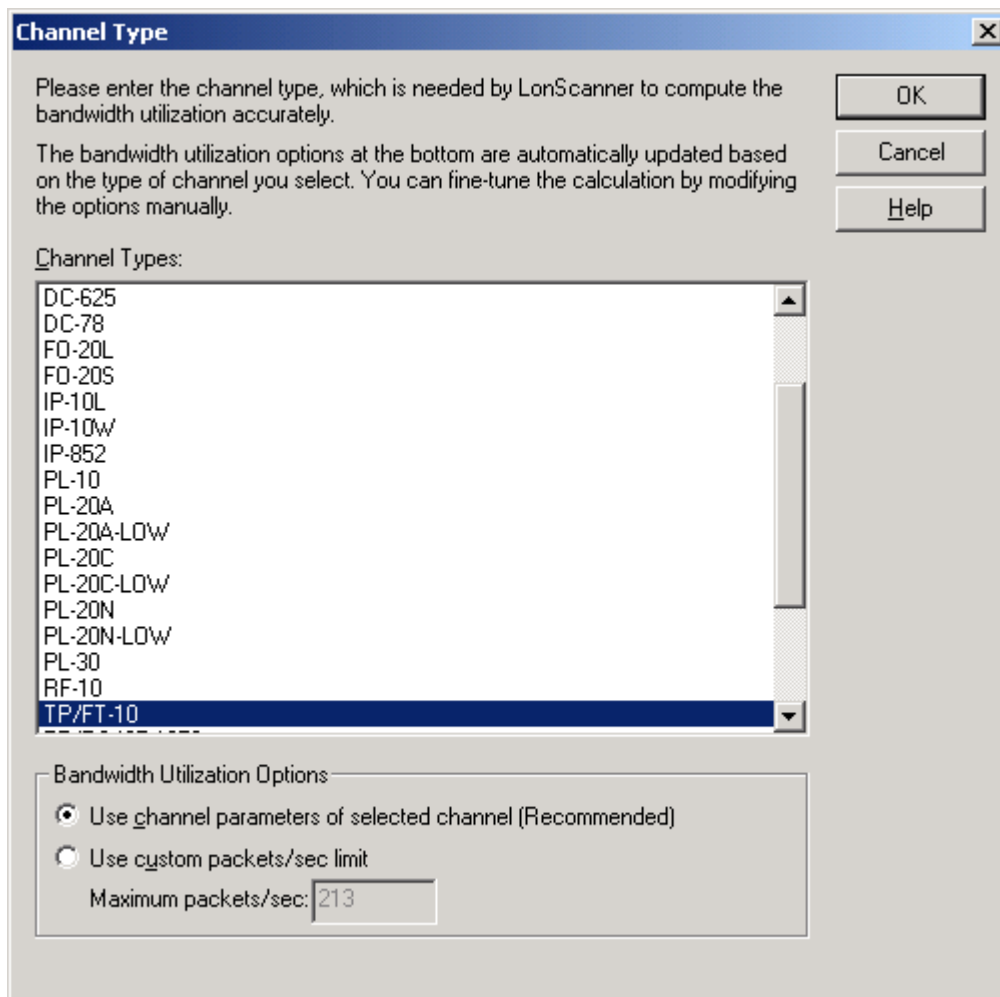


Figure 2.11 Error Graph Dialog

6. Configure the settings on the Error Graph tab. These settings determine the number of historical points that will be displayed on the Error Rate History chart, whether or not logarithmic scaling should be used for the chart, and the colors that will be used to display the chart. Consult the online help for detailed descriptions of these fields.
7. Click **OK** to save your changes and close the dialog. Or, click **Apply** to save your changes and continue editing the statistics options settings. You can click **Defaults** at any time to return the settings to their default values.
8. To choose the channel type you are monitoring, select **Channel Type** from the **Statistics** menu. The dialog shown in Figure 2.12 opens.



**Figure 2.12** Channel Type Dialog

9. Select the channel type and bandwidth utilization options for the channel you are monitoring, and then click **OK**. These settings are important for calculating bandwidth utilization, since the available bandwidth is determined by the channel type.

When you begin monitoring a channel, the protocol analyzer will attempt to determine the channel type automatically. If the protocol analyzer cannot do so, this dialog will open to remind you to select the correct channel type.

---

## Using Names

You can assign names to devices, network variables, domains, groups, and message codes on the channel you are monitoring. The domain and group assignments associated with a network are used to determine which devices a given packet should be sent to, and to identify which part of the network a device belongs to. For a more detailed overview of domains, groups and the rest of the ANSI/CEA-709.1 control networking protocol, consult the *Introduction to the LONWORKS System* document. You can view this document by clicking the Windows Start menu, opening the Echelon LonScanner Protocol Analyzer program folder, and then clicking **Introduction to LonWorks**

Names are not included in the packets sent over the network, nor are they saved in log files. However, you can still use names to identify the devices that are sending or receiving messages on the channel you are monitoring, to identify the network variables that are being updated by these messages, or to identify the domains and groups that exist on your network.

When you start a LonScanner session, you can import names from an LNS database or from another channel. You can also manually add and customize names. You can import and modify names at any time—such as when you are actively monitoring a channel or when you are viewing a saved log file.

When you import or create a set of names for a channel, the protocol analyzer will save those names in a *channel names file*. These names will be used each time you open a connection to that channel, even after you have stopped and restarted the protocol analyzer. The channel names file is updated and saved automatically each time you modify the names that apply to a channel.

You can also save the names into a *local names file* on your computer once you have imported or created a set of names to use. Following that, you can import the names saved in the file and use them at any time. This may be useful if you are using multiple network interfaces to monitor the same network. You could define one names file containing all the names for the network, and then import the names from that file whenever you start a LonScanner session with any of the network interfaces on that network. You can also copy the local names file to another computer with the protocol analyzer, and then import the names file on the second computer.

This section describes these options. It includes the following major topics:

- *Importing Names.* This section describes how to import names from an LNS database, a channel names file, or a local names file.
- *Creating and Customizing Names.* This section describes how to edit any names you have imported, and how to create new names from scratch.
- *Managing Names Files.* The previous sections in this chapter describe how to build a set of names by importing or manually creating them. This section describes how to save those names for future use by saving them into a names file.

---

## Importing Names

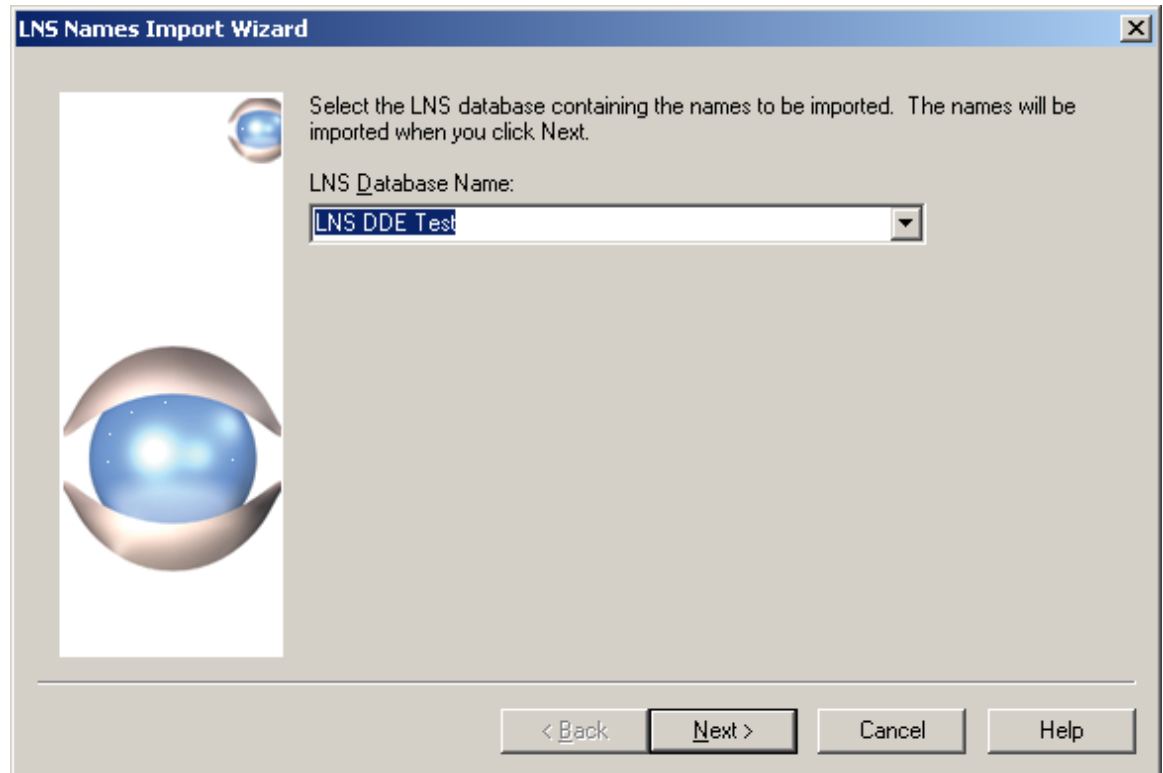
This section describes how to import names from an LNS database, a local names file, or a channel names file.

### Importing Names from an LNS Database

You can import the names stored in an LNS database for your network. The network database must be stored on the same computer you are running the protocol analyzer on, and you must have an LNS Turbo Edition Server or an LNS 3 Server installed on the computer.

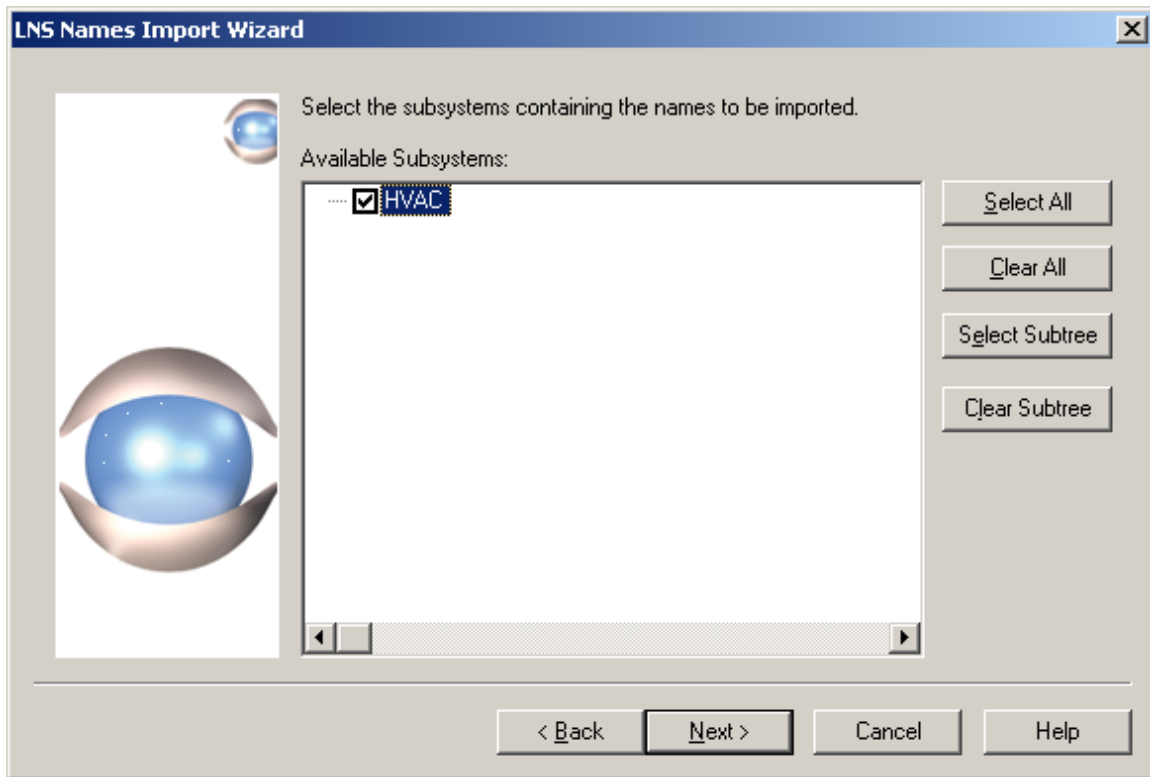
To import names from an LNS database, follow these steps:

1. From the **Names** menu, select **Import from LNS Database**. The window shown in Figure 2.13 opens.



**Figure 2.13** LNS Names Import Wizard – First Window

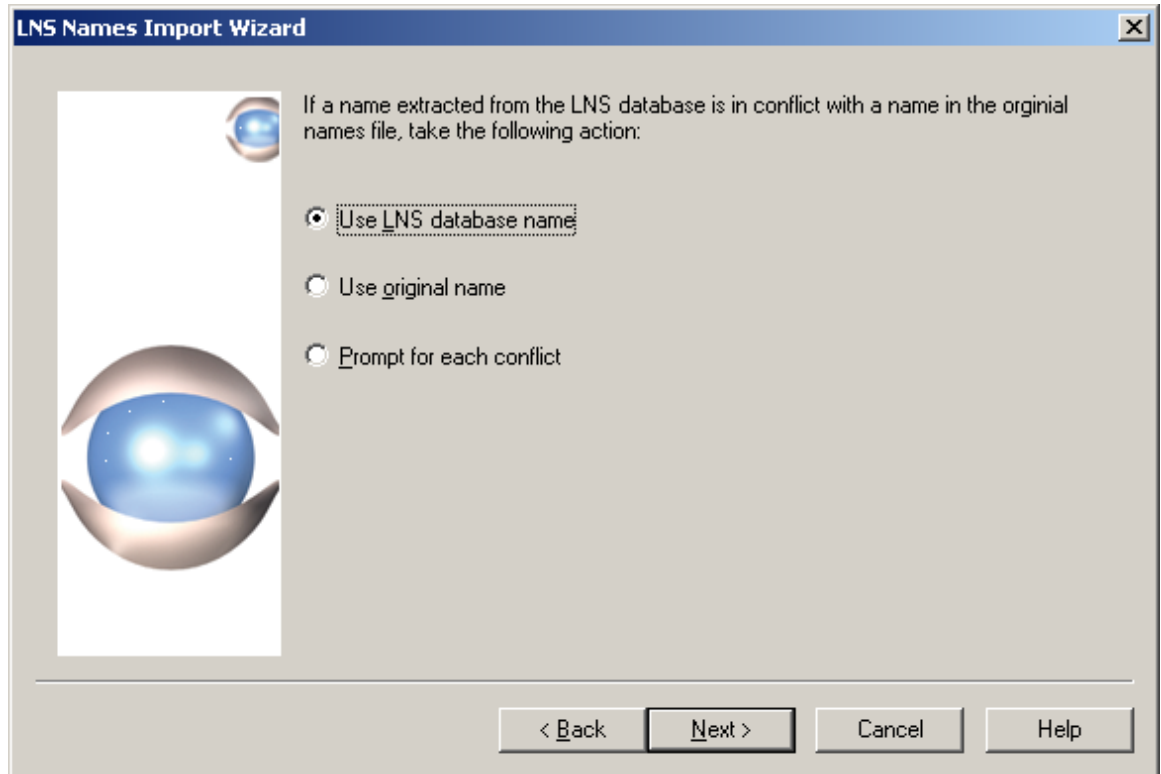
2. Select the database containing the names you want to import from the LNS Database Name box, and then click **Next**. The dialog shown in Figure 2.14 opens.



**Figure 2.14** LNS Names Import Wizard – Window Two

3. Select the subsystem or subsystems containing the names that you want to import from the Available Subsystems list. Alternatively, you can click **Select All** to select all subsystems, or click **Select Subtree** to select all child subsystems of the currently selected subsystem. When you have made a choice, click **Next** to continue. The window shown in Figure 2.15 opens.



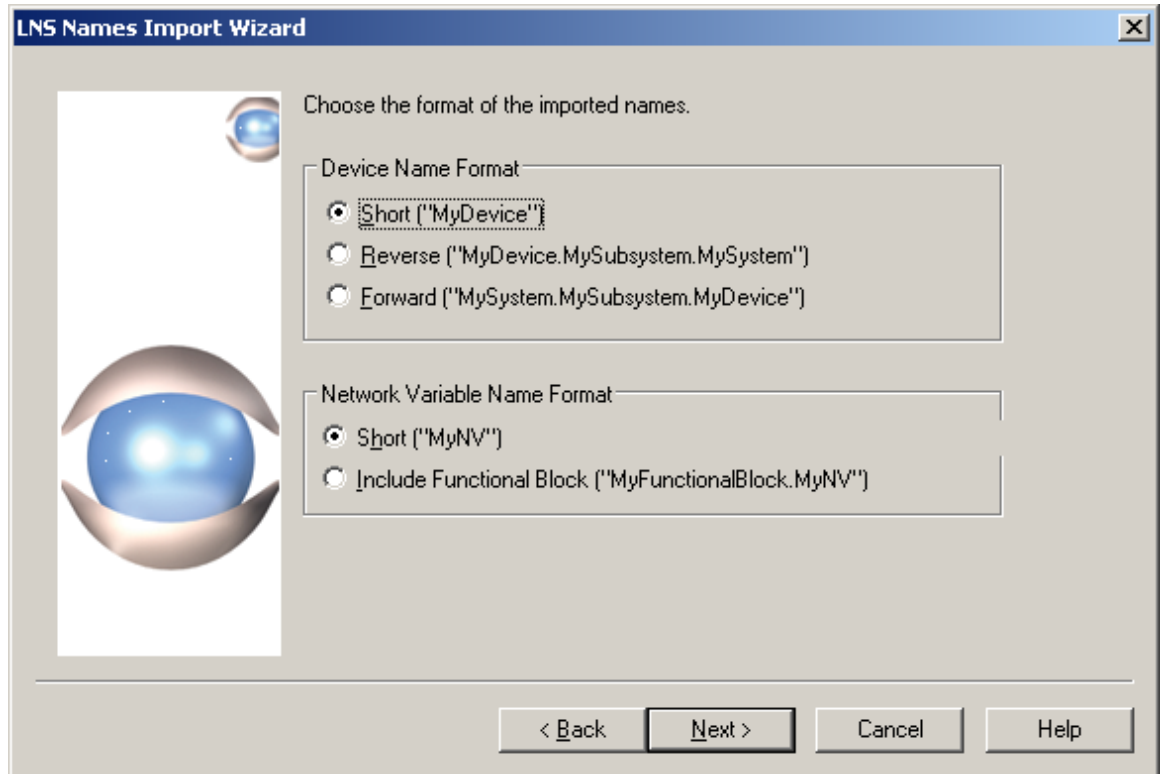


**Figure 2.15** LNS Names Import Wizard – Window Three

4. As the names are imported, it is possible that the names stored in the LNS database may conflict with the names that you have previously imported or assigned. These conflicts may occur under the following circumstances:
  - Two domains have the same ID.
  - Two devices or router sides in the same domain have the same Neuron<sup>®</sup> ID.
  - Two devices or router sides in the same domain have the same subnet/node address.
  - Two network variables belonging to the same device have the same index.
  - Two network variables belonging to the same device have the same direction and selector.

Select **Use LNS Database Name** or **Use Original Name** to automatically use the name from the LNS database or from the current names file when a conflict occurs. Select **Prompt for Each Conflict** to be prompted each time a conflict is detected, allowing you to decide on a case-by-case basis.

Click **Next**. The window shown in Figure 2.16 opens.



**Figure 2.16** LNS Names Import Wizard – Window Four

5. Select a format for device and network variable names. Examples for each option are shown on the dialog.
6. Click **Next**. The LonScanner software imports the names from the LNS database. When it finishes, a completion window will appear. Click **Finish** to exit the wizard. If you want, you can click **Save** from the completion window to save the imported names into a .RTF file.
7. You can now use the imported names. You can also use the **Names** menu to add new names, and customize the ones you have imported. For more information on this, see *Creating and Customizing Names* on page 38.

## Importing Names from a Local Names File

You can import names from a *local names file* on your computer. Names files contain pre-defined sets of names. You can create a names file by importing names from an LNS database or from a network channel, and then saving them into a file. Or, you can manually create a names file from scratch. The *Managing Names Files* section later in this chapter describes how to save names files for this purpose.

This may be useful if you are using multiple network interfaces to monitor the same network. You could define one names file containing all the names for the network, and then import the names from that file whenever you start a LonScanner session with any of the network interfaces on that network.

To import names from a names file, follow these steps:

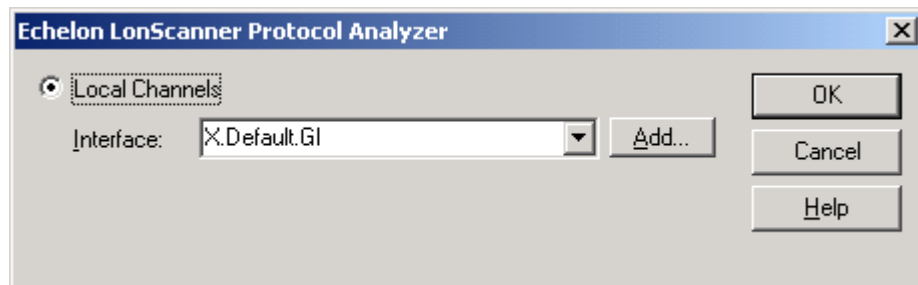
1. Select **Import from Names File** from the **Names** menu. A dialog opens reminding you that the names you are currently using will be overwritten if you continue.
2. Click **Yes** to continue. The Windows Open File dialog opens.
3. Browse for the names file you want to use, and click **Open** to import the names.
4. You can now use the imported names as you desire. You can also use the **Names** menu to add new network object names and customize the ones you have imported. For more information on this, see *Creating and Customizing Names* on page 38.

## Importing Names from a Channel

As noted previously, the protocol analyzer will save the names created for a channel as the default names for that channel in a *channel names file*. The channel names file is updated automatically each time a name is added to or removed from a channel. The names defined in the channel names file are used each time you open a connection to that channel, even after you have stopped and re-started the protocol analyzer.

You can import names from one channel to another, if you want multiple channels to use the same set of names. When you import these names into a channel, the protocol analyzer clears all the names currently being used from memory. To import names from a channel names file, follow these steps:

1. From the **Names** menu, select **Import from Channel**. A dialog opens reminding you that the names you are currently using will be overwritten if you continue.
2. Click **Yes** to continue. The dialog shown in Figure 2.17 opens.



**Figure 2.17** Select a Channel

3. Select the network interface you are using to connect to the channel you want to import the names from, and then click **OK** to import the names.

You can now use the imported names. You can also use the Names menu to save the imported names file for later use, or to add new network object names and customize the ones you have imported. For more information on this, see *Creating and Customizing Names* on page 38.

---

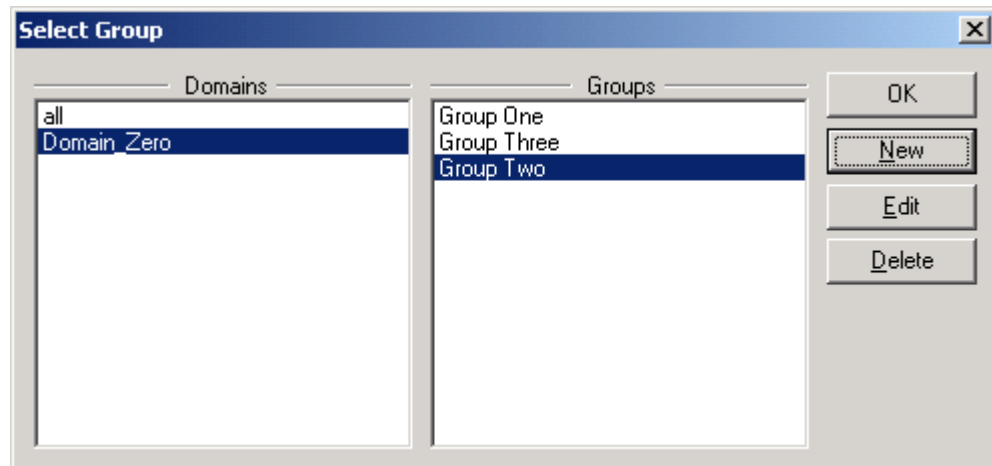
## Creating and Customizing Names

You can use the **Names** menu to create your own names, or to customize the names you have already created. This section describes how to do so.

