ECHELON

IP-852 Channel User's Guide

078-0312-01C

Table of Contents

Preface v

Purpose vi
Audience vi
Content vi
Installing the Echelon IP-852 Configuration Server vi
Related Manuals vii
For More Information and Technical Support vii

1 Introduction 1

Introduction to the IP-852 Channel 2

2 Creating an IP-852 Channel 5

Creating an IP-852 Channel 6
Checking IP-852 Device Status 11
Backing Up the IP-852 Configuration Server Database 12
Managing Multiple IP-852 Configuration Server Databases 12
Creating a Network with an IP-852 Channel 12
Creating an IP-852 Interface 13
Configuring an IP-852 Device as a LONWORKS Router 15
Verifying LONWORKS/IP-852 Router Functionality 17

3 IP-852 Channel Parameters 21

Channel Mode 22
Aggregation 23
MD5 Authentication 24
IP-852 Channel Timing Considerations 26
Channel Timeout 26
Channel Delay 27
Packet Reorder Timer 27
Using SNTP When Creating IP-852 Channels 27
Specifying System SNTP Servers 27
Specifying SNTP Servers for a Channel or Device 29
Choosing an SNTP Server 30

4 Using NAT, DHCP, and DNS on an IP-852 Channel 31

Network Address Translation (NAT) 32
Setting up an IP-852 Channel with NAT 32
NAT Example: Simple Home Network 33
Ports and Port Mapping 34
IP-852 Device Ports 35
Creating a Virtual Wire 35
DHCP 38
DHCP Servers 39
ISP Address Allocation 39
DNS 40
DNS and the Echelon IP-852 Configuration Server 41
Linking DNS and DHCP 42
Dynamic DNS 42
How DDNS Works 42

Appendix A Troubleshooting 45

Common Troubleshooting Problems 46

Preface

You can use an IP-852 channel to implement a LONWORKS® control network over an IP network, and you can use an IP-852 channel to integrate multiple native LONWORKS® networks into one large network that uses a high-speed IP-852 channel as a backbone. With an IP-852 channel, you can use a single LNS® application to monitor and control the networks attached to the IP-852 channel remotely and use LONWORKS connections to bind the devices on the networks together, regardless of the distance between the networks. You just need to attach your IP-852 devices, LNS Server computer, and the computer running the LNS application to the same IP-852 channel.

.

Purpose

This document describes how to create an IP-852 channel and how to use the channel with any IP-852 device. The IP-852 protocol is defined by the ISO/IEC 14908-4 standard. IP-852 devices are available from multiple manufacturers, and the Echelon IP-852 Configuration Server may be used with any IP-852 compliant device from any manufacturer. Echelon IP-852 devices include the SmartServer Energy Manager, i.LON 100 Internet Server, i.LON 600 IP-852 Router, and LNS server. This document explains how to configure an IP-852 channel with the Echelon IP-852 Configuration Server, and guidelines to follow when using NAT, DNS or DHCP on the IP-852 channel.

Audience

This document is intended for Echelon customers, OEMs, and system designers and integrators with knowledge of control systems and IP networking.

Content

This guide includes the following content:

- *Introduction*. Provides an introduction to IP-852 channels, and describes the devices you can use to create and manage these channels.
- *Creating an IP-852 Channel*. Describes how to create an IP-852 channel with the Echelon IP-852 Configuration Server.
- *IP-852 Channel Parameters*. Provides details on the channel parameters you can set when creating an IP-852 channel with the IP-852 Configuration Server.
- *Using NAT, DHCP and DNS on an IP-852 Channel*. Describes considerations you should make when using NAT, DHCP and DNS on an IP-852 channel.
- *Appendix A: Troubleshooting*. This appendix can be used to diagnose common problems that could occur when you create an IP-852 channel with the IP-852 Configuration Server.

Installing the Echelon IP-852 Configuration Server

The Echelon IP-852 Configuration Server stores and distributes the configuration of the IP-852 channel, including the IP addresses of all the IP-852 devices attached to the channel. You will initially configure the IP-852 channel with the IP-852 Configuration Server, and the IP-852 Configuration Server must be running anytime you modify the configuration of the IP-852 devices on the IP-852 channel.

You can install the Echelon IP-852 Configuration Server on any computer with IP connectivity to the IP-852 devices to be configured. The IP-852 Configuration Server is available as a free download from *www.echelon.com/ilon*, and a version of the IP-852 Configuration Server is also included with many products including Echelon's SmartServer, i.LON, LonMaker®, and LNS products.

To install the standalone version of the Echelon IP-852 Configuration Server, download a copy from *www.echelon.com/ilon*, and follow the installation instructions provided with the ReadMe document that is available with the download.

Related Manuals

The documentation related to the Echelon IP-852 Configuration Server is provided as Adobe® PDF files and online help files. The PDF files are installed in the **Echelon IP-852 Configuration Server** program folder when you install the IP-852 Configuration Server. You can download the latest version of this guide, from Echelon's Web site at *www.echelon.com/docs*.

The following manuals provide supplemental information to the material in this guide. You can download these documents from Echelon's Web site at *www.echelon.com/docs*.

i.LON 600 IP-852 Router Server User's Guide	Describes how to use the i.LON 600 IP-852 Router Server.
Introduction to the LONWORKS® Platform	Provides a high-level introduction to LONWORKS networks and the tools and components that are used for developing, installing, operating, and maintaining them.
LNS® Programmer's Guide	Describes how to use the LNS Object Server ActiveX Control to develop an LNS application that can manage, monitor, and control devices on an IP-852 channel
SmartServer 2.0 Hardware Guide	Describes how to assemble, mount, and wire the SmartServer hardware.
SmartServer 2.0 User's Guide	Describes how to configure the SmartServer and use its apps to manage control networks.

For More Information and Technical Support

The **Echelon IP-852 Configuration Server ReadMe** document provides descriptions of known problems, if any, and their workarounds. To view the **Echelon IP-852 Configuration Server ReadMe**, click **Start**, point to **Programs**, point to **Echelon IP-852 Configuration Server**, and then select **ReadMe First**.

If you have technical questions that are not answered within this document or the online help files provided with the IP-852 Configuration Server, you can contact Echelon for technical support. Your Echelon product distributor may also provide technical support. To receive technical support from Echelon, you must purchase support services from Echelon or an Echelon support partner. See *www.echelon.com/support* for more information on Echelon support and training services.

You can also enroll in training classes at Echelon or an Echelon training center to learn more about developing devices. You can find additional information about device development training at *www.echelon.com/training*.

You can obtain technical support via phone, fax, or e-mail from your closest Echelon support center. The contact information is as follows:

Region	Languages Supported	Contact Information
The Americas	English Japanese	Echelon Corporation Attn. Customer Support 550 Meridian Avenue San Jose, CA 95126 Phone (toll-free): 1-800-258-4LON (258-4566) Phone: +1-408-938-5200 Fax: +1-408-790-3801 *lonsupport@echelon.com*
Europe	English German French Italian	Echelon Europe Ltd. Suite 12 Building 6 Croxley Green Business Park Hatters Lane Watford Hertfordshire WD18 8YH United Kingdom Phone: +44 (0)1923 430200 Fax: +44 (0)1923 430300 *lonsupport@echelon.co.uk*
Japan	Japanese	Echelon Japan Holland Hills Mori Tower, 18F 5-11-2 Toranomon, Minato-ku Tokyo 105-0001 Japan Phone: +81-3-5733-3320 Fax: +81-3-5733-3321 *lonsupport@echelon.co.jp*
China	Chinese English	Echelon Greater China Rm. 1007-1008, IBM Tower Pacific Century Place 2A Gong Ti Bei Lu Chaoyang District Beijing 100027, China Phone: +86-10-6539-3750 Fax: +86-10-6539-3754 *lonsupport@echelon.com.cn*
Other Regions	English Japanese	Phone: +1-408-938-5200 Fax: +1-408-328-3801 *lonsupport@echelon.com*

1

Introduction

This chapter provides an introduction to IP-852 channels, and describes the devices you can use to create and manage these channels.

Introduction to the IP-852 Channel

An IP-852 channel carries ISO/IEC 14908-1 packets enveloped in ISO/IEC 14908-4 packets. Unlike traditional LONWORKS channels that use a dedicated physical wire to create connections between the devices on the channel, an IP-852 channel uses a shared IP network to connect IP-852 devices and is defined by a group of IP addresses. These IP addresses form a channel that connects *IP-852 devices* on a shared control network so they can communicate with each other. IP-852 devices include the SmartServer Energy Manager, i.LON 100 Internet Server, i.LON 600 LONWORKS/IP-852 Router, LNS Server computers, and LonMaker® computers. Devices from other manufacturers that comply with the LONMARK IP-852 channel definition can also be used as IP-852 devices. For systems using an LNS server, an IP-852 channel enables an LNS remote full client to connect directly to a LONWORKS network and perform monitoring and control tasks.

The concept of an IP-852 channel is similar to a Virtual Private Network (VPN). Each IP-852 device in the system is aware of its peers and each IP-852 device keeps peer information in its routing tables so it can forward LONWORKS packets to the correct IP address or addresses.

Figure 1.1 shows a typical channel configuration in which three SmartServers are used to create an IP-852 channel connecting three TP/FT-10 channels, each of which contains the devices installed on a different floor in a building. The circled portion of the diagram represents the IP-852 channel connecting the three SmartServers. As a result of this connection, a single application can connect to devices on all three of the TP/FT-10 channels in the building, and monitor and control the entire building.