### Creating Group Names

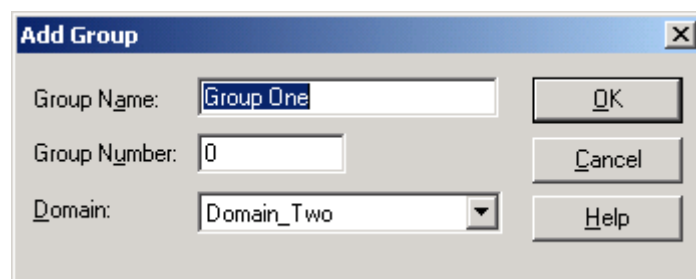
You can create or change an ANSI/CEA-709.1 group name with the protocol analyzer. To do so, follow these steps:

1. From the **Names** menu, select **Edit Groups**. The dialog shown in Figure 2.18 opens.



**Figure 2.18** Select Group Dialog

2. Select a domain from the Domains list, and the groups that have been assigned names in that domain will be listed in the Groups list. To create new group name, click **New**. The dialog shown in Figure 2.19 opens.



**Figure 2.19** Add Group Dialog

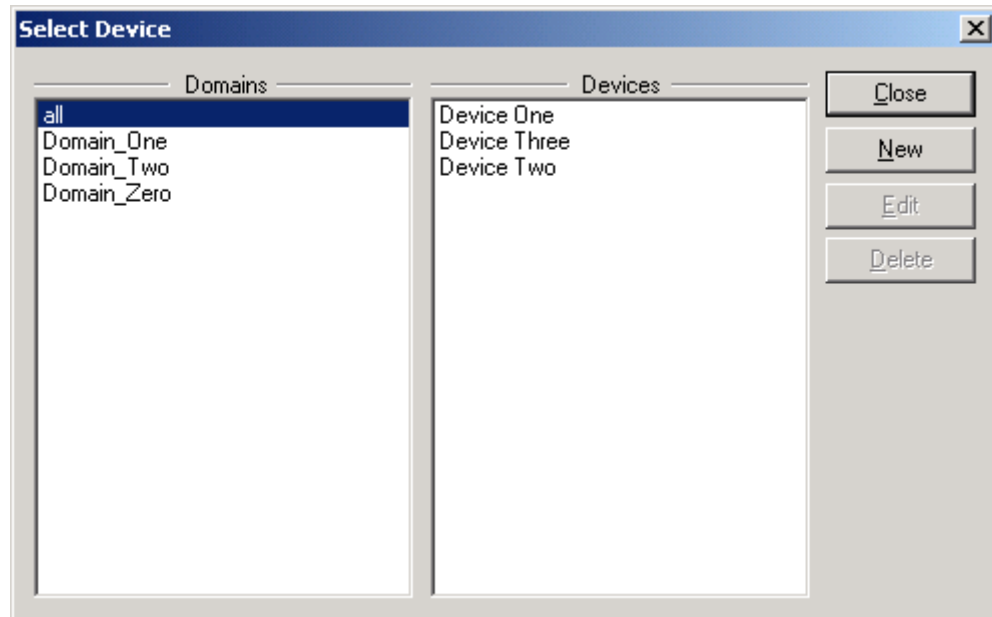
3. Select the domain containing the group from the **Domain** box.
4. Enter the group ID for the group in the **Group Number** box, and enter the name you want to use in the **Group Name** box.
5. Click **OK**. This returns you to the Select Group dialog shown in Figure 2.18.

6. The new group name will be listed in the Groups list. You can edit the group name later by selecting it and clicking **Edit**. You can delete the group name later by selecting it and clicking **Delete**.

## Creating Device Names

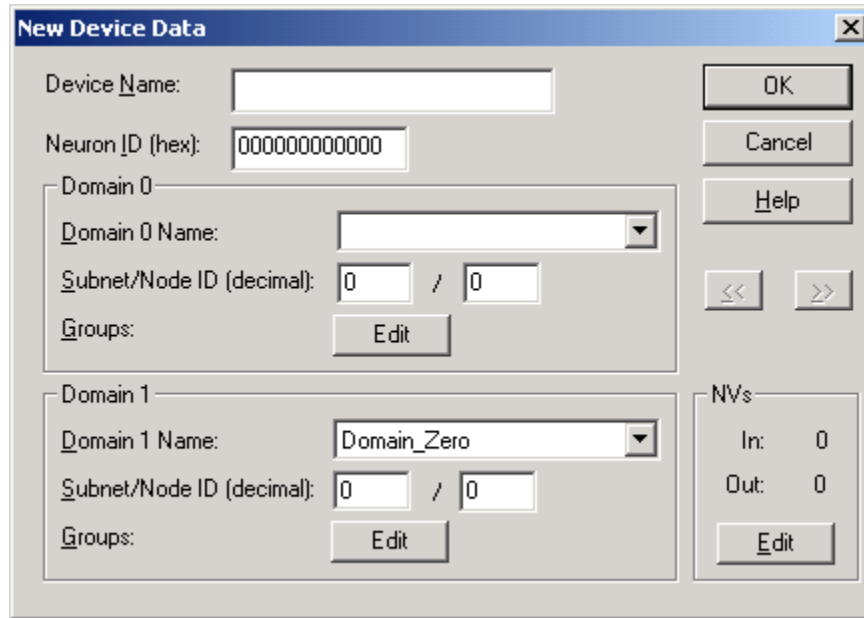
You can create or change a device name based on ANSI/CEA-709.1 subnet and node IDs. To create or edit a device name, follow these steps:

1. From the **Names** menu, select **Edit Devices**. The dialog shown in Figure 2.20 opens.



**Figure 2.20** Select Device Dialog

2. Select a domain from the Domains list, and the devices that have been assigned names in that domain will be listed in the Devices list. To add a new device name, click **New**. The dialog shown in Figure 2.21 opens.



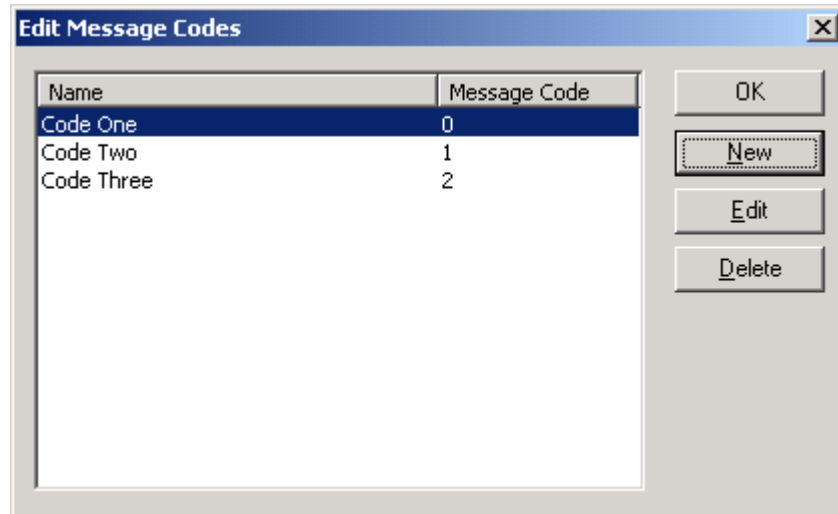
**Figure 2.21** New Device Data Dialog

3. Enter the device's name in the Device Name box, and then fill in the rest of the fields on the New Device Data dialog. Consult the online help for details on these fields.
4. Click **OK**. This returns you to the Select Device dialog shown in Figure 2.20. The new device name will be listed in the Devices list. You can edit the device name later by selecting it and clicking **Edit**. You can delete the device name later by selecting it and clicking **Delete**.

## Creating Message Code Names

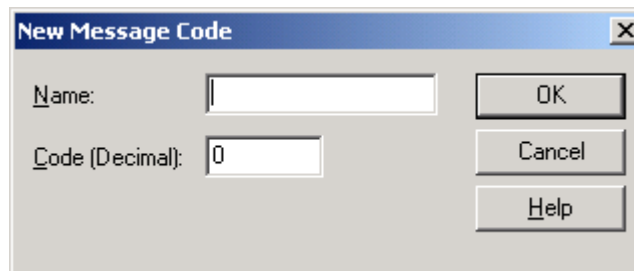
You can create or change an ANSI/CEA-709.1 message code name, and you can optionally specify formatting for a message. To do so, follow these steps:

1. From the **Names** menu, select **Edit Message Codes**. The dialog shown in Figure 2.22 opens.



**Figure 2.22** Edit Message Codes Dialog

2. The Edit Message Codes dialog lists all the currently defined message code names. To create a new message code name, click **New**. The dialog shown in Figure 2.23 opens.



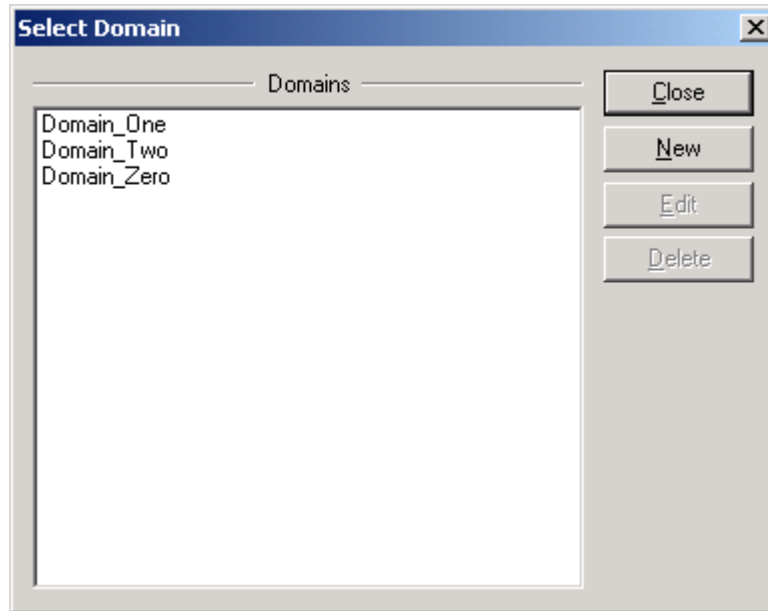
**Figure 2.23** New Message Code Dialog

3. Enter the name of the message code, and the message code the new name should apply to. Consult the online help for more information on these settings.
4. Click **OK**. This returns you to the dialog shown in Figure 2.22. The new message code name will be listed on the dialog. You can edit the message code name later by selecting it and clicking **Edit**. You can delete the message code later by selecting it and clicking **Delete**.

## Creating Domain Names

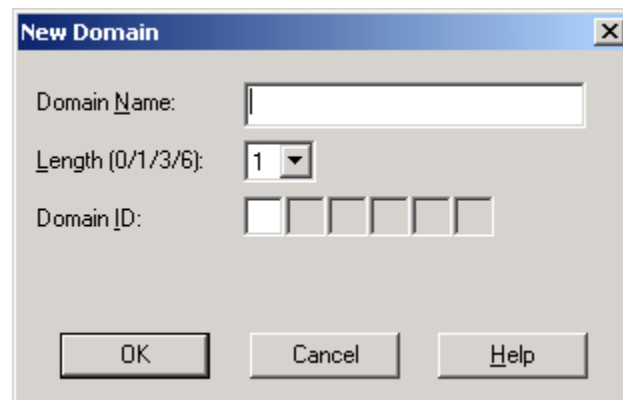
You can create or change an ANSI/CEA-709.1 domain name with the protocol analyzer. To do so, follow these steps:

1. From the **Names** menu, select **Edit Domains**. The dialog shown in Figure 2.24 opens.



**Figure 2.24** Select Domain Dialog

2. The Select Domain dialog lists the domain names currently defined on your network. To create a new domain name, click **New**. The dialog shown in Figure 2.25 opens.



**Figure 2.25** Edit Domain Dialog

3. Enter a name for the domain in the **Domain Name** box, and then set the domain ID and length for the domain. Consult the online help for more information on these fields.
4. Click **OK**. This returns you to the dialog shown in Figure 2.24. The new domain name will be listed on the dialog. You can edit the domain name later by selecting it and clicking **Edit**. You can delete the domain name later by selecting it and clicking **Delete**.

---

## *Managing Names Files*

You can save names that you have created, edited, or imported for later use by saving them into a names file. When you create, edit, or import names, the



protocol analyzer starts using those names immediately. However, you must save the names to a *names file* to prevent changing them in future LonScanner sessions. You can also backup the names file for safekeeping, and you can copy the names file to another computer with the LonScanner software for interpreting names within a packet log on the second computer.

To manually save the names into a names file, select **Save Copy** from the **Names** menu. This opens a Windows Save File dialog you can use to select the name and directory of the names file. Once you have saved the names file, you can back it up, copy it to another computer, or import it for use in future LonScanner sessions, as described in the *Importing Names from a Local Names File* section on page 33.



# 3

## Analyzing Packet Log Details

This chapter describes how to organize and analyze the data stored in your log files, including how to search a log file for a specific packet, how to bookmark certain packets as being of interest, and how to format the data in the Packet Log tab for display. It also describes how to print and export log files.