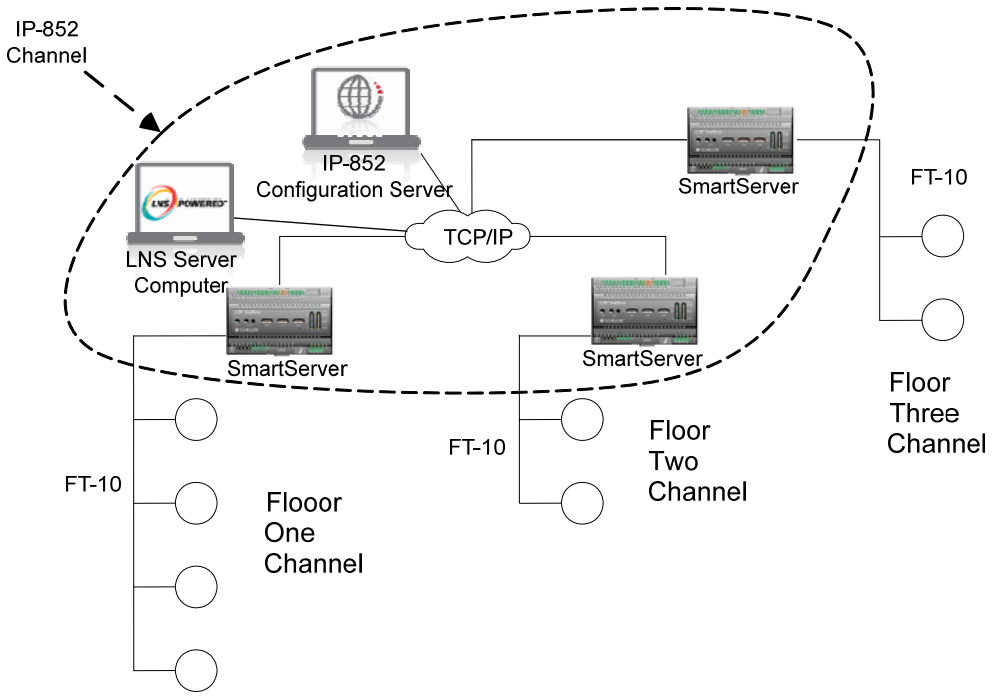

Figure 1.1 An IP-852 Channel

Figure 1.1 shows the IP-852 Configuration Server inside the IP-852 channel. The IP-852 Configuration Server stores the configuration of the IP-852 channel, including the IP addresses of all the devices and routers installed on the channel. You will initially configure the IP-852 channel with the IP-852 Configuration Server, and the IP-852

Configuration Server must be running anytime you modify the configuration of the devices on the IP-852 channel. You can run the IP-852 Configuration Server on any computer with access to the IP network containing the IP-852 channel. Chapters 2 and 3 of this document describe how to use the IP-852 Configuration Server. The IP-852 Configuration Server is available as a free download from *www.echelon.com/ilon*, and a version of the IP-852 Configuration Server is also included with many products including Echelon's SmartServer, i.LON, LonMaker®, and LNS products.

The IP-852 channel definition accounts for the potentially large latencies introduced by large IP networks such as the Internet. This enables key control network services such as duplicate packet detection to function correctly over a high-latency IP network.

A complete installation may contain many IP-852 devices and computers—all sharing a single IP-852 channel. Because the IP-852 channel can exist on any IP network, a system may span the entire globe as easily as it spans a single building, as shown in Figure 1.2.

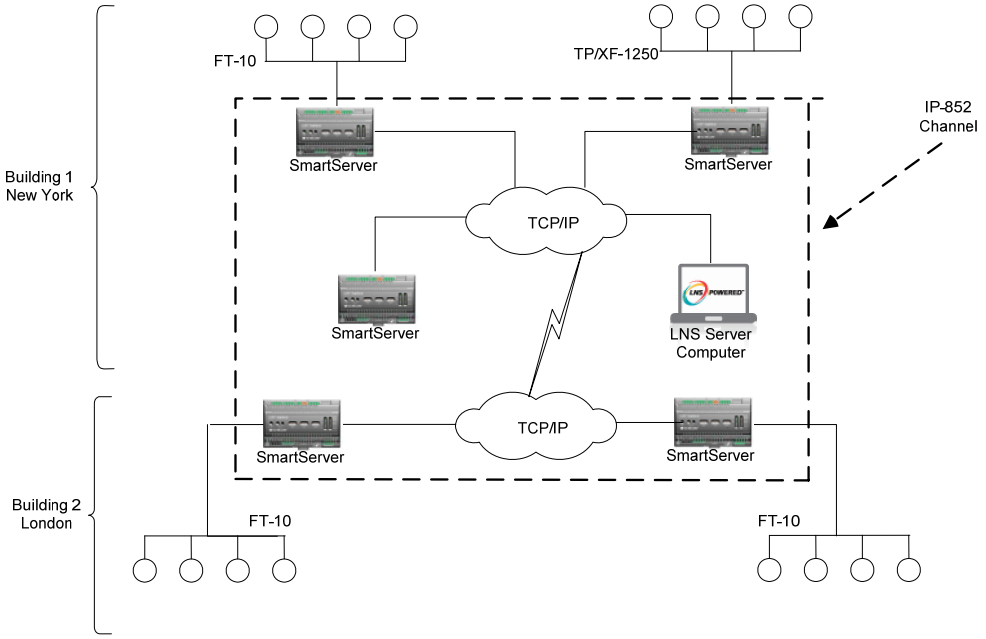

Figure 1.2 Large LONWORKS Network using an IP-852 Channel

Note: A single IP-852 channel may contain up to 256 IP-852 devices. If your installation requires more than 256 IP-852 devices, you must create multiple IP-852 channels.

2

Creating an IP-852 Channel

This chapter describes how to create an IP-852 channel with the Echelon IP-852 Configuration Server.

Creating an IP-852 Channel

You can create an IP-852 channel by configuring the IP-852 devices that are to be attached to the IP-852 channel, and entering information about each IP-852 device in the IP-852 Configuration Server.

This section describes how create an IP-852 channel using an example network with two devices on an IP backbone to illustrate the process. In Figure 2.1, a LONWORKS device on channel 1 is bound to a device on channel 2 across an IP-852 backbone. The computer running the IP-852 Configuration Server resides on the IP-852 channel, and has access to both IP-852 devices through an IP connection. The computer running the LonMaker software is connected to channel 1. To simplify the network, you can run the LonMaker software and the IP-852 Configuration Server software on a single computer.

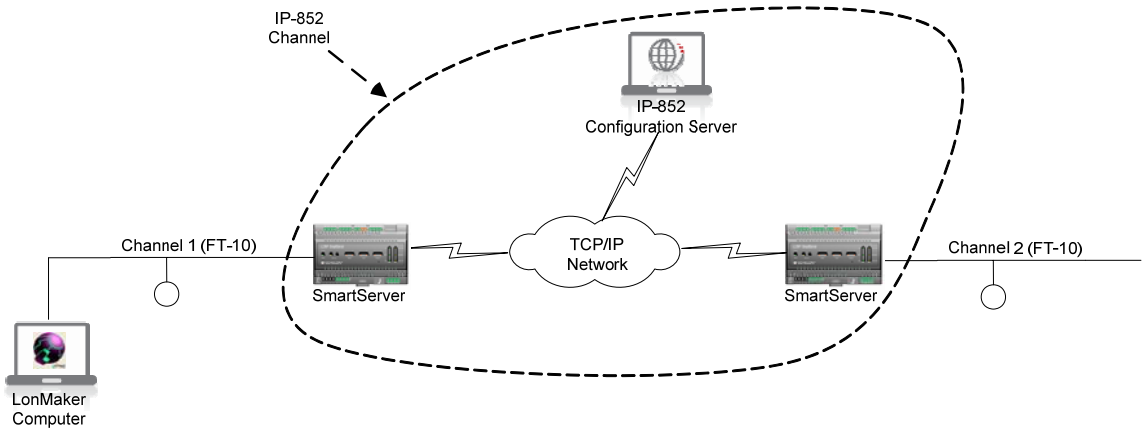

Figure 2.1 Setting Up an IP-852 Channel

To create a network like the one illustrated in Figure 2.1, follow the steps below:

1. If you do not already have an Echelon IP-852 Configuration Server installed on a computer with access to the IP network, download it from *www.echelon.com/ilon*, and install the IP-852 Configuration Server as described in the ReadMe document that accompanies the download.
2. Set the IP address, subnet mask, and default gateway for all the IP-852 devices you plan to use on the channel. In Figure 2.1, the two IP-852 devices are SmartServers, although your network could contain any IP-852 devices. Consult the documentation for your IP-852 device for instructions on how to perform this step.
3. Start the Echelon IP-852 Configuration Server application. To do this, click **Start**, point to **Programs**, point to **Echelon IP-852 Configuration Server**, and then select **IP-852 Configuration Server**. The IP-852 Configuration Server main dialog opens.

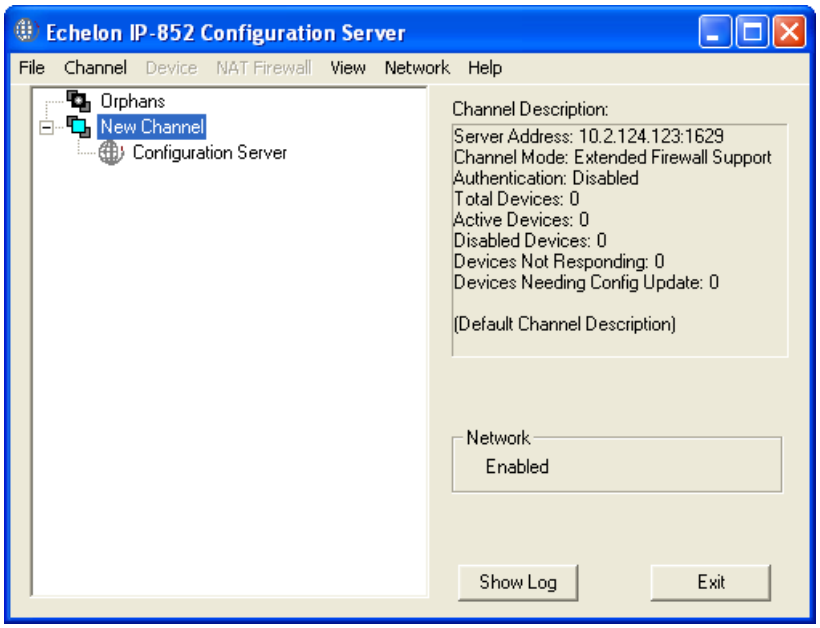

Figure 2.2 Echelon IP-852 Configuration Server

4. Verify that the IP-852 Configuration Server is attached to your IP network. The **Network** status box should indicate **Enabled**. If it does not, select **Enabled** from the **Network** menu. The IP-852 Configuration Server should correctly detect and display the IP address of your computer in the Channel Description window.

   To verify the IP-852 Configuration Server computer's IP address, click **Network** and then click **Settings**. The **Network Settings** dialog opens. Confirm that the IP address of the IP-852 Configuration Server is shown in the **IP Address or Host Name** property as shown in Figure 2.3.

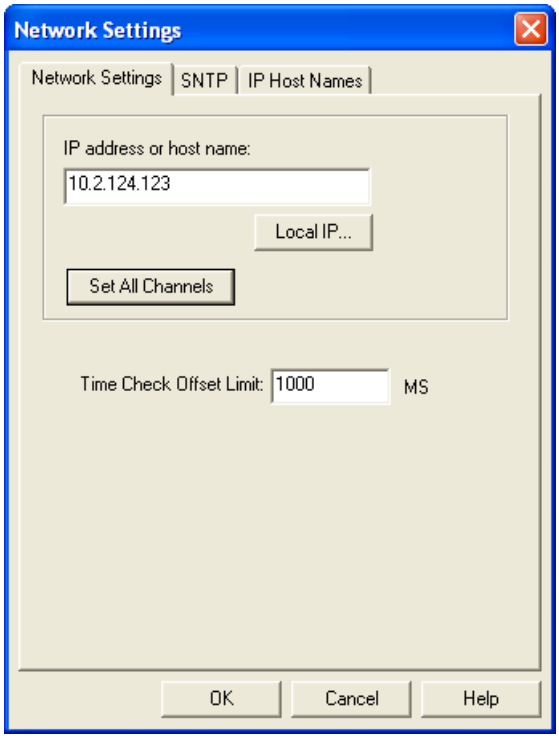

Figure 2.3 IP-852 Configuration Server Network Settings

5. If your computer has more than one IP address assigned to it, you can click **Local IP** and specify the IP address to be used by the IP-852 Configuration Server.
6. The defaults for the channel properties will work in cases where network delays are low. If you anticipate large delays in the IP segment (many routers / hops, or slow media segments), you can adjust the channel property settings and/or use SNTP time servers to synchronize IP-852 Router member devices. See Chapter 3 for more information on this.
7. To configure the channel mode, right-click the **New Channel** entry and select **Properties** from the shortcut menu. Select **Backward Compatible, Standard EIA-852** or **Extended Firewall Support** mode. See the *Channel Mode* section in Chapter 3 for more detailed information on these settings.
8. From the IP-852 Configuration Server main dialog, right-click the new channel, and select **New Device** from the shortcut menu. An icon representing an IP-852 device is added to the channel.
9. Right-click on the new device and select **Rename Device** from the shortcut menu to enter a name for the device.
10. Right-click the device and select **Device Properties**. The device properties dialog opens.

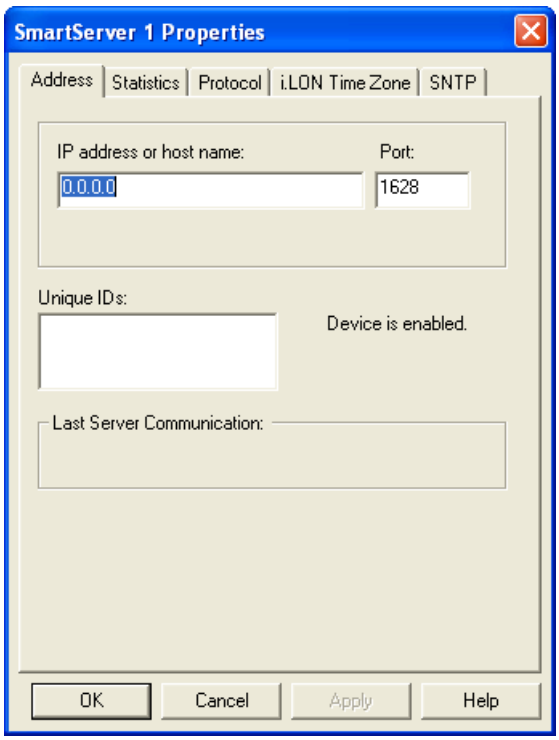

Figure 2.4 IP-852 Configuration Server Device Properties: Address Tab

11. Enter the IP address of the IP-852 device and click **Apply**. This is the same address that you assigned to the IP-852 device using the setup Web pages.

    If you use a host name, it must be registered in a DNS server that is available to the IP-852 Configuration Server computer.

12. Click the **SNTP** tab, and then select the **Use Channel Default** check box.
13. Click the **Protocol** tab, and then select the **Use Channel Default** check box.

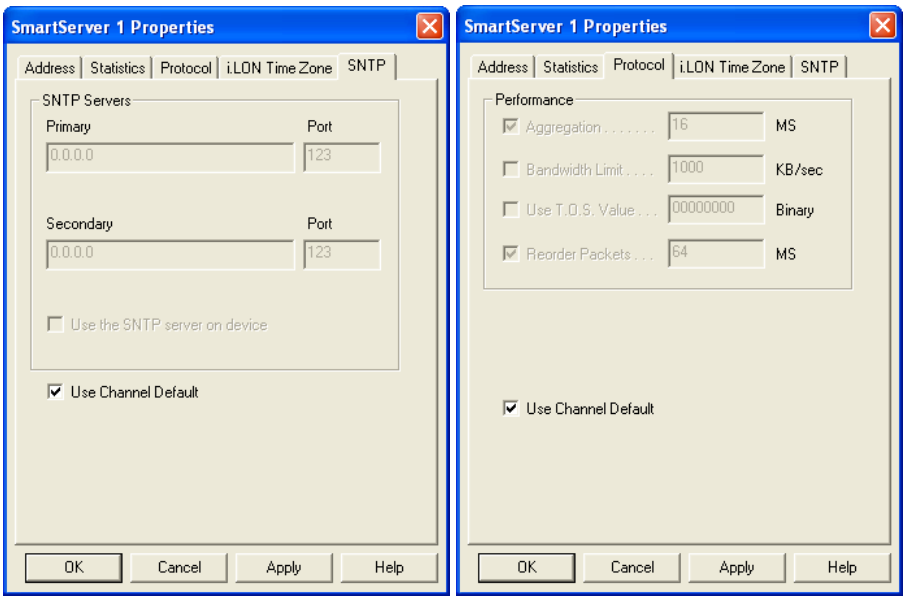

Figure 2.5 IP-852 Configuration Server Device Properties: **SNTP** and **Protocol** Tabs

14. Click the **i.LON Time Zone** tab, and then set the time zone to correspond with the geographical area of the device.
15. Click **Apply**.
16. Repeat steps 6 – 15 for each IP-852 device to be added to the IP-852 channel. You can change the IP-852 device's settings (for example, IP address, local port, and so on) later. When you modify IP-852 device settings, update the device's configuration with the device software before modifying the device's settings in the IP-852 Configuration Server. **The IP-852 Configuration Server must be running when you modify the device's configuration with the device software. You can keep the IP-852 Configuration Server running at all times.**
17. Either click **Channel** and then click **Update Members**, or click **Device** and then click **Update Device**. The IP-852 Configuration Server automatically attempts to set up the device's routing tables by updating all members of the channel with the current channel configuration and membership.

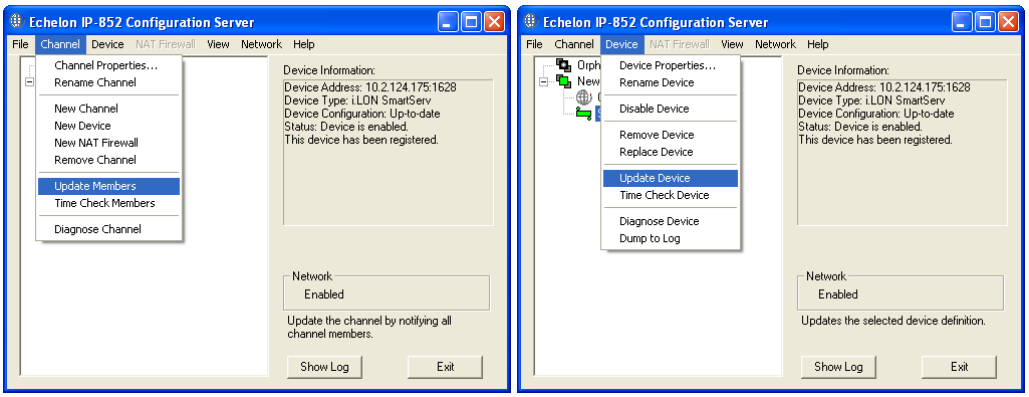

Figure 2.6 IP-852 Configuration Server: Update Members and Update Device

When you select **Update Members** or **Update Device,** a communication process starts between the IP-852 Configuration Server and the IP-852 devices that you added to the IP-852 channel. You can view this process by clicking **Show Log**.

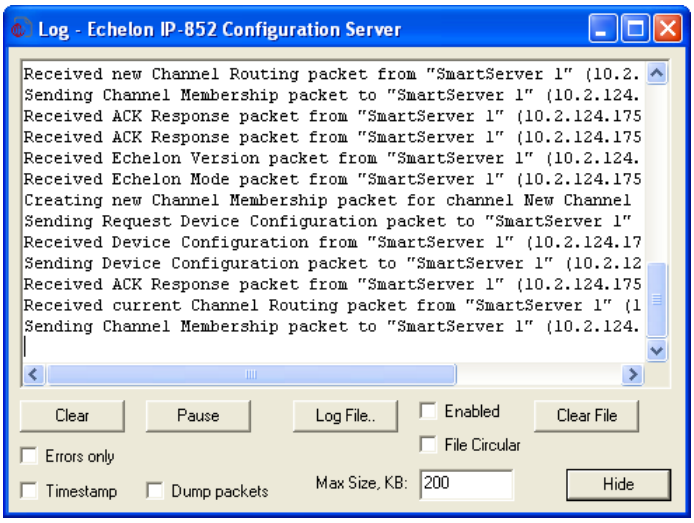

Figure 2.7 Log Dialog

Checking IP-852 Device Status

If any information between IP-852 devices on the IP-channel needs to be updated, the IP-852 Configuration Server will send updated information to each IP-852 device. Success or failure of this step is reflected in the IP-852 Configuration Server log screen and the color of the devices in the navigation pane on the left side of main dialog. The meaning of each color of the device status is listed in Table 2.1.

Table 2.1 IP-852 Configuration Server Device Status Indicator

Color	**Status Description**
Green	Normal. The IP-852 Configuration Server has communicated with the IP-852 device and configuration is up to date.
Yellow	Normal, but the Time Check failed for device. The IP-852 device's time differs from the time on the computer running the IP-852 Configuration Server by more than a few milliseconds. This usually means that either the IP-852 device or the computer is not referencing an SNTP server to set the local time. The system may work with some yellow devices, but the probability of data loss is increased. You can provide an SNTP server to both the computer and the IP-852 device so that their time bases can be automatically synchronized. When synchronized, the yellow icon turns green.
Red	Communication with the device has failed. The IP-852 Configuration Server cannot communicate with the IP-852 device. This usually occurs when no response is received from a device to which a request was made. This may happen if the IP-852 device is powered down, disconnected from the IP network, or has been configured improperly with the wrong IP address/subnet mask/gateway etc. It may also occur if an intervening NAT gateway has not been configured to statically map ports to the IP-852 device as described above. Make sure that all security and IP settings are configured properly.
Orange	The IP-852 device's configuration is out of date or the IP address has not been specified (0.0.0.0). This indicates work in progress. When the IP-852 Configuration Server updates the IP-852 device, the icon turns green. in a large channel (> 40 devices) this can take several minutes. Changing a connection in a network management tool can require that the routing tables in every IP-852 device on the IP-852 channel be updated. In this case, you may see many icons turn orange, and then one-by-one turn green again when their routing tables have been updated.

Red/White Checkerboard	Disabled. Typically, the user right clicked on the IP-852 device in the IP-852 Configuration Server tree and selected **Disable Device** from the shortcut menu.
Cyan	The IP-852 Configuration Server has not yet attempted to communicate with the IP-852 device. The IP-852 Configuration Server may be busy communicating with other channel members (this is common on a large channel). If the IP-852 Configuration Server appears not to be attempting communication, click **Show Log** and monitor the progress. Click **Channel** and then click **Update Members**.