You can use the features described in this chapter when viewing a saved log file, or when viewing an active log file.

---

## Searching For Packet Log Entries

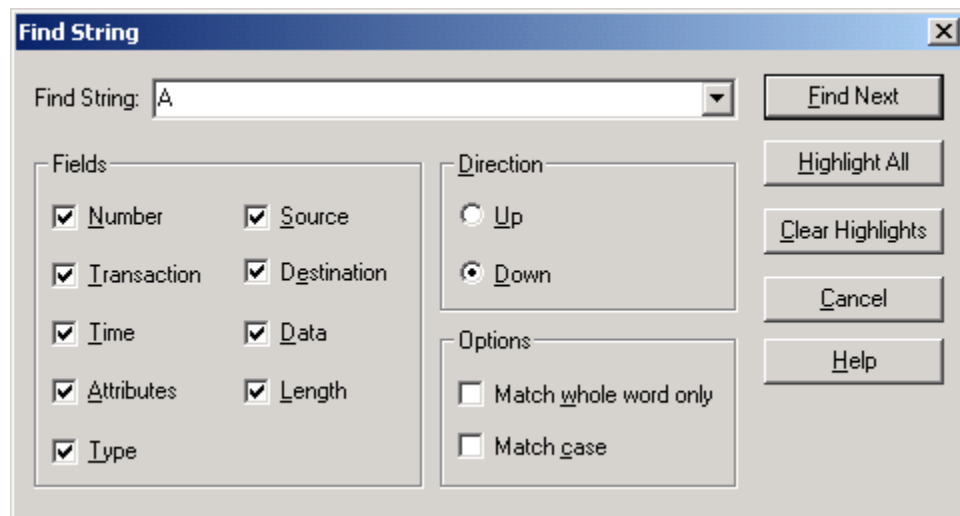
You can quickly search a packet log to find a specific packet, even if your log file contains log entries for hundreds or even thousands of packets. You can search a log file for a specific packet number, or for a string.

---

### Searching By String

You can search any of the fields listed in the Packet Log tab for a specific string by following these steps:

1. From the **Edit** menu, select **Find**. The dialog shown in Figure 3.1 opens.



**Figure 3.1** Find String Dialog

2. Enter the string you want to search the log for in the **Find String** box.
3. Select the data fields you want to search by setting each applicable entry in the Fields box. For example, select the **Data** check box to search the data field of every packet in the log.

Set a **Direction** button to determine whether you want to search upwards or downwards through the log.

Consult the online help for descriptions of the fields listed on the dialog.

4. Click **Find Next** to find the next occurrence of the string in the log file. Following this, you can use the **Find Next** and **Find Prev** commands in the **Edit** menu to find additional occurrences of the string, without having to fill in the Find String dialog again.

You can highlight each log entry containing the string in the Packet Log by clicking **Highlight All**. You can clear the highlights later by clicking **Clear Highlights**.

The LonScanner toolbar also includes buttons you can use to find a string, and to move to the next occurrence of a string once you have begun a search.

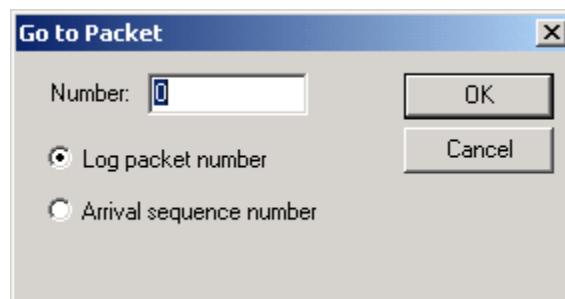
For more information on the LonScanner toolbar, see *LonScanner Toolbar* on page 12.

---

## Searching By Log Number

You can find a particular log entry by searching for its log packet number or its arrival sequence number. The *log packet number* is the number currently assigned to the packet in the log. If you are using a circular log, this number may change as log entries are added to and removed from the log. The *arrival sequence number* is a unique number assigned to the packet when the protocol analyzer collects it from the channel. To search for a log entry by its log packet or arrival sequence number, follow these steps:

1. From the **Edit** menu, select **Go To**. The dialog shown in Figure 3.2 opens.



**Figure 3.2** Go To Packet Dialog

2. Select **Log Packet Number** to search for a packet by its log packet number. Select **Arrival Sequence Number** to search for a packet by the sequence number assigned to the packet when the protocol analyzer received it.
3. Enter the packet or sequence number in the **Number** box, and click **OK**. The Packet Log tab will scroll to the specified packet.

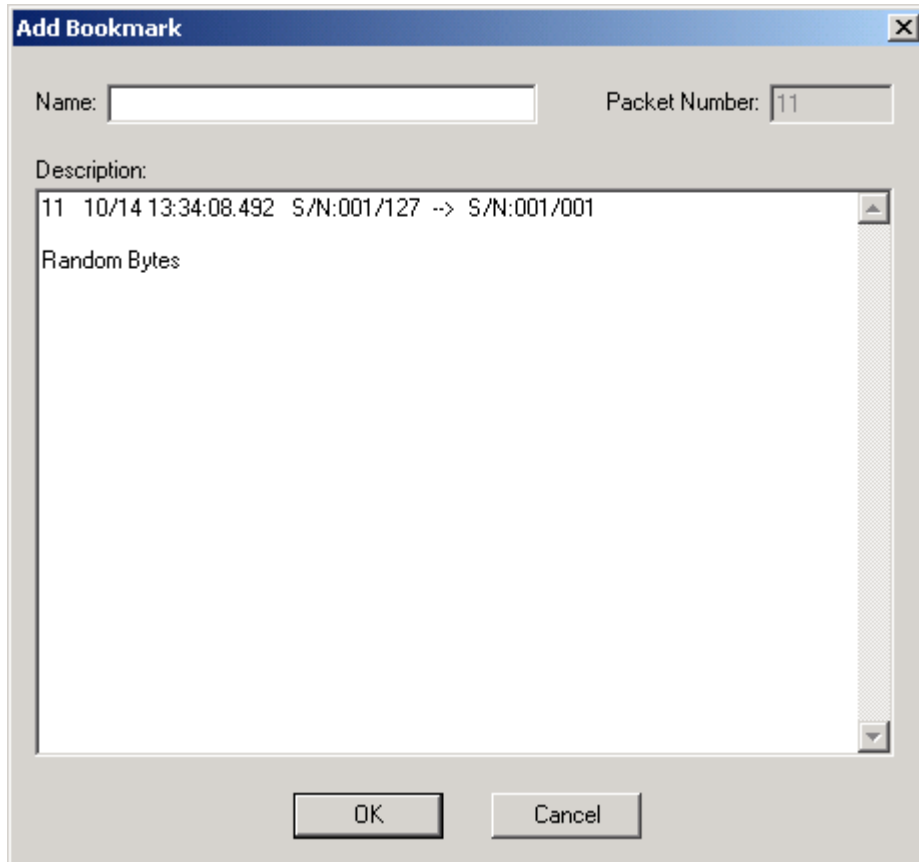
---

## Bookmarking Packet Log Entries

You can use bookmarks to mark specific log entries as being of interest, so that they are easier to find in the log. When you bookmark a log entry, that log entry will be highlighted in the Packet Log tab, so that it stands out. Once you have created a set of bookmarks, you can scroll through the log from bookmarked packet to bookmarked packet.

To use bookmarks, follow these steps:

1. Right-click the log entry in the Packet Log tab and then click **Toggle Bookmark** on the shortcut menu, or select **Toggle Bookmark** from the **Edit** menu. The dialog shown in Figure 3.3 opens.



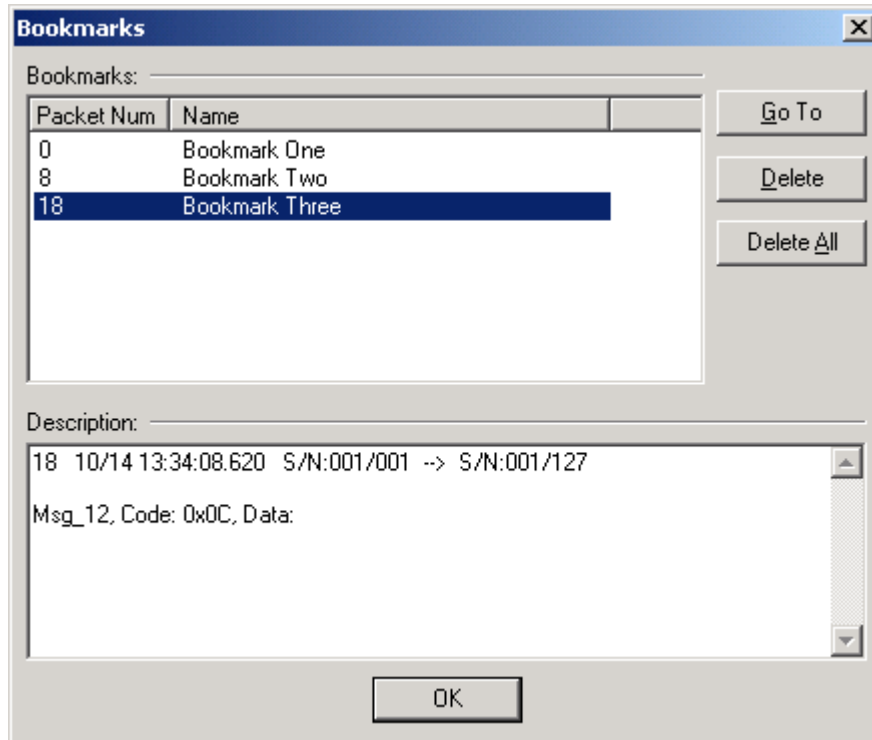
**Figure 3.3** Add Bookmark Dialog

2. Enter a name for the bookmark in the **Name** box. You can optionally enter any descriptive text you want associated with the bookmark in the Description box. The Description box contains the message data associated with the log entry by default.
3. Click **OK** to save the bookmark and return the Packet Log tab. The packet will appear highlighted in the Packet Log tab.

To scroll from bookmark to bookmark, use the **Next Bookmark** and **Prev Bookmark** commands in the **Edit** menu. The LonScanner toolbar also includes buttons you can use to scroll from bookmark to bookmark. For more information on the LonScanner toolbar, see *LonScanner Toolbar* on page 12.

To view all your bookmarks or delete any of your bookmarks, follow these steps:

1. From the **Edit** menu, select **Bookmarks**. The dialog shown in Figure 3.4 opens:



**Figure 3.4** Bookmarks Dialog

2. The bookmarks are listed at the top of the dialog, sequentially by packet number. Click a bookmark in the list to select that bookmark, and then click **Go To** to scroll the Packet Log to that log entry. Or, click **Delete** to remove the log entry from the log. To remove all packets at once, click **Delete All**.

---

## Formatting the Packet Log

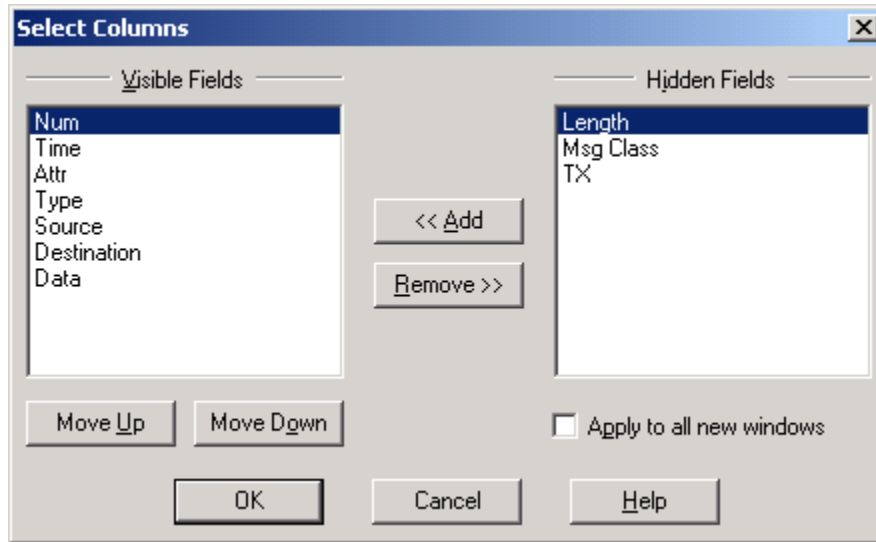
There are several ways to format the data that is displayed in the Packet Log tab. You can select the fields to be displayed in the Packet Log, and you can change the formatting for a field. You can also change the color that will be used to highlight bookmarked packets.