Backing Up the IP-852 Configuration Server Database

To back up all the files associated with a LONWORKS network that contains an IP-852 channel, include the **LTIPCDB.BIN** file in your backup. The location of this file is stored in the **LonWorks Data Path** string entry in the **HKEY_LOCAL_MACHINE\Software\LonWorks** registry key.

Managing Multiple IP-852 Configuration Server Databases

The IP-852 Configuration Server maintains a single database in the LONWORKS **DataPath** folder. The IP-852 Configuration Server database includes the current configurations of the IP-852 Configuration Server, IP-852 channels, and IP-852 devices you have created, and the current network settings. You cannot manage multiple IP-852 configurations at the same time; however, you can create multiple IP-852 configurations for separate sites by backing up the IP-852 Configuration Server database after configuring a site, and then restoring the database for an alternate site. The IP-852 Configuration Server uses the database in the LONWORKS DataPath folder.

Creating a Network with an IP-852 Channel

You can create a network containing an IP-852 channel and multiple IP-852 devices. One or more of the IP-852 devices may be routers to native LONWORKS channels, typically TP/FT-10 free topology twisted pair or TP/XF-1250 high-speed twisted pair channels. You can install devices in the network using a network management tool such as the LonMaker Turbo Integration Tool. For the best performance, you can attach the network management tool to the IP-852 channel, making the computer running the network management tool another IP-852 device on the IP-852 channelFigure 2.8 shows an example of a LONWORKS network that contains an IP-852 channel with a network management tool attached to the channel.

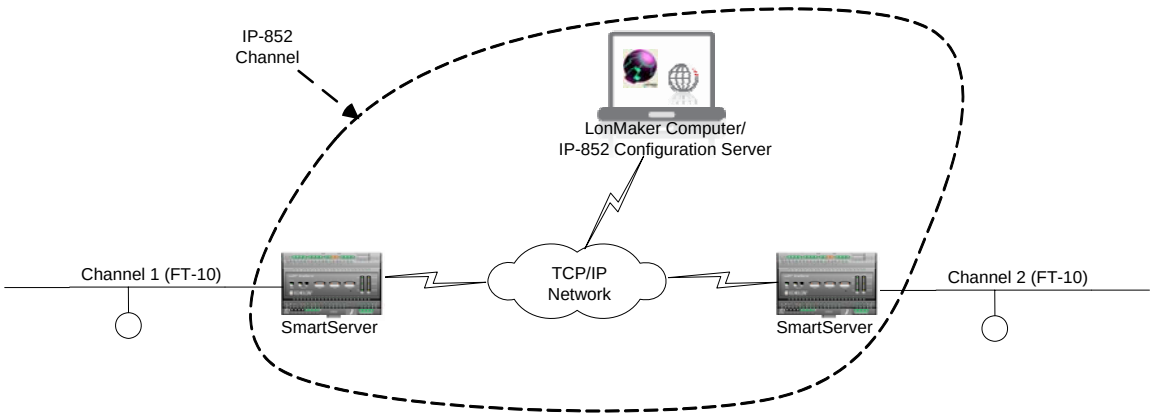

Figure 2.8 Typical Network Containing an IP-852 Channel

To create a LonWorks network with an IP-852 channel using an LNS network management tool such as the LonMaker tool, follow steps:

1. Create an IP-852 channel containing the LONWORKS/IP-852 routers for the channel as described in the previous section.
2. Create an IP-852 interface for the computer with the network management tool using the LONWORKS Interfaces application.
3. Add the IP-852 interface created in step 2 as an IP-852 device in the IP-852 Configuration Server. See the previous section, *Creating an IP-852 Channel*, for more information on how to do this.
4. Configure the IP-852 devices that are routers to other LONWORKS channels as LONWORKS routers.
5. Verify that your IP-852 device is functioning as a LONWORKS/IP-852 router.

The following sections describe how to perform steps 2, 4, and5.

Creating an IP-852 Interface

You can attach your network management tool directly to the IP-852 channel to get the best performance. If you are using a network management tool based on the LNS Network Operating System such as the LonMaker Turbo Network Integration Tool, you can attach both the computer with the LNS Server and the computer with the network management tool to the IP-852 channel. Both the LNS Server and the network management tool may be running on the same computer. You will have to create an IP-852 interface definition on your LNS Server computer, your network management computer, and on any other LNS remote client computers that will be attached to the IP-852 channel. To create an IP-852 interface definition, follow these steps

1. Open the LONWORKS Interfaces application in the Windows Control Panel. To do this, click **Start** on the taskbar, click **Control Panel**, and then double-click **LonWorks Interfaces**.

   Note: The following steps describe how to create an IP-852 interface using OpenLDV 4.0. If you are using a different version, the subsequent steps may vary slightly.
2. Click **Interface**, point to **Add**, and then either click **IP-852 Interface** or click **New Interface** and then click **IP-852** in the **Select Interface Type** dialog.
3. The **Add Network Interface Wizard** dialog opens.

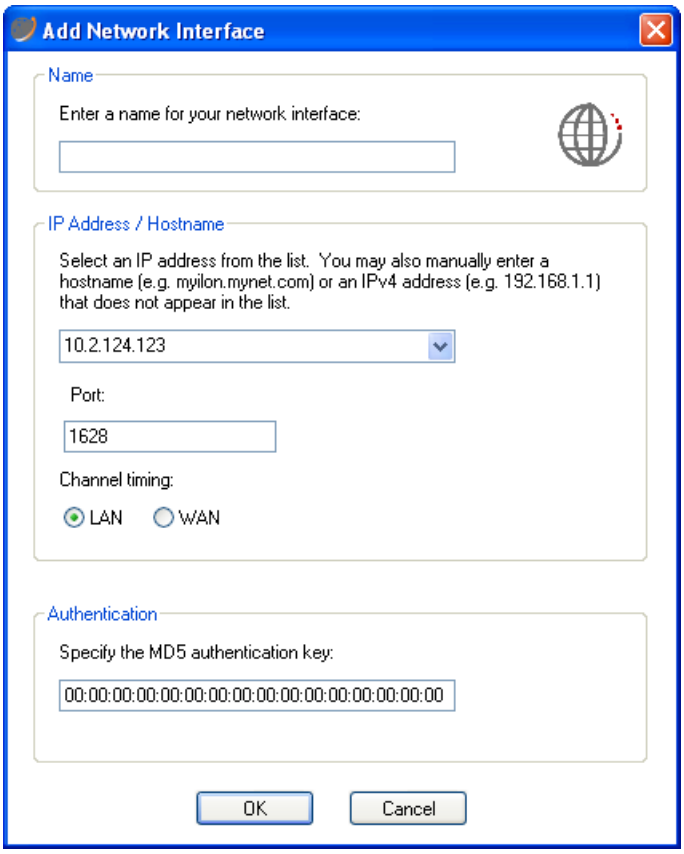

Figure 2.9 Add Network Interface Wizard Dialog

4. Enter the following properties for the IP-852 interface:

Name — Enter a name for the IP-852 interface definition that is unique to your computer.

IP Address / Hostname

IP Address — Enter the IP address to be used by the IP-852 interface definition on your computer.

Each IP-852 interface definition must use a unique IP address/port combination. This property defaults to the IP address of your computer's IP network card. If your computer contains multiple network cards, select the IP address from the list box that appears.

You can also manually enter an IP address that is not already defined on your computer. In this case, a warning icon appears next to the IP Address property; however, you can still enter the non-defined IP address for the IP-852 interface definition. The non-defined IP address is marked by "***".

Note: The IP-852 interface definition is not functional until the IP address has been defined on your computer.

Port — Enter the port number to be used by the IP-852 interface definition on your computer. The default port is **1628**.

You can change the port number; however, you must avoid any conflicts with other applications that are using the IP network card. Each IP-852 interface definition you create with the LONWORKS Interfaces application must use a unique port. If you modify the port used by an IP-852 interface definition, the change will be implemented once all applications using the IP-852 interface definition are closed.

Channel Timing Select the channel delay. You have the following two choices:

- **LAN**. Select this if your IP-852 channel spans a local area network. This is the default.
- **WAN**. Select this if your IP-852 channel spans a wide area network. This results in a larger channel delay value.

Authentication If the IP channel used by this IP-852 interface definition is using authentication, enter the authentication key as a 32-character hexadecimal string representing a 128-bit MD5 key. The following is an example authentication key:

A9048749F4BF89590310C547BD4594D7

You can enable authentication for an IP-852 channel with the IP-852 Configuration Server. See *MD5 Authentication* in Chapter 3 for more information on using authentication on the IP-852 channel.

Configuring an IP-852 Device as a LONWORKS Router

An IP-852 device may be either a native IP-852 device or a router to a native LONWORKS channel. An LNS server may be configured as a native IP-852 device, and any IP-852 to native LONWORKS compliant router may be configured as a LONWORKS router. Examples of native LONWORKS channels are TP/FT-10 free topology twisted pair and TP/XF-1250 high-speed twisted pair. IP-852 to LONWORKS routers are available from multiple manufacturers. Echelon's IP-852 to LONWORKS routers include versions of the SmarServer Energy Manager and i.LON 100 Internet Server with IP-852 routing enabled, and the i.LON 600 LONWORKS/IP-852 router.

The procedure that you will use to configure an IP-852 device as a LONWORKS router depends on the network management tool that you use to configure you LONWORKS network. You can use any network management tool that complies with the ISO/IEC 14908-1 Control Network Protocol. The following procedure illustrates how to use the LonMaker tool to integrate an IP-852 router with the LONWORKS network described in Figure 2.8. For more information on the LonMaker tool, see the *LonMaker User's Guide*.

1. With the IP-852 Configuration Server running, create a new LonMaker network and specify the IP-852 network interface created with the LONWORKS Interfaces application in the previous section as the network interface. Change the name of *Channel 1* to *IP852 Channel* and assign specify **IP-10L** (if using a local IP network) or **IP-10W** (if using a wide area IP network, such as the Internet) as the transceiver type in the Channel's properties.

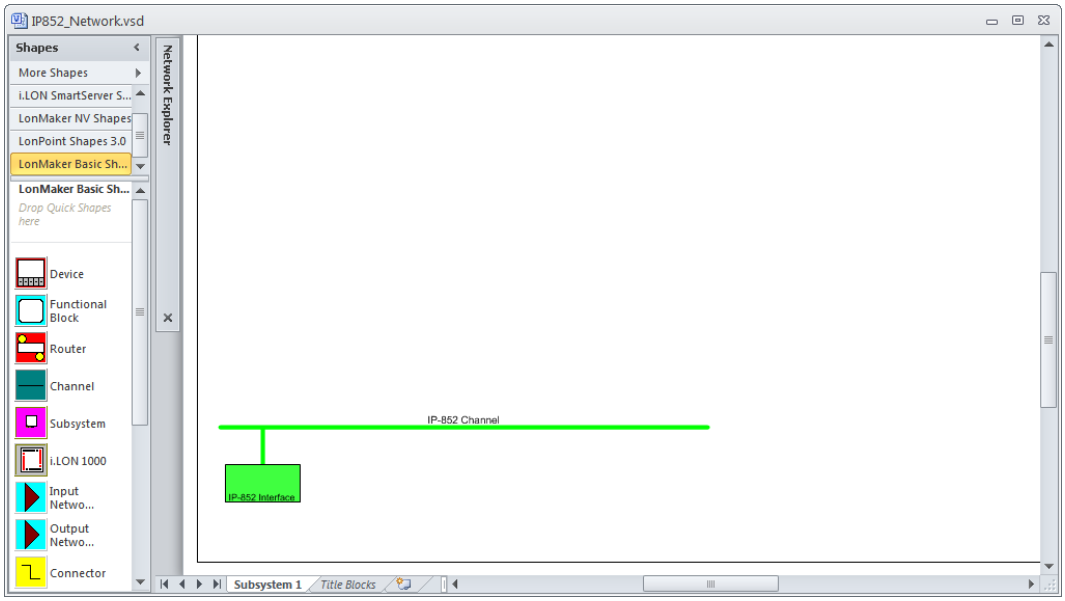

Figure 2.10 Creating a New Channel Using LonMaker

2. Drag channel shapes to the drawing representing the *FT-10 Channel 1* and *FT-10 Channel 2* and assign **TP/FT-10** as the *Transceiver Type for both channels*.
3. Drag two LONWORKS Router shapes to the drawing:
   - *iLONRTR_1*. Connects *IP-852 Channel* (Channel A) *to FT-10 Channel 1* (Channel B).
   - *iLONRTR_2*. Connects *IP-852 Channel* (Channel A) *to FT-10 Channel 2* (Channel B).
4. Commission the *iLONRTR_1* and *iLONRTR_2* routers, and leave them in the Online state.

   If your IP network contains large latencies, you may need to change the network timing properties as described in Chapter 3.

   Note: Verify that the IP-852 Configuration Server is running when you commission the IP-852 routers or make any other changes to your LONWORKS network, such as adding or deleting devices or connections. You can keep the IP-852 Configuration Server running at all times so that you don't forget to start it when it is required.

   Once the IP-852 devices have been installed and commissioned, you can add devices, functional blocks, and connections just as you would in any LonMaker network. See the *LonMaker User's Guide* for more information. For example, Figure 2.11 shows the network described above with a Digital Input device (*DI-10*) device added to *FT-10 Channel 1*, and one of the digital output network variables from the DI-10 device bound to a DO device (*DO-2*) connected to *FT-10 Channel 2* (switch band to lamp).

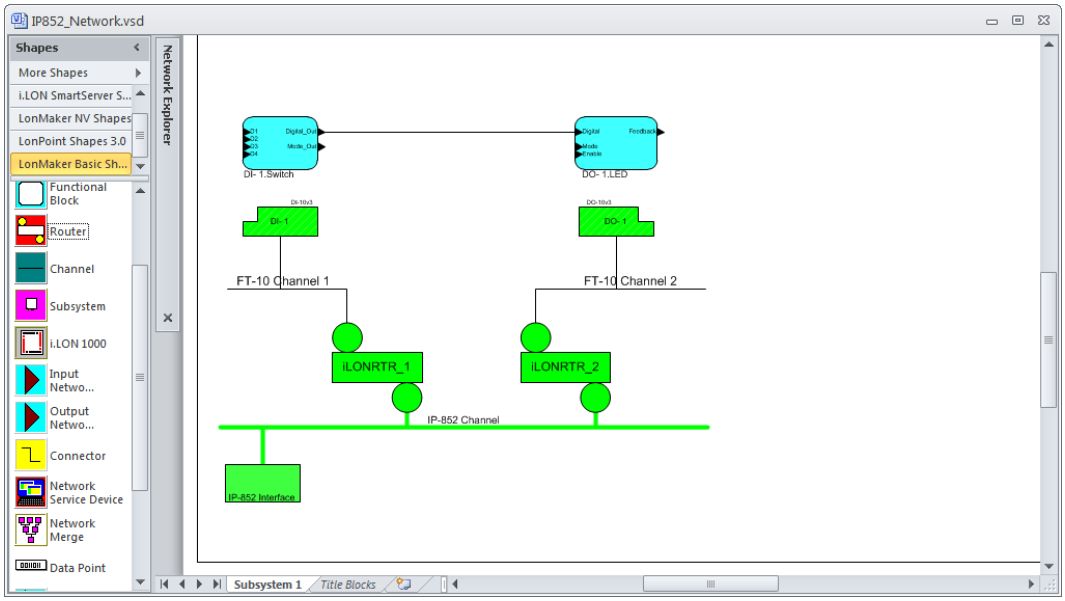

Figure 2.11 IP-852 Routers Configured on a LONWORKS Network

Verifying LONWORKS/IP-852 Router Functionality

You can verify that an IP-852 device that you have configured as a LONWORKS/IP-852 router is functioning as a LONWORKS network. You will typically use the network management tool that you used to configure the IP-852 device as a LONWORKS router to do the verification. This section describes how to use the LonMaker Integration Tool to do the verification.

To verify that the IP-852 devices in the network shown in Figure 2.11 are working correctly, right-click on the network variable connection between DI-10 (switch) functional block and DO-10 (LED) function block and select **Monitor Input Value**. Verify that the value displayed on the connection in LonMaker is tracking the value of the Digital Output network variable in *DI-10 functional block*. If you do not see network variable updates reported by the LonMaker tool, there is a problem. Refer to Table 2.2 for troubleshooting information.

Table 2.2 Troubleshooting the IP-852 Device

Symptom	Probable Cause	Corrective Action
No service pin message is received from the near router (*i*LONRTR_1 in Figure 2.10).	There is a problem with network connectivity, or the network interface in the computer may not be functioning properly.	Test connectivity between the network interface driver and the network interface card in the computer using LONWORKS Interfaces in the Windows Control Panel . Test to make sure that the LONWORKS Interfaces application receive a service pin message from some other device on the same channel as the IP-852 device.
	The IP-852 device may not be physically connected to the network interface.	Check the network wiring between the computer and the IP-852 device.
	No IP address has been assigned to the IP-852 device.	Configure the IP address in the IP-852 device using the setup Web pages and the IP-852 Configuration Server.
	If you are using an i.LON 600 IP-852 router as the near router, the router application has not yet been created on the IP-852 device.	Create the LONWORKS router application using the Console Application, as described in Chapter 5 of the *i.LON 600 LonWorks/IP-852 Router User's Guide*.
	If you are using a SmartServer or an i.LON 100 Internet Server as the near router, it may not be licensed or configured to operate as an IP-852 router.	License and configure the SmartServer or i.LON 100 server to operate as an IP-852 router, as described in Chapter 3 of the *SmartServer 2.0 User's Guide* or *i.LON 100 e3 User's Guide.*
	The IP channel properties have not been properly set.	For a local Intranet, make sure the channel property/transceiver type in the LonMaker tool is IP-10L. For a WAN (Internet), choose IP-10W.

Symptom	Probable Cause	Corrective Action
The near router (iLONRTR_1) commissions successfully, but no service pin message is received from the far router (iLONRTR_2).	There is a problem with the IP-852 channel setup.	Be sure the IP-852 Configuration Server is running when you commission the devices on the IP-852 channel. Verify that the near router is online and that the IP-852 Configuration Server reports connectivity among all members of the IP-852 channel (for example, all icons are green).
Both IP-852 device routers commission successfully, but the device on the far side of iLONRTR_2 (the DI-10 device) does not install correctly.	There is a problem with the IP-852 channel or the device being installed.	Verify that the far router is online. Test devices on the far side channel (using the LonMaker Test command). If the test succeeds for any other device on the far channel, the IP-852 channel is working, and the improperly working device may not be installed correctly. If no test succeeds, verify connectivity between the IP-852 devices in the main dialog status window of the IP-852 Configuration Server.
An IP-852 device added to an IP-852 channel using the IP-852 Configuration Server remains red in the device tree.	IP connectivity problem: the IP-852 Configuration Server is not able to communicate with the IP-852 device on the defined IP-852 channel.	Verify that the computer running the IP-852 Configuration Server can ping the IP-852 device. To perform a ping, open the Windows Command Prompt (in the Accessories program folder) and type “ping X.X.X.X” (the device’s IP address). You should receive a reply from your device. Examine the IP-852 Configuration Server trace window for clues as to what may be going wrong. Verify that you can ping the IP-852 Configuration Server computer or members of the IP-852 channel using the Windows Command Prompt.

Symptom	Probable Cause	Corrective Action
The IP-852 device on the IP-852 channel pings successfully, but will not commission.	Address translation may take place somewhere between the two devices. The router application does not exist.	Make sure that the IP address of the target IP-852 device matches the IP address defined for it in the IP-852 Configuration Server. If you are using an i.LON 600 router, determine if the router application exists by using the **listapp** command in the Console Application. Create the router app with the **createapp Router** command if it does not exist. If you are using a SmartServer or i.LON 100 router, make sure the device is licensed and configured to operate as an IP-852 router.

3

IP-852 Channel Parameters

This chapter provides details on the channel parameters you can set when creating an IP-852 channel with the Echelon IP-852 Configuration Server.

Channel Mode

You can set the IP-852 device channel mode using one of three options in the **New Channel Properties** dialog box. If you are using an LNS Turbo Edition server (LNS 3.2) or higher, it is compatible with all three channel modes.

To access the **New Channel Properties** dialog box, start the IP-852 Configuration Server, right-click the **New Channel** entry, and then click **Channel Properties** on the shortcut menu.

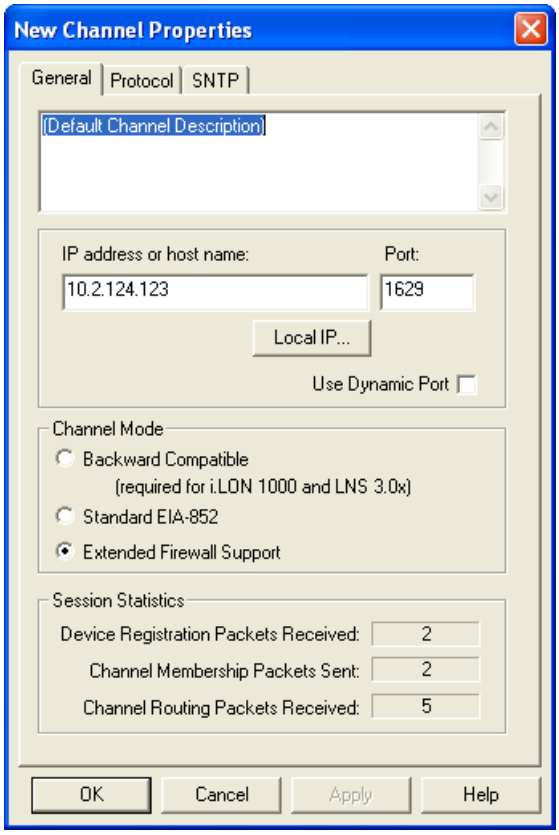

Figure 3.1 New Channel Properties Dialog Box

Table 3.1 describes each channel mode.