---

## Selecting Data Fields

You can select the fields that will be displayed in the Packet Log by following these steps:

1. From the **View** menu, click **Select Columns**. The dialog shown in Figure 3.5 opens.



**Figure 3.5** Select Columns Dialog

2. The fields that will be displayed in the Packet Log are listed in the **Visible Fields** list. Consult the online help for descriptions of these fields. To change the position of a field in the log, click the field and then click **Move Up** or **Move Down** to move the field. The top field will be displayed on the left side of the Packet Log, and the bottom field will be displayed on the right side of the Packet Log.

To remove a field from the Visible Fields list, select it and then click **Remove**. The field will move to the Hidden Fields list. To add a hidden field back to the Visible Fields list, select it and then click **Add**.

Select the **Apply to All New Windows** check box to apply your changes to all the log files you subsequently open during the current LonScanner session. The default is for all data fields to be displayed.

3. Click **OK** to save your changes.

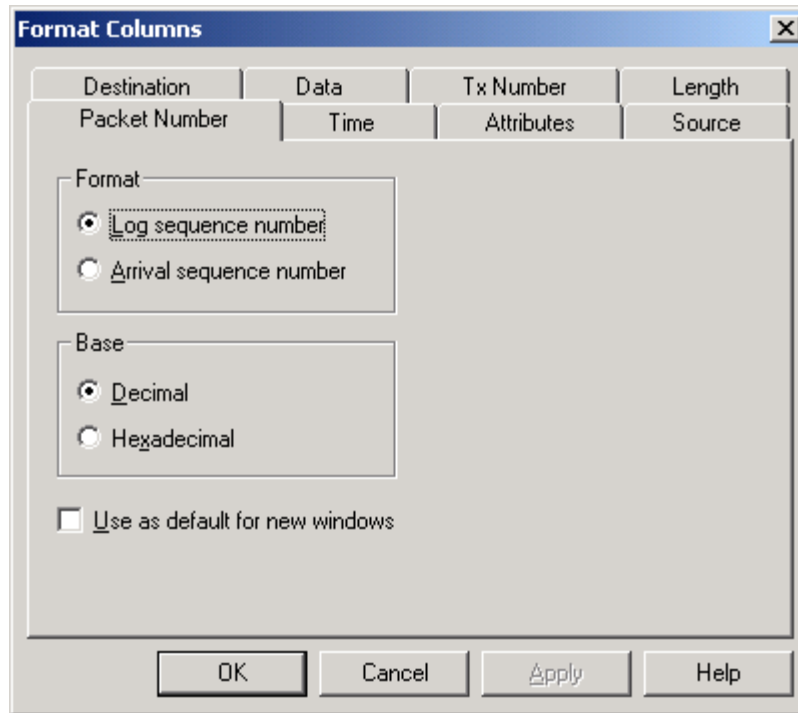
---

## *Formatting Data Field Columns*

You can change the formatting used to display the fields in the Packet Log tab by following these steps:

1. From the **View** menu, select **Format Columns**. The dialog shown in Figure 3.6 opens:





**Figure 3.6** Format Columns Dialog

2. The dialog defaults to the Packet Number tab, which you can use to format the Packet Number field. You can select the other tabs to format the other data fields in the Packet Log window.

Fill in the fields on each tab, and then click **OK** to save your changes and close the dialog. Or, click **Apply** to save your changes and continue formatting the data fields. Consult the online help for more extensive details on how to use each tab.

3. To change the font used to display the fields in the Packet Log tab, select **Fonts** from the **View** menu. A Windows Font dialog opens. Select the font you want to use and then click **OK** to save your changes.

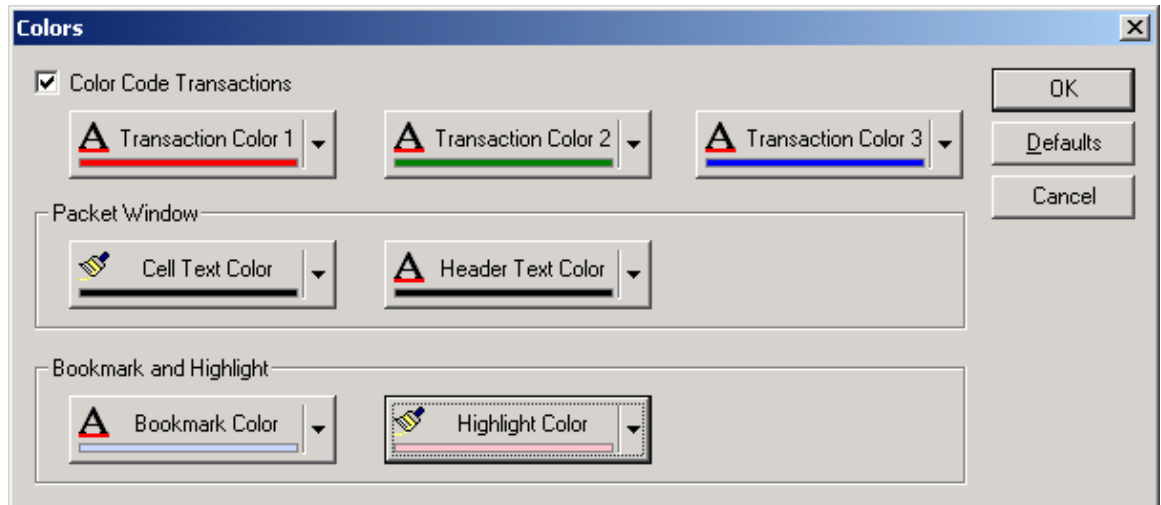
---

## *Color-Coding the Packet Log*

You can color-code certain log entries to make them stand out. This includes bookmarked packets and messages that belong to certain transactions. For an acknowledged message, a transaction includes the original message, all acknowledgements from all receiving devices, all retries, and any challenge and response messages. For a request/response message, a transaction includes the request message, the response message, and any challenge messages involved. When transaction color-coding is enabled, all packets within the same transaction will be colored the same color, so that it will be easier for you to find log entries for the packets involved in a given transaction.

To use color-coding, follow these steps:

1. From the **View** menu, select **Color**. The dialog shown in Figure 3.7 opens.



**Figure 3.7** Colors Dialog

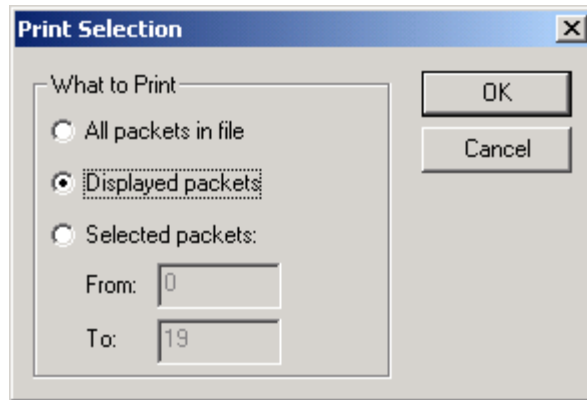
2. To enable transaction color-coding, select the **Color Code Transactions** check box. When you enable this feature, the log entries for all the packets involved a single transaction will be colored the same color. Click the Transaction Color buttons to select the three transaction colors. The LonScanner tool will use Transaction Color 1, Transaction Color 2 and Transaction Color 3 boxes in a rotation as new transactions begin.
3. To disable transaction color-coding, clear the **Color Code Transactions** check box.
4. To change the cell text or header text color in the Packet Log tab, click the **Cell Text Color** or **Header Text Color** button in the Packet Window box.
5. To change the bookmark or highlight color, click the **Bookmark Color** or **Highlight Color** button in the **Bookmark and Highlight** box. The highlight color is the color that packets highlight with the Find String dialog described earlier in this chapter will be shaded with.
6. To restore the default colors, click **Default**.
7. Click **OK**.

---

## Printing Log Files

To print a log file, follow these steps:

1. From the **File** menu, select **Print**. The dialog shown in Figure 3.8 opens.



**Figure 3.8.** Print Selection Dialog

2. Select the packets you want to be printed, and then click **OK**. The Windows Print dialog appears, which you can use to select a printer and then print the selected log entries.

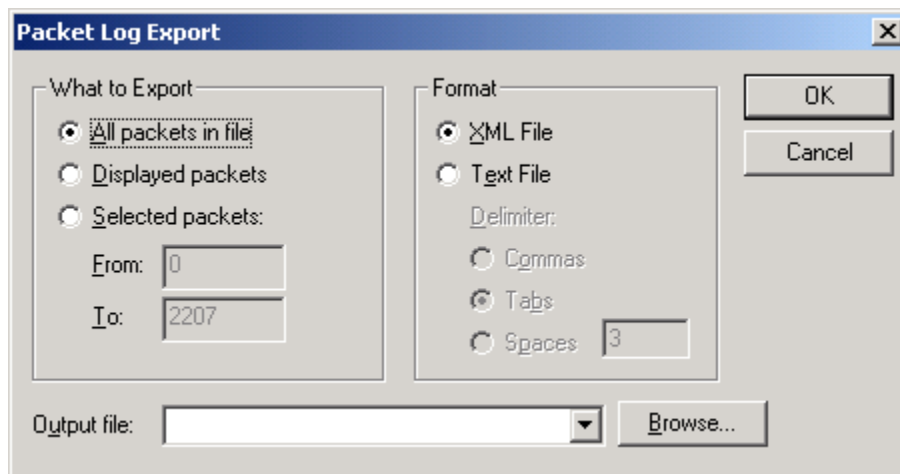
**NOTE:** You can also print any of the statistics tabs described in the *Viewing Channel Statistics and Trend Graphs* section in Chapter 2. To do so, select the tab you want to print, and then select **Print** from the **File** menu. This opens the Windows Print dialog. You will not need to use the Print Selection dialog in this case.

---

## Exporting Log Files

You can export the contents of a log file to a text or XML file. XML is an open data interchange format that you can use to export packets to other applications.

1. From the **File** menu, select **Export**. The dialog shown in Figure 3.9 opens.



**Figure 3.9** Packet Log Export Dialog

2. Select the packets to be exported in the **What to Export** box.
3. Use the Format box to determine whether the selected log entries will be exported into a text file or an XML file. If you select a text file, each log entry will be written to the output file as a single line of plain ASCII text, followed

by an end-of-line terminator. If you are exporting a text file, choose what character will be used to separate the fields of a single log entry under **Delimiter**.

Enter the name of the file to contain the exported log in the **Output File** box. The file will be created in the LONWORKS\Echelon LonScanner Protocol Analyzer directory by default. To select another directory, click **Browse**.

4. Click **OK** to export the selected log entries.

# 4

## Example Logs

This chapter describes the example log files included with the LonScanner software.

## Example Packet Logs

Two example logs are included with the LonScanner software. One of the example log files is taken from a channel without any names defined. The second example log file is taken from a channel that has imported a set of names from an LNS database.

### Channel Without Assigned Names

The first example log file is shown below. There are no names defined for this log file. This example shows how you can use a log file to find the log entry for a request message, find the log entry for the response to the request, and finally how you can find the acknowledgement of the response.

The screenshot displays the Echelon LonScanner Protocol Analyzer interface. The main window shows a packet log with columns for Num, Time, Attr, Type, Source, Dest, and Data. Packet C is selected, showing a Request message from S/N:001/001 to S/N:001/002 with data 'Net Var Fetch (6)'. The Packet Detail pane on the right shows the properties of this packet, including General, Address, Transaction, and Attributes. The Data field in the Packet Detail pane shows 'Net Var Fetch (6)' and 'NV Index: 6'.