Table 3.1 Channel Modes

Setting	Description
Backward Compatible	Select this option if your channel will contain any legacy i.LON 1000 servers or LNS 3.0 LONWORKS /IP network interfaces. This causes the IP-852 device to operate using a protocol that is compatible with these devices, but is not strictly EIA-852 compliant. In backward compatible mode, you can use a maximum of 40 devices. If you select this option, you can only have one device located behind each NAT firewall, the i.LON 1000 and LNS 3.0 devices cannot be located behind a NAT firewall, and you cannot have duplicate IP addresses or duplicate port assignments.
Standard EIA-852	Select this option if your channel contains any mix of IP-852 compliant devices. You can use a maximum of 256 IP-852 devices per channel in Standard EIA-852 mode. In Standard EIA-852 mode, you can only have one device located behind each NAT firewall. The IP address (including the port assignment) must be unique.
Extended Firewall Support	Select this option whenever your IP-852 channel crosses an IP firewall, regardless of whether the firewall is using Network Address Translation (NAT). Depending on the particular firewall and its configuration, this option may be required. In addition, this will allow you to place more than one IP-852 router device behind an NAT firewall, and to create multiple IP-852 interfaces in the same channel using the same IP address (but with different ports). If this option is disabled, only one device may reside behind a NAT firewall, and all devices on the channel must have unique IP addresses. This option extends the EIA-852 protocol in a way that is not strictly compliant with that standard, though it should still be compatible with other IP-852 devices. You can use up to 256 devices per channel in this mode.

Aggregation

Click the **Protocol** tab and then select the **Aggregation** check box to enable aggregation on the IP-852 channel. Each IP-852 router aggregates LONWORKS packets for transport over the IP channel. LONWORKS packets are relatively small in size and often arrive at the IP-852 router in bursts or at a high rate. Aggregating packets decreases the bandwidth necessary to send packets over IP, decreases IP network traffic, and increases the performance of the IP-852 router.

The IP-852 router is set through the IP-852 Configuration Server to use aggregation by default. The aggregation time parameter controls how long the router will wait for

packets. The resolution of the timer depends on the IP-852 device. The resolution for SmartServer and i.LON devices is in multiples of 10 milliseconds. The default aggregation time is **16** milliseconds.

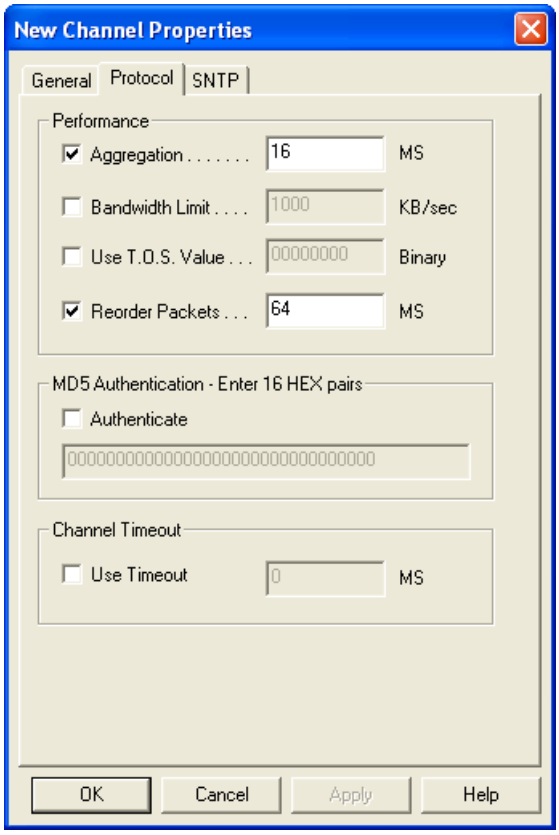

Figure 3.2 Aggregation Settings

If the network is idle and a single LONWORKS packet arrives at the IP-852 device, the aggregation timer starts and the first packet is sent across the IP channel without delay. If the network remains idle, the timer resets. However, if another LONWORKS packet arrives within the aggregation time period, the router waits the designated time for subsequent packets to arrive (anticipating a burst) so it can aggregate before sending them onto the IP channel.

MD5 Authentication

MD5 authentication is a channel-wide property that uses an authentication key to set security on an IP-852 channel. The authentication key is used to calculate the MD5 digest. When authentication is enabled and the IP-852 device prepares to send an IP packet, the IP-852 device uses the authentication key and the public MD5 algorithm to compute a digest over each LONWORKS packet in the UDP payload.

For standard channels, the packet format is described in the ISO/IEC 14908-4 standard for sending LONWORKS packets over IP. The computed digest is appended to the end of the packet and the packet is sent over the network. Authentication digests are appended to both LONWORKS data packets and the IP-852 Configuration Server control packets. One or more IP-852 devices receive the packet and use their authentication key to compute a digest over the same payload (not including the appended digest). The receiving IP-852 device compares the digest it computed to the one that was sent in the

packet. If the digests match, the packet is authentic. If the digests do not match, the packet is considered to have been corrupted, tampered with, or otherwise unacceptable, and is discarded. The digest includes the entire packet, which contains a time stamp for preventing replay attacks when used in conjunction with a configured channel timeout value. For more information on the MD5 algorithm refer to RFC 1321.

Note: MD5 authentication should not be confused with authenticated LONWORKS messaging. MD5 authentication applies to IP packets; authenticated LONWORKS messaging applies to native LONWORKS packets.

The authentication key, consisting of 16 hex pairs, is set for each IP-852 device using the device's configuration interface (for example, using SmartServer configuration Web pages). Authentication is enabled and the authentication key set for the IP-852 channel through the IP-852 Configuration Server. To reset a lost authentication key, you must obtain physical access to the device and reset the key through the device's configuration interface.

To enable authentication and set the authentication key on an IP-852 channel, follow these steps:

1. Click **Channel** and then click **Channel Properties**, or right-click on a channel and click **Channel Properties** in the shortcut menu. Click the **Protocol** tab.

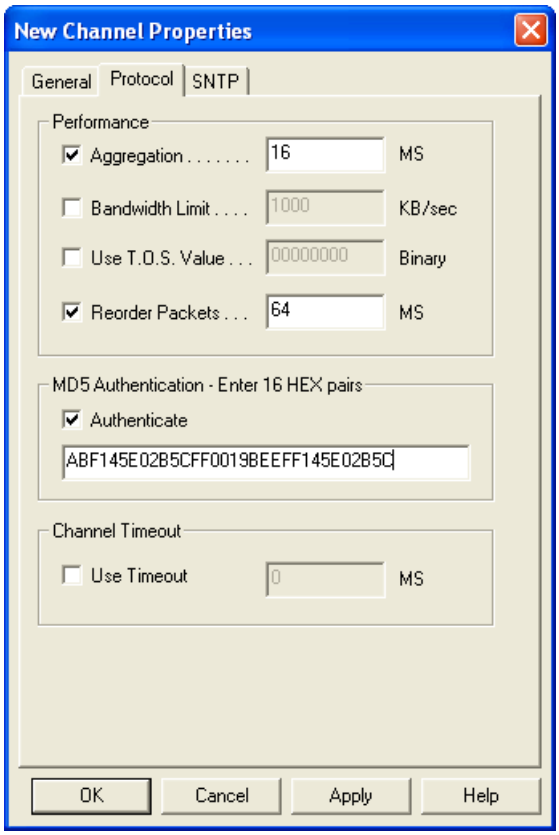

Figure 3.3 Protocol Tab

2. Select the **Authenticate** check box to enable authentication, and then enter 16 hex pairs that represent the MD5 authentication key into the entry field. The following is an example key: ABF145E02B5CFF0019BEEFF145E02B5C.

All authentication keys within a single network must match. Verify that you have previously entered the same authentication key on all the IP-852 devices defined on this channel

To disable authentication on a channel that has authentication enabled, clear the **Authenticate** check box and click **Apply**.

IP-852 Channel Timing Considerations

When designing an IP-852 channel over an IP network that might have a large latency, such as the Internet, you may need to adjust three timing parameters when configuring the channel. You ca set two of the timing parameters, *Channel Timeout* and *Reorder Packets*, using the IP-852 Configuration Server. You can set the *Channel Delay* using an application network management tool such as the LonMaker tool.

On local area networks, set a **Channel Timeout** if MD5 Authentication is used, disable **Reorder Packets**, and set the **Channel Delay** for the channel to twice the aggregation timer.

On networks using the Internet, set the **Channel Timeout** and **Reorder Packets** values to be consistent with the **Channel Delay** parameter. Table 3.2 specifies how to approximate the timing values for network implementations using the Internet.

Table 3.2 Timing Parameter Calculations for Internet IP-852 Channels

Timing Parameter	Set to:
Channel Timeout	(Average Ping Delay / 2) + 20%. A typical LAN based channel will require at least a 50 ms delay and a typical WAN based channel will require at least a 100 ms delay.
Packet Reorder Timer	The lesser of the following two values: ¼ of Channel Timeout Value, or 64 MS
LonMaker Channel Delay	Average Ping Delay + 10%

If you are using aggregation and the aggregation delay is a high percentage of the channel timeout or channel delay, add twice the aggregation delay to the **Channel Delay** property and one times the aggregation delay to the **Channel Timeout** property.

Use the ping command from a Command Prompt to obtain the average ping delay.

Channel Timeout

The channel timeout property sets the delay for a packet to travel across a channel. The assigned delay is a time parameter set in milliseconds that indicates how old a packet can be before it is discarded. If you are sending packets across a virtual private network or any configuration that uses the Internet, set the Channel Timeout parameter to ½ the average ping delay. Synchronize the IP-852 device routers with an SNTP time server.

Set the channel timeout parameter to a value in relation with the ping delay specified in Table 3.2. In a LONWORKS network, each channel is assigned a *cost* defined as the round trip delay for a packet traveling across that channel. The channel delay is based on a combination of bit rate, packet size, and media access. Generally, you should set the channel timeout on your IP-852 channel to more than half the channel delay value.

Set a channel timeout when using MD5 authentication. When using MD5 authentication, start with a minimum channel timeout of **100** ms and a channel delay of **200** ms. The following factors in affect the **Channel Timeout** property:

- *Variations on each leg of a round trip*. Factor the maximum delay into one leg of the trip.
- *Maximum difference between the times on the IP-852 devices*. The IP-852 device stamps its time on a packet when it is sent on the IP network and the target IP-852 device compares the stamp to its own time. If the time has expired, (time of device – time stamp in packet is greater than channel timeout), the IP packet is discarded by the target device as stale. You can estimate the maximum difference between the times on the devices by comparing the offsets displayed in the IP-852 Configuration Server log window log when you run the channel **Time Check** command.