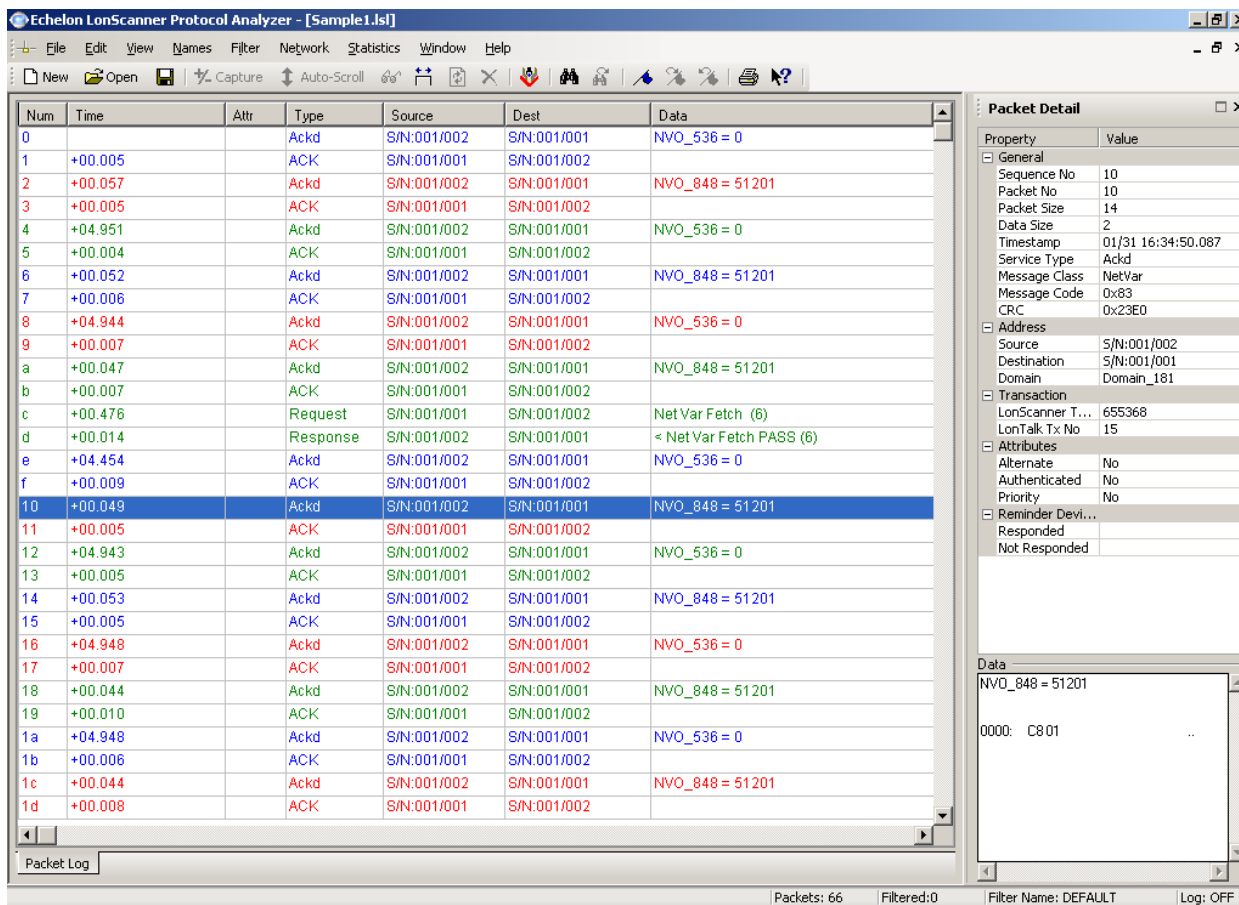
Num	Time	Attr	Type	Source	Dest	Data
0			Ackd	S/N:001/002	S/N:001/001	NVO_536 = 0
1	+00.005		ACK	S/N:001/001	S/N:001/002	
2	+00.057		Ackd	S/N:001/002	S/N:001/001	NVO_848 = 51201
3	+00.005		ACK	S/N:001/001	S/N:001/002	
4	+04.951		Ackd	S/N:001/002	S/N:001/001	NVO_536 = 0
5	+00.004		ACK	S/N:001/001	S/N:001/002	
6	+00.052		Ackd	S/N:001/002	S/N:001/001	NVO_848 = 51201
7	+00.006		ACK	S/N:001/001	S/N:001/002	
8	+04.944		Ackd	S/N:001/002	S/N:001/001	NVO_536 = 0
9	+00.007		ACK	S/N:001/001	S/N:001/002	
a	+00.047		Ackd	S/N:001/002	S/N:001/001	NVO_848 = 51201
b	+00.007		ACK	S/N:001/001	S/N:001/002	
c	+00.476		Request	S/N:001/001	S/N:001/002	Net Var Fetch (6)
d	+00.014		Response	S/N:001/002	S/N:001/001	< Net Var Fetch PASS (6)
e	+04.454		Ackd	S/N:001/002	S/N:001/001	NVO_536 = 0
f	+00.009		ACK	S/N:001/001	S/N:001/002	
10	+00.049		Ackd	S/N:001/002	S/N:001/001	NVO_848 = 51201
11	+00.005		ACK	S/N:001/001	S/N:001/002	
12	+04.943		Ackd	S/N:001/002	S/N:001/001	NVO_536 = 0
13	+00.005		ACK	S/N:001/001	S/N:001/002	
14	+00.053		Ackd	S/N:001/002	S/N:001/001	NVO_848 = 51201
15	+00.005		ACK	S/N:001/001	S/N:001/002	
16	+04.948		Ackd	S/N:001/002	S/N:001/001	NVO_536 = 0
17	+00.007		ACK	S/N:001/001	S/N:001/002	
18	+00.044		Ackd	S/N:001/002	S/N:001/001	NVO_848 = 51201
19	+00.010		ACK	S/N:001/001	S/N:001/002	
1a	+04.948		Ackd	S/N:001/002	S/N:001/001	NVO_536 = 0
1b	+00.006		ACK	S/N:001/001	S/N:001/002	
1c	+00.044		Ackd	S/N:001/002	S/N:001/001	NVO_848 = 51201
1d	+00.008		ACK	S/N:001/001	S/N:001/002	

Figure 4.1 Example Log File One – Packet C Selected

In Figure 4.1, packet C is selected in the Packet Log. In this example, the formats for the Time and Num fields have been changed from the default. You can tell from the data fields in the Packet Log that a device with subnet/node address 1/1 (Source field) is sending a Network Variable Fetch request message to a device with subnet/node address 1/2 (Destination field). From the information in the Packet Detail pane, you can determine that the request

message code is 0x73. For a complete list of network diagnostic messages, see the *ANSI/CEA-709.1 Control Network Protocol Specification*.

A network variable fetch retrieves the value of a network variable on a device by its index on the device. This can be used to poll the value of a network variable. In this example, the network variable index is 6. At packet d, device 1/2 responds back to device 1/1. The success response code is 0x33 and the returned data is 0 0 in raw format.



**Figure 4.2** Example Log File One – Packet 10 Selected

In Figure 4.2, packet 10 is selected in the Packet Log. At packet number 10, device 1/1 sends an acknowledgement to device 1/2. The Data field for packet 10 is “NVO\_848=51201.” This means the network variable is an output network variable, and 848 is the selector number of that network variable. A selector is the number used by the Neuron firmware to associate a network variable update message with a network variable on the device. In this example, the network variable type is **SNVT\_switch** and the data sent is C8 01 (hex) which is 200 1 in raw format. 51201 is the decimal display of C801. At packet number 11, ACK is the acknowledgment.

## ***Channel with Names Imported from LNS Database***

The second example log file is shown below. The names shown in this log file have been imported from an LNS database. This example shows how you can

search a log for responses to a message sent using the acknowledged messaging service.

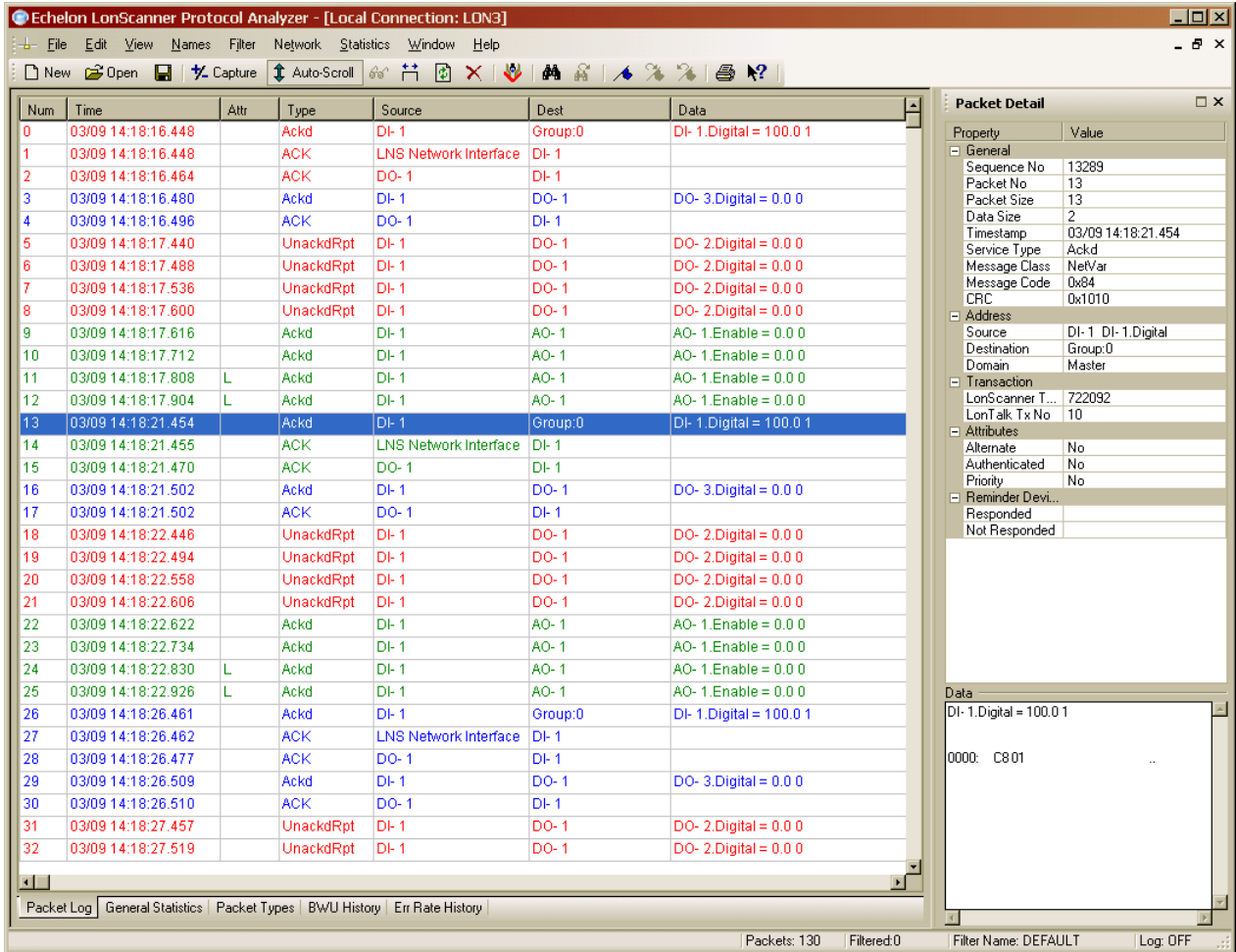
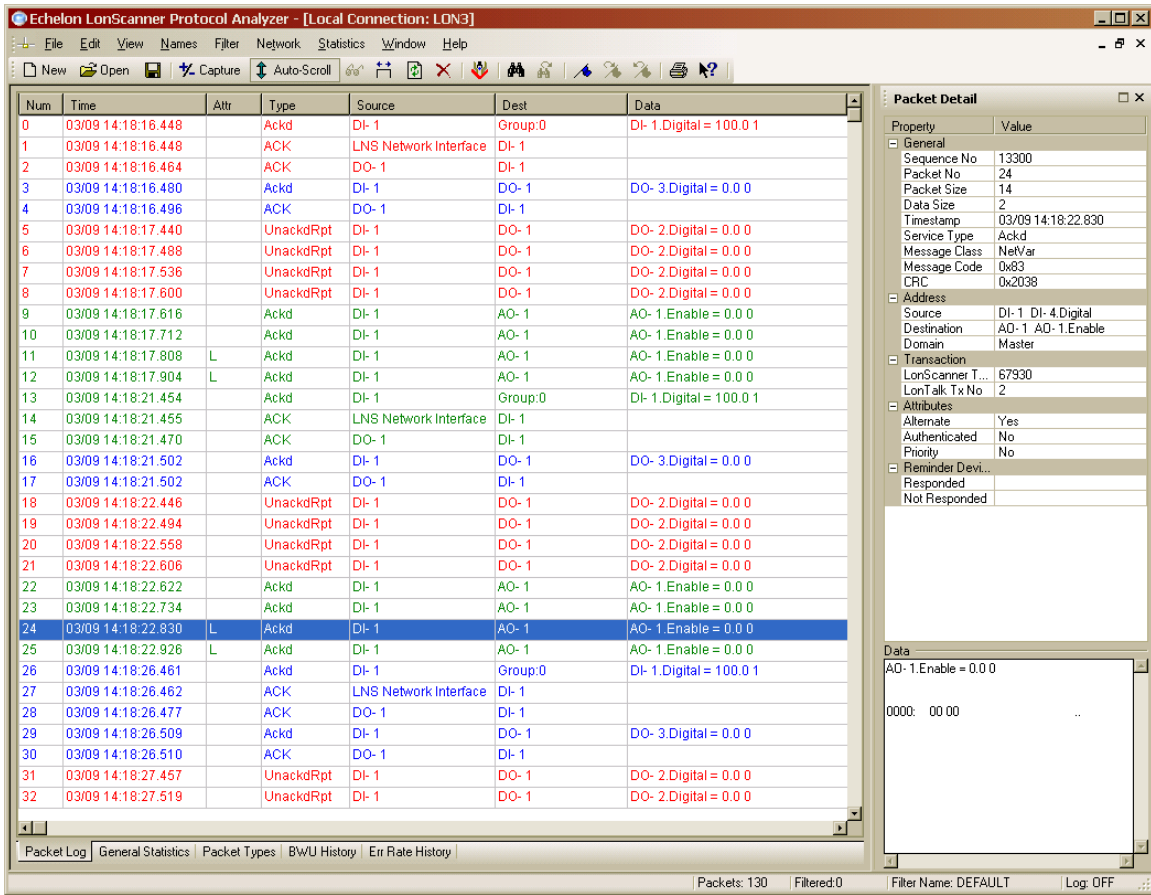


Figure 4.3 Example Log File Two – Packet 13 Selected

In Figure 4.3, packet 13 is selected in the Packet Log. At packet number 13, device DI-1 is sending out a group acknowledged network variable update message (group number 0). The message data (Data field) is 100.0 1, which is a SNVT\_switch structure. At packets 14 and 15, device DO-1 and LNS Network Interface send acknowledgments back to device DI-1. This is a fan-out connection from device DI-1 to device DO-1 and an LNS Network Interface.