Channel Delay

The channel delay specifies the value of the expected round trip time of a message (for example, message and response). This allows expected traffic patterns to be input to the system so that the timer calculations can be affected accordingly. You can set this property using a network management tool such as the LonMaker tool. See you network management tool documentation for more information on the **Channel Delay** property.

Packet Reorder Timer

You can use the packet reorder timer property to set the amount of time that an IP-852 device will wait for an out-of-order IP packet to arrive. This parameter is important for wide area networks (WANs) where IP packets can traverse multiple routers from source to destination causing packets to appear on the receiver in a different order than transmitted. If selected, the property defaults to **64** milliseconds.

Packets on a local area network do not get out-of-order; therefore, you can clear the **Reorder Packets** check box in this case. Using the packet reordering feature or an overly long reordering timer value can cause unnecessary delays in packet processing if a packet is lost or corrupted. Whether enabled or disabled, out-of-order packets are never sent onto the LONWORKS network.

Using SNTP When Creating IP-852 Channels

In small IP networks where there is no appreciable latency, it is not necessary to specify an SNTP server for your IP-852 channel; however, when creating IP-852 channels that span large IP networks where large network delays may be present, you must specify an SNTP time server. This allows each participant in the channel to synchronize to a common time base. Time synchronization is required to implement some of the LONWORKS protocol's messaging services. For example, the LONWORKS protocol's stale packet detection algorithm requires a common time base to function properly.

You can specify SNTP servers at three levels: system, channel, and device. Each device and channel may be configured to synchronize to its own SNTP servers, or default to the next level up. For example, a device can default to its channel SNTP servers, and a channel can default to its system SNTP servers.

Specifying System SNTP Servers

To specify the system SNTP servers, follow these steps:

1. In the IP-852 Configuration Server, click **Network**, click **Settings**, and then click the **SNTP** tab.

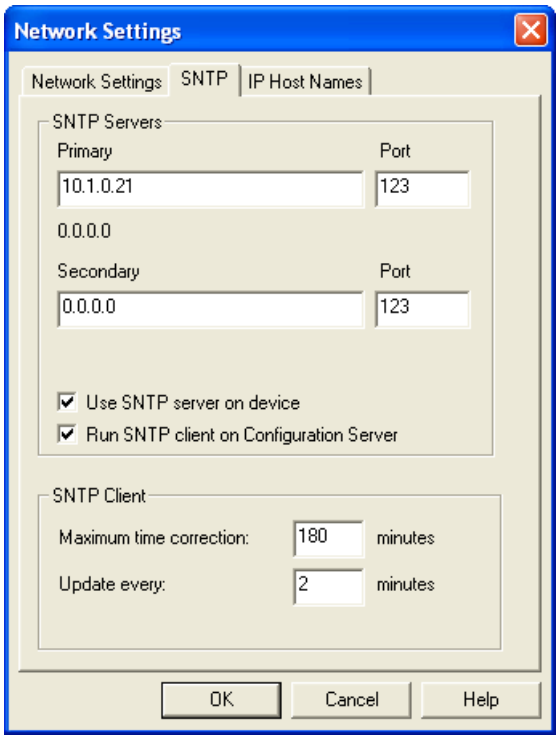

Figure 3.4 Setting the System SNTP Server

2. Enter the IP address or host name of the primary and secondary SNTP servers. The IP addresses must be static IP addresses. You can typically use the default port numbers of 123.

3. The **Use SNTP Server on Device** check box is selected by default. This means that the IP-852 device fetches the time from the specified SNTP time server to update its clock.

   If this check box is cleared, the IP-852 device does not fetch the time from the SNTP server. This may be desirable in small IP networks that have no significant latency, and do not define a channel timeout (see *Channel Timeout* earlier in this chapter for more information).

4. The **Run SNTP Client on Configuration Server** check box is selected by default. In this case, the IP-852 Configuration Server fetches the time from the specified SNTP time server and calculates the effective time to be used by all the IP-852 devices on the IP-852 channel.

   If this check box is cleared, the IP-852 Configuration Server does not fetch the time from the SNTP server. This may be desirable if all the IP-852 devices and your computer's clock are already being synchronized by the same SNTP time server, or the IP-852 devices are using individual SNTP time servers but those time server are providing sufficiently close times. In these cases, you can clear this check box to save the overhead created by the IP-852 Configuration Server having to independently fetch the time.

If the IP-852 Configuration Server is not on a domain, you should keep this check box selected because your computer's clock may drift too much as a result of Windows synchronizing to the system clock infrequently (once per week) by default.

The **Maximum Time Correction** and **Update Every** properties only apply if the **Run SNTP Client on Configuration Server** check box is selected. The IP-852 device SNTP options are self-adjusting and cannot be configured.

5. Click **OK** to save and return to the main dialog.

Specifying SNTP Servers for a Channel or Device

All channels default to the SNTP server specified for the system as described above, and all devices default to the SNTP server specified for the channel (for example, the System SNTP Server if the Channel SNTP server is not changed). Each channel and device in the network can be configured to synchronize to a different SNTP time server.

To specify SNTP servers for a channel or device, follow these steps:

1. Select the channel or device in the main dialog of the IP-852 Configuration Server, and then right-click the channel or device and click **Properties** on the shortcut menu (or double-click the desired channel or device). Click the **SNTP** tab.
2. Clear the **Use Channel Default** or **Use System Default** check box.
3. Enter the IP addresses or host names of the SNTP servers as shown in Figure 3.5. Leave the default port numbers of 123.

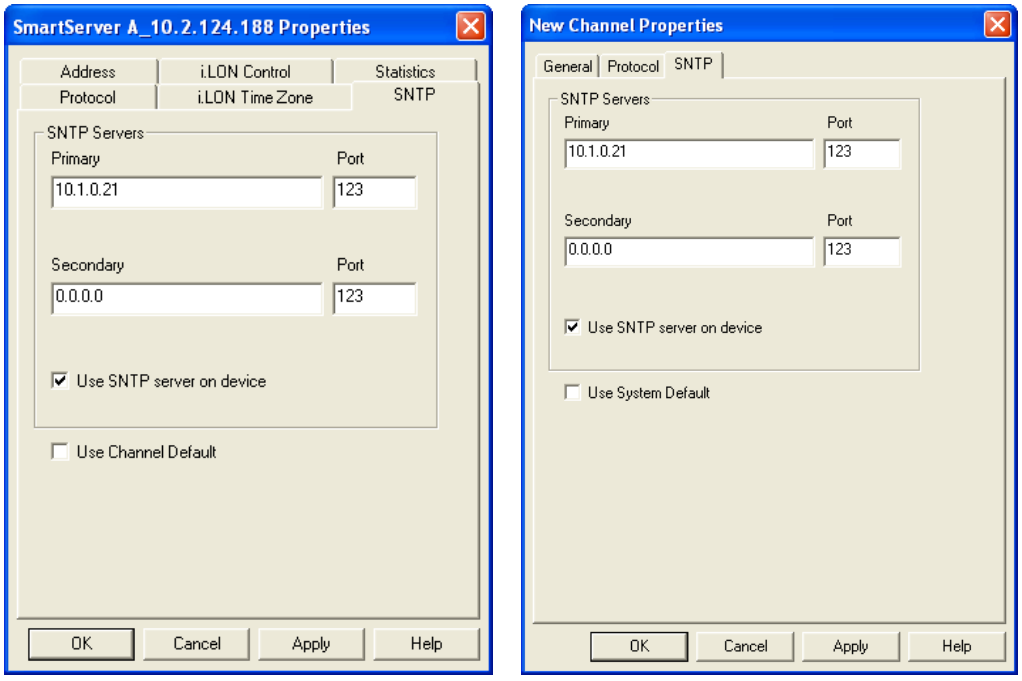

Figure 3.5 SNTP Server Configuration for a Channel and a Device

4. Click **OK** to save and return to the main dialog.

Choosing an SNTP Server

You can obtain an IP address for an SNTP server for your IP-852 Channel in any of the following ways:

- Ask your network administrator for the IP address of an SNTP server in your corporate network.
- Connect to a time server on the Internet. There are many available public access servers; a comprehensive list may be found at *http://ntp.isc.org/bin/view/Servers/StratumTwoTimeServers*.
- Install an SNTP server on any computer in your LAN. You can use the same computer on which the IP-852 Configuration Server is installed. One option is Tardis2000 shareware available from *http://www.kaska.demon.co.uk*. You can configure the software to synchronize with any other SNTP server, or use local time on the computer by setting Tardis2000 to use the loop back address 127.0.0.1.

4

Using NAT, DHCP, and DNS on an IP-852 Channel

This chapter describes how to use NAT, DHCP, and DNS on an IP-852 channel.

Network Address Translation (NAT)

Network address translation (NAT) allows multiple computers (hosts) to share a single IP address. The address is normally set up at the gateway between a private network and the Internet, allowing the computers on the private network to share a global, ISP assigned address. This is achieved by modifying the headers of each packet traveling through the NAT gateway. At a minimum, an IP address in each packet header is replaced (translated). For outbound packets (to the Internet), source addresses are translated from private to public. For inbound packets, destination addresses are translated from public to private.

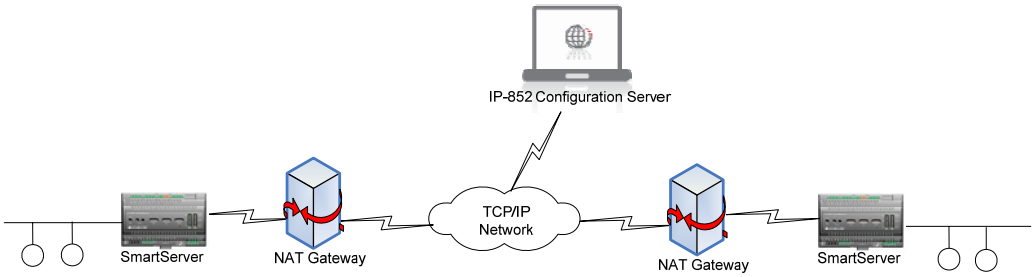

Figure 4.1 IP-852 Devices Communicating Through Two NAT Gateways

An IP-852 device may be placed behind an NAT gateway or firewall and can communicate with another IP-852 device placed behind another NAT gateway, as shown in Figure 4.1.

The port (1628 by default) that the IP-852 device uses to communicate with its peers and the IP-852 Configuration Server must be opened, mapped, and properly forwarded to the IP-852 device. See your NAT gateway's user manual for details on how to setup port forwarding (sometimes called static port mapping) on your particular NAT gateway.

Once the ports are mapped on the NAT gateway, setting up an IP-852 channel is much like the procedure described in Chapter 2 with the exception that additional entries are added to the IP-852 Configuration Server's device tree for each of the NAT gateways.