At packet number 18, device DI-1 is sending out an unacknowledged repeated network variable update message to device DO-1. The retry count is 3 by default, and packets 19 to 21 are the retry messages. Since this message was sent using the unacknowledged messaging service, no response is expected from the target device DO-1.





**Figure 4.4** Example Log File Two – Packet 24 Selected

At packet number 22, device DI-1 is sending out an acknowledged network variable update message to device AO-1, but device AO-1 fails to respond. Packets 23 through 25 are retry messages. The alternate path attribute is set on the last two attempts, packet number 24 and 25, of an acknowledged transaction. This concept also applies to request/response transaction. If a host monitoring application fails to get an update, check the log file to verify whether the target device fails to response to a network variable fetch message.



# Appendix A

## Network Interfaces

This appendix lists the Echelon 709.1 and IP-852 network interfaces that you can use with the protocol analyzer, and details any special considerations you will need to make when using each type of network interface.

---

## Network Interfaces Overview

There are a variety of network interfaces you can use with the protocol analyzer. This includes all Echelon layer 2 709.1 and IP-852 network interfaces, including the network interfaces listed below. Consult Echelon's Web site at [www.echelon.com](http://www.echelon.com) for more information on any of these network interfaces.

- *U10 and U20 USB Network Interfaces*—Two 709.1 network interfaces for any computer with a USB interface, which includes most desktop, laptop, and embedded computers. These network interfaces are ideal for use in applications that require a computer to monitor, manage, or diagnose a network. The interfaces feature support for TP/FT-10 channels (U-10) or PL-20 channels (U-20), downloadable memory, an LNS network management interface, and Plug n' Play capability with the Microsoft Windows XP, Windows Server 2003, and Windows 2000 and operating systems.
- *PCLTA-20*—A 709.1 network interface for desktop and embedded personal computers equipped with a 5V 32-bit PCI interface. There are four versions of the card that include an onboard transceiver (TP/FT-10, TP/XF-78, TP/XF-1250, or TP-RS485), and one version that accepts a standard modular transceiver (SMX) which may be used with any media type for which an SMX transceiver exists. The PCLTA-20 supports the Windows Plug n' Play standard. Before using a PCLTA-20 with the protocol analyzer, you must configure it to operate as a layer 2 network interface. For instructions, see *PCC-10 and PCLTA-20/21* on page 64.
- *PCLTA-21*—A 709.1 network interface for desktop and embedded personal computers equipped with a 3V or 5V 32-bit PCI interface. This network interface is ideal for use in applications that require a desktop or embedded computer to monitor, manage, or diagnose a network. The PCLTA-21 card features support for TP/XF-78, TP/XF-1250, TP/FT-10, and RS-485 channels, downloadable memory, an LNS network management interface, and Plug n' Play capability with the Microsoft Windows XP, Windows Server 2003, and Windows 2000 operating systems. The four versions of the PCLTA-21 interface with integral twisted pair transceivers support the TP/FT-10 (Model 74501), TP/XF-78 (Model 74502), TP/XF-1250 (Model 74503), and TP-RS485 (Model 74504) channels, respectively. Before using a PCLTA-21 with the protocol analyzer, you must configure it to operate as a layer 2 network interface. For instructions, see *PCC-10 and PCLTA-20/21* on page 64.
- *PCC-10*—A 709.1 network interface for any computer equipped with a type II PC card (formerly PCMCIA) interface, which includes most laptop computers. Includes an integral TP/FT-10 transceiver for use with TP/FT-10 channels. Other transceiver types can be connected to the PCC-10 via external transceiver pods. This network interface is ideal for use in applications that require a laptop computer. The PCC-10 features downloadable memory, an LNS network management interface, and Plug n' Play capability with the Microsoft Windows XP, Windows Server 2003, and Windows 2000 operating systems. Before using a PCC-10 with the protocol analyzer, you must configure it to operate as a layer 2 network interface. For instructions, see *PCC-10 and PCLTA-20/21* on page 64.

- *i.LON 100 Internet Server*—A controller, Web server, and remote 709.1 network interface that can be accessed via an Ethernet or dial-up IP connection. This network interface is ideal for use in applications requiring remote access via a LAN or the Internet. To monitor the 709.1 channel attached to an *i.LON 100 Internet Server*, the LonScanner computer must have IP connectivity to the *i.LON 100 Internet Server*, and the LonScanner monitoring module must be installed on the *i.LON 100 Internet Server*. In addition, the *i.LON 100 e2 Service Pack 1* (or newer) firmware must be installed on the *i.LON 100 Internet Server*. For more information on the LonScanner monitoring module, see *i.LON 100 Internet Server* on page 63.

*i.LON 100 e2 Service Pack 1* is included with the LonScanner software. To install it, double-click the `LON100e2_SP1.exe` file in the `Service Packs/i.LON 100 e2 SP 1` folder on the LonScanner CD.

- *i.LON 600 LONWORKS/IP Server*—An IP-852 router that can be used to connect a 709.1 channel to an IP-852 backbone. The LNS Turbo runtime includes a software network interface (also called a *virtual network interface*) that can be used to attach an LNS computer to an IP-852 channel, which in turn may also be attached to one or more *i.LON 600* routers. This router is ideal for use in large networks requiring an IP backbone.

When used with an *i.LON 600* router, the protocol analyzer can be used to either locally monitor the IP-852 channel, or remotely monitor the 709.1 channel on the other side of the *i.LON 600* router. To monitor the IP-852 channel, the LonScanner computer must be attached to the IP-852 channel, and an LNS Turbo runtime must be installed on the computer. There are limitations when monitoring the IP-852 channel. For more information, see *Using LonScanner with LNS Turbo Edition* on page 3. To monitor the 709.1 channel, the LonScanner computer must have IP connectivity to the *i.LON 600* router, and the version 1.03 (or later) firmware must be installed on the *i.LON 600* router.

*i.LON 600 Service Pack 3* is included with the LonScanner software. To install it, double-click the `LON600_SP3.exe` file in the `Service Packs/i.LON 600 SP 3` folder on the LonScanner CD.

---

## *i.LON 100 Internet Server*

You can use an *i.LON 100 Internet Server* as a remote network interface for the LonScanner software, and monitor the 709.1 channel attached to the *i.LON 100 Internet Server*. To do so, you will need to download the LonScanner monitoring module into your *i.LON 100 Internet Server*.

Before doing this, make sure that your *i.LON 100 Internet Server* is running the *e2 Service Pack 1* firmware. *i.LON 100 e2 Service Pack 1* is included with the LonScanner software. To install it, double-click the `LON100e2_SP1.exe` file in the `Service Packs/i.LON 100 e2 SP 1` folder on the LonScanner CD.

To download the LonScanner monitoring module into your *i.LON 100* router, follow these steps:

1. Copy the contents of the *i.LON* 100 Images folder. To access the *i.LON* 100 Images folder, select **Echelon LonScanner Protocol Analyzer** from the Windows **Programs** list, and then select **iLON100 Images**.
2. In the window that opens, double-click the appropriate folder for the *i.LON* 100 firmware version you are running (1.11 or later). Press CTRL-A to Select all of the files in the folder, and press CTRL-C to copy them.
3. Start Internet Explorer or another FTP client, and then open an FTP session to your *i.LON* 100 Internet Server. Enter your user name and password to access the main directory.
4. Press CTRL-V to paste the contents of the *i.LON* 100 Images folder into the main directory of the 100 Internet Server.
5. Reboot the *i.LON* 100 Internet Server. Once it has rebooted, you will be able to monitor the *i.LON* 100 Internet Server with the protocol analyzer

Consult the documentation for the *i.LON* 100 Internet Server for details on how to open an FTP session to the *i.LON* 100 Internet Server, and on how to reboot the *i.LON* 100 Internet Server.

---

## *i.LON* 600 LONWORKS/IP Server

You can use an *i.LON* 600 LONWORKS/IP Server as a remote network interface for the LonScanner software, and monitor the 709.1 channel attached to the *i.LON* 600 server. To do so, the version 1.03 (or later) firmware must be installed on the *i.LON* 600 router.

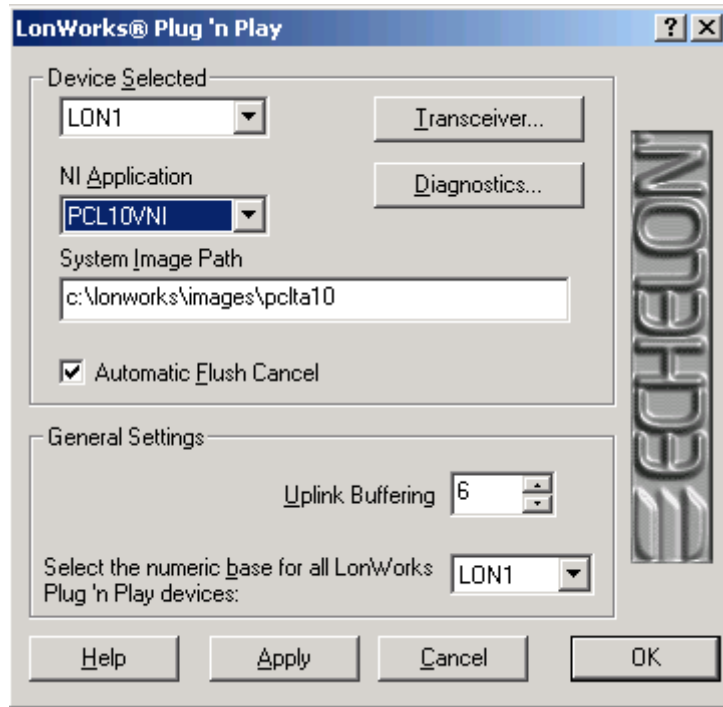
*i.LON* 600 Service Pack 3 (i.e. an update to *i.LON* 600 version 1.03) is included with the LonScanner software. To install it, double-click the LON600\_SP3.exe file in the Service Packs/*i.LON* 600 SP 3 folder on the LonScanner CD.

---

## *PCC-10 and PCLTA-20/21*

You can use a PCC-10, PCLTA-20, or PCLTA-21 with the protocol analyzer. Before using one of these cards, you must configure the card to operate as a layer 2 network interface with the LONWORKS Plug 'n Play application. To do so, follow these steps:

1. Open the Windows Control Panel, and then double-click the **LONWORKS Plug 'n Play** icon. The dialog shown in Figure A.1 opens.



**Figure A.1** LONWORKS Plug 'n Play Application

2. Make sure that the **Device Selected** field is set to the network interface you want to configure.
3. If you are using a PCC-10, set the **NI Application** box to **PCC10VNI**. If you are using a PCLTA-20 or a PCLTA-21, set the **NI Application** box to **PCL10VNI**.
4. Click **OK** to save your changes and close the LONWORKS Plug 'n Play application. You can now use your PCC-10, PCLTA-20 or PCLTA-21 with the protocol analyzer.





# Appendix B

## LonScanner Software License Agreement

When installing the LonScanner software, you must agree to the terms of the LonScanner software license agreement detailed in this appendix.

## **LONSCANNER™ PROTOCOL ANALYZER**

### **NOTICE**

This is a legal agreement between you and Echelon Corporation (“Echelon”). YOU MUST READ AND AGREE TO THE TERMS OF THIS SOFTWARE LICENSE AGREEMENT BEFORE ANY LICENSED SOFTWARE CAN BE DOWNLOADED OR INSTALLED OR USED. BY CLICKING ON THE “I AGREE” OR “I ACCEPT” BUTTON OF THIS SOFTWARE LICENSE AGREEMENT, OR DOWNLOADING LICENSED SOFTWARE, OR INSTALLING LICENSED SOFTWARE, OR USING LICENSED SOFTWARE, YOU ARE AGREEING TO BE BOUND BY THE TERMS AND CONDITIONS OF THIS SOFTWARE LICENSE AGREEMENT. IF YOU DO NOT AGREE WITH THE TERMS AND CONDITIONS OF THIS SOFTWARE LICENSE AGREEMENT, THEN YOU SHOULD EXIT THIS PAGE AND DO NOT DOWNLOAD OR INSTALL OR USE ANY LICENSED SOFTWARE. BY DOING SO YOU FOREGO ANY IMPLIED OR STATED RIGHTS TO DOWNLOAD OR INSTALL OR USE LICENSED SOFTWARE.

### **LonScanner Software License Agreement**

In consideration of Your agreement to the terms of this Agreement, Echelon grants You a limited non-exclusive, non-transferable license to one copy of the Licensed Software and accompanying documentation and any updates or upgrades thereto provided by Echelon according to the terms set forth below. If the Licensed Software is being provided to You as an update or upgrade to software which You have previously licensed, then You agree to destroy all copies of the prior release of this software within thirty (30) days after installing the Licensed Software; provided, however, that You may retain one (1) copy of the prior release for backup, archival and support purposes.

### **DEFINITIONS**

For purposes of this Agreement, the following terms shall have the following meanings:

- “Licensed Software” means all computer software and associated media, printed materials, and online or electronic documentation that accompany the LonScanner product; including, without limitation, any and all executable files, add-ons, stencils, templates, filters, tutorials, help files and other files, that accompany such software or are in the accompanying documentation.
- “Demonstration Mode” refers to a restricted mode of the Licensed Software where it will operate without full functionality as described in the documentation that accompanies the Licensed Software, including but not limited to partial display of incoming packets.
- “Activation Key” refers to a software key provided by Echelon that activates a copy of the Licensed Software on a particular computer such that the Licensed Software is no longer in Demonstration Mode.
- “Activate” refers to the process of entering an Activation Key into the Licensed Software such that the Licensed Software is no longer running in Demonstration Mode.
- “You(r)” means Licensee, i.e. the company, entity or individual who has rightfully acquired the Licensed Software.

## LICENSE

### You may:

- (a) use the Licensed Software on any number of computers in Demonstration Mode;
- (b) Activate the Licensed Software on any number of computers, provided that you have a unique and valid serial number for each activated computer, and you have purchased and installed an Activation Key from Echelon for each activated computer,
- (c) physically transfer an Activation Key from one computer to another, provided that the Licensed Software is no longer Activated on the computer on which it was previously used and the Licensed Software is Activated on only one computer per purchased Activation Key at a time,
- (d) copy the licensed software as necessary for the uses expressly permitted above;
- (e) transfer Your rights under this Agreement to an end user of the Licensed Software; provided that (i) You require the transferee to execute both copies of the Software License Transfer Agreement included with the Licensed Software, (ii) You retain one (1) signed original thereof and furnish Echelon with a copy of same upon request, and (iii) the Licensed Software is Activated on only one computer per purchased Activation Key at a time. This right of transfer is exercisable on a one-time-only basis, and Your transferee shall have no right whatsoever to further transfer any rights to the Licensed Software.

### You may not, and shall not permit others to:

- (a) use an Activation Key on more than one computer at a time;
- (b) Activate the licensed software without purchasing an Activation Key;
- (c) copy the Licensed Software (except as expressly permitted above), or copy the accompanying documentation;
- (d) modify, translate, reverse engineer, decompile, disassemble or otherwise attempt (i) to defeat, avoid, bypass, remove, deactivate, or otherwise circumvent any software protection mechanisms in the Licensed Software, including without limitation any such mechanism used to restrict or control the functionality of the Licensed Software, or (ii) to derive the source code or the underlying ideas, algorithms, structure or organization from the software from the Licensed Software (except to the extent that such activities may not be prohibited under applicable law); or
- (e) except for the limited rights granted above, distribute, rent, loan, lease, transfer or grant any rights in the Licensed Software or modifications thereof or accompanying documentation in any form to any person without the prior written consent of Echelon.
- (f) use the Licensed Software with network interfaces not manufactured by Echelon.

This license is not a sale. Title, copyrights and all other rights to the Licensed Software, Activation Key, accompanying documentation and any copy made by You remain with Echelon. Unauthorized copying of the Licensed Software, Activation Key, or the accompanying documentation, or failure to comply with the above restrictions, will result in

automatic termination of this license and will make available to Echelon other legal remedies.

## **TRADEMARKS**

You may make appropriate and truthful reference to Echelon, Echelon products and technology in Your company and product literature; provided that You properly attribute Echelon's trademarks and do not use the name of Echelon or any Echelon trademark in Your name or product name. No license is granted, express or implied, under any Echelon trademarks, trade names, trade dress or service marks.

## **LIMITED WARRANTY AND DISCLAIMER**

Echelon warrants that, for a period of ninety (90) days from the date of delivery or transmission to You, the Licensed Software under normal use will perform substantially in accordance with the Licensed Software specifications contained in the documentation accompanying the Licensed Software. Echelon's entire liability and Your exclusive remedy under this warranty will be, at Echelon's option, to use reasonable commercial efforts to attempt to correct or work around errors, to replace the Licensed Software with functionally equivalent Licensed Software, or to terminate this Agreement and accept return of the Licensed Software and refund Your purchase price less a reasonable amount for use.

EXCEPT FOR THE ABOVE EXPRESS LIMITED WARRANTIES AND CONDITIONS GIVEN BY ECHELON ABOVE, ECHELON AND ITS SUPPLIERS MAKE AND YOU RECEIVE NO OTHER WARRANTIES OR CONDITIONS, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE OR IN ANY COMMUNICATION WITH YOU, AND ECHELON AND ITS SUPPLIERS SPECIFICALLY DISCLAIM ANY IMPLIED WARRANTY OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT AND THEIR EQUIVALENTS. Echelon does not warrant that the operation of the Licensed Software will be uninterrupted or error free or that the Licensed Software will meet Your specific requirements.

SOME STATES OR OTHER JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY FROM STATE TO STATE AND JURISDICTION TO JURISDICTION.

## **LIMITATION OF LIABILITY**

IN NO EVENT WILL ECHELON OR ITS SUPPLIERS BE LIABLE FOR LOSS OF OR CORRUPTION TO DATA, LOST PROFITS OR LOSS OF CONTRACTS, COST OF PROCUREMENT OF SUBSTITUTE PRODUCTS OR OTHER SPECIAL, INCIDENTAL, PUNITIVE, CONSEQUENTIAL OR INDIRECT DAMAGES, LOSSES, COSTS OR EXPENSES OF ANY KIND ARISING FROM THE SUPPLY OR USE OF THE LICENSED SOFTWARE OR ACCOMPANYING DOCUMENTATION, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY (INCLUDING WITHOUT LIMITATION NEGLIGENCE). THIS LIMITATION WILL APPLY EVEN IF ECHELON OR AN AUTHORIZED DISTRIBUTOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY. EXCEPT TO THE EXTENT THAT LIABILITY MAY NOT BY LAW BE

LIMITED OR EXCLUDED, IN NO EVENT SHALL ECHELON'S OR ITS SUPPLIERS' LIABILITY EXCEED THE AMOUNTS PAID FOR THE LICENSED SOFTWARE. YOU ACKNOWLEDGE THAT THE AMOUNTS PAID BY YOU FOR THE LICENSED SOFTWARE REFLECT THIS REASONABLE ALLOCATION OF RISK.

SOME STATES OR OTHER JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU.

### **SAFE OPERATION**

YOU ASSUME RESPONSIBILITY FOR, AND HEREBY AGREE TO USE YOUR BEST EFFORTS IN, DESIGNING, MANUFACTURING, COMMISSIONING, AND RECOVERING LONWORKS DEVICES HEREUNDER TO PROVIDE FOR SAFE OPERATION THEREOF, INCLUDING, BUT NOT LIMITED TO, COMPLIANCE OR QUALIFICATION WITH RESPECT TO ALL SAFETY LAWS, REGULATIONS AND AGENCY APPROVALS, AS APPLICABLE. THE LICENSED SOFTWARE, NEURON® CHIP, LONTALK PROTOCOL, NEURON CHIP FIRMWARE AND THE LONWORKS NETWORK INTERFACES ARE NOT DESIGNED OR INTENDED FOR USE AS COMPONENTS IN EQUIPMENT INTENDED FOR SURGICAL IMPLANT INTO THE BODY, OR OTHER APPLICATIONS INTENDED TO SUPPORT OR SUSTAIN LIFE, FOR USE IN FLIGHT CONTROL OR ENGINE CONTROL EQUIPMENT WITHIN AN AIRCRAFT, OR FOR ANY OTHER APPLICATION IN WHICH THE FAILURE THEREOF COULD CREATE A SITUATION IN WHICH PERSONAL INJURY OR DEATH MAY OCCUR, AND YOU SHALL HAVE NO RIGHTS HEREUNDER FOR ANY SUCH APPLICATIONS.

### **LANGUAGE**

The parties hereto confirm that it is their wish that this Agreement, as well as other documents relating hereto, have been and shall be written in the English language only. Any translations are provided for convenience only, and the English language version shall control.

Les parties aux présentes confirment leur volonté que cette convention de même que tous les documents y compris tout avis qui s'y rattache, soient rédigés en langue anglaise.

### **COMPLIANCE WITH EXPORT CONTROL LAWS**

You agree to comply with all applicable export and reexport control laws and regulations, including the Export Administration Regulations ("EAR") maintained by the United States Department of Commerce. Specifically, you covenant that You shall not -- directly or indirectly -- sell, export, reexport, transfer, divert, or otherwise dispose of any software, source code, or technology (including products derived from or based on such technology) received from Echelon under this Agreement to any country (or national thereof) subject to antiterrorism controls or U.S. embargo, or to any other person, entity, or destination prohibited by the laws or regulations of the United States, without obtaining prior authorization from the competent government authorities as required by those laws and regulations. You agree to indemnify, to the fullest extent permitted by law, Echelon from and against any fines or penalties that may arise as a result of your breach of this provision. This export control clause shall survive termination or cancellation of this Agreement.

## GENERAL

This Agreement shall not be governed by the 1980 U.N. Convention on Contracts for the International Sale of Goods; rather, this Agreement shall be governed by the laws of the State of California, including its Uniform Commercial Code, without reference to conflicts of laws principles. This Agreement is the entire agreement between You and Echelon and supersedes any other communications or advertising with respect to the Licensed Software and accompanying documentation. If any provision of this Agreement is held invalid or unenforceable, such provision shall be revised to the extent necessary to cure the invalidity or unenforceability, and the remainder of the Agreement shall continue in full force and effect. If You are acquiring the Licensed Software on behalf of any part of the U.S. Government, the following provisions apply. The Licensed Software and accompanying documentation are deemed to be “commercial computer software” and “commercial computer software documentation”, respectively, pursuant to DFAR Section 227.7202 and FAR 12.212(b), as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Licensed Software and/or the accompanying documentation by the U.S. Government or any of its agencies shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement. Any technical data provided that is not covered by the above provisions is deemed to be “technical data-commercial items” pursuant to DFAR Section 227.7015(a). Any use, modification, reproduction, release, performance, display or disclosure of such technical data shall be governed by the terms of DFAR Section 227.7015(b).

Echelon, LON, LonMaker, LonTalk, LONWORKS, and Neuron are U.S. registered trademarks of Echelon Corporation. LonScanner is a trademark of Echelon Corporation. Windows is a U.S. registered trademarks of Microsoft Corporation.