Setting up an IP-852 Channel with NAT

To set up an IP-852 channel that spans NAT gateways, start the IP-852 Configuration Server and perform the following steps:

1. Click **Channel** and then click **New NAT Firewall**.
2. Enter a descriptive name for your NAT firewall and then press ENTER.
3. Either double-click the new NAT firewall in the navigation pane or right-click it and select **NAT Firewall Properties**, enter the IP address of the NAT gateway/firewall, and then click **OK**.
4. Click the new NAT firewall in the navigation pane, click **Channel**, and then click **New Device**. Configure the device's IP address and other properties, as described in Section 2. Use the device's local IP address (typically a private, non-routable address, such as 10.x.x.x or 192.168.x.x).
5. Repeat steps 1 through 4 to add another NAT firewall and device. The IP-852 Configuration Server should look like the one in Figure 4.2.

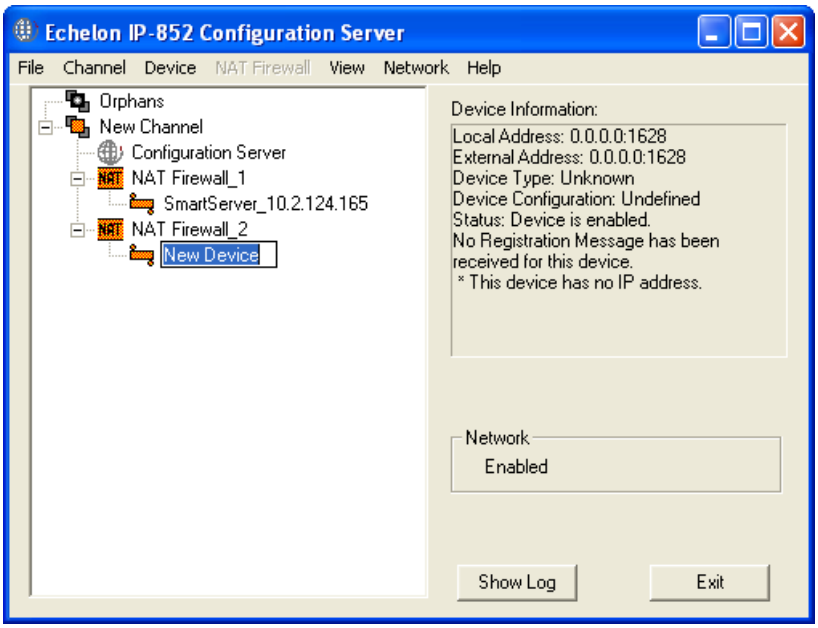

Figure 4.2 Setting up Multiple Firewalls with Multiple IP-852 Devices

6. Right-click the channel and click **Update Members** in the shortcut menu, or right-click the device and select **Update Device** in the shortcut menu.

NAT Example: Simple Home Network

If you have a home network with DSL or cable Internet access, you can setup all of your computers to communicate on the same IP address (assigned by your ISP) with the help of a NAT gateway. Usually, addresses used in the private network (your home) are taken from the range of addresses designated as "reserved" by the Internet Assigned Numbers Authority (IANA). The subnets reserved for private use are as follows:

10.x.x.x or 10/8 (Class A)
172.16.x.x - 172.31.x.x or 172.16/12 (Class B)
192.168.x.x or 192.168/16 (Class C)
169.254.x.x or 169.254/16 – "Auto-configuration"

Note: Reserved addresses are reusable, but are not globally unique; therefore, they are not routable on the Internet.

NAT translates the source addresses of outbound messages (sent by computers on your home network) to a single address, making all of the computers on your home network look like a single computer with a single IP address. When your home network receives messages from an outside network, the NAT gateway "maps" the response to the proper computer on your home network by changing the destination of the response to the correct internal address, as in Figure 4.3.

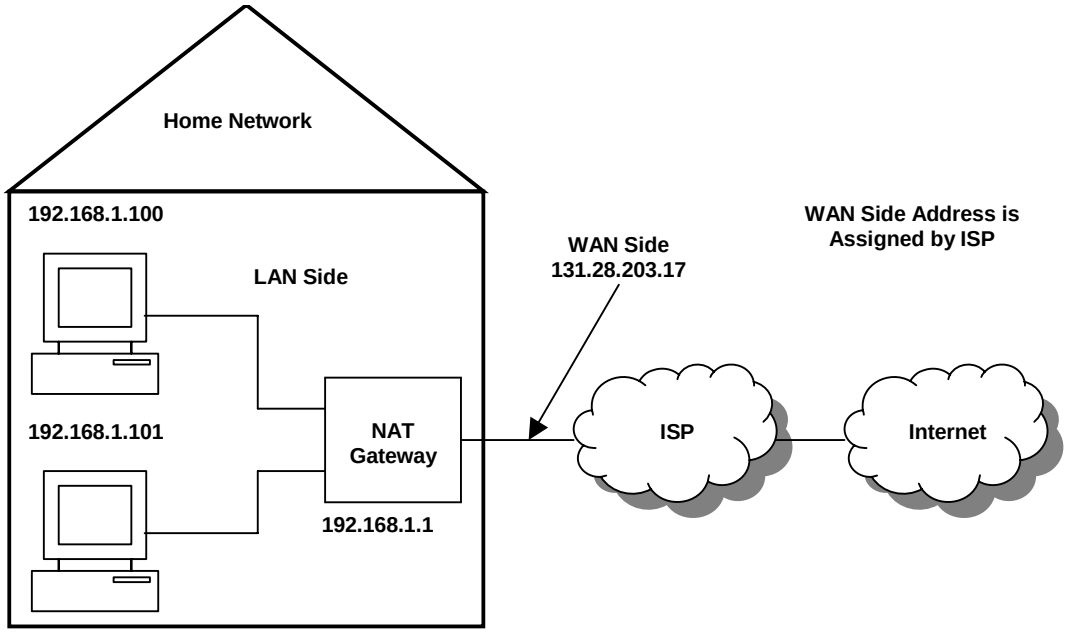

Figure 4.3 NAT Gateway Structure

Ports and Port Mapping

A fully qualified URL consists of an IP address and a port. The URL www.echelon.com:80 is a fully qualified URL. Port 80 is recognized as the default port for Web servers worldwide. Browsers typically append a URL with port 80 so you do not have to enter the full URL when accessing a Web site.

Ports allow a single computer to run multiple services. For example, www.echelon.com can run both a Web server and an FTP server. It could also run a time server and other applications as well. Each service may be assigned different ports. For example, Web browsers use port 80 as the default when they access www.echelon.com and maps the address to an IP address:port such as 205.229.51.8:80. When accessing an FTP client, FTP clients typically use port 21 so ftp://www.echelon.com will map to an IP address:port such as 205.229.51.8:21. Both the browser and the FTP client may simultaneously access www.echelon.com because the requests are differentiated by port.

Most businesses use port 80 for their public Web site so customers have easy access to their Web sites. However, if you wanted to host a less public site, you could assign it a non-standard port number. For example, you could use www.mycompany.com to attract a wide audience to your business, or you could assign your URL a non-standard port (www.mycompany.com:81) to "hide" your Web site from the general public. Changing ports does not provide security to your Web site, so other methods of security must be used for servers that contain sensitive information. Another reason to use non-standard ports is to allow access from the Internet to one of your home computers.

The Internet Assigned Numbers Authority (IANA) lists common or "well known" ports as well as registered and dynamic ports.
See *www.iana.org/assignments/port-numbers* for more information.

Port mapping can be used to connect two computers behind a NAT gateway that access the Internet through a single IP address. The NAT gateway forwards packets received from the Internet to the correct computer using different port settings. To ensure that packets are forwarded to the proper computer, the NAT gateway must be setup to perform static port mapping.

IP-852 Device Ports

The IP-852 device uses IANA designated ports for LONWORKS traffic (ports 1628 and 1629). Continuing with the example described above, you could connect an IP-852 device to your network with an IP address of 192.168.1.102.

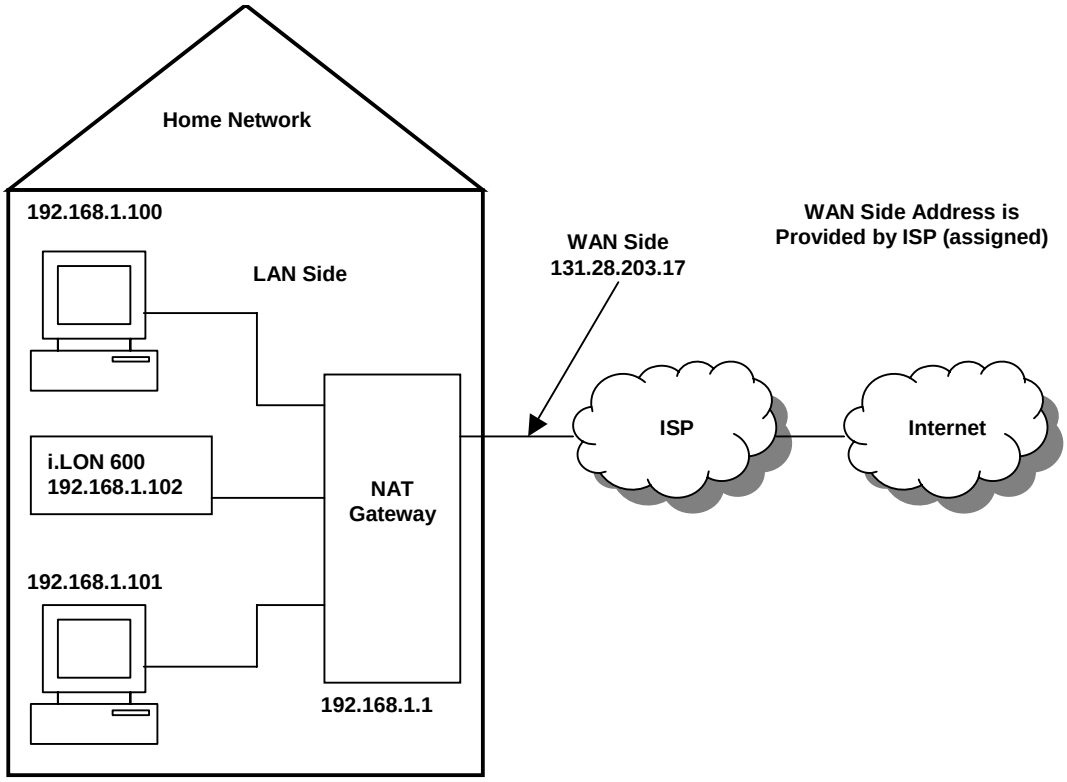

Figure 4.4 Adding an IP-852 Device to an NAT Gateway

To allow Internet access to your IP-852 device, you must map the necessary ports on your NAT gateway (as you did for the computers when setting up Web access). Once port 1628 is mapped to 192.168.1.102, the NAT gateway will forward any requests from peer IP-852 devices or from the IP-852 Configuration Server.

IP-852 devices can be configured to use ports other than the IANA defaults. This allows multiple IP-852 devices to reside behind a single NAT gateway. The default Web server port for a SmartServer or i.LON 600 server is 80. In the example, port 80 is already used by 192.168.1.100, so you must change the port on the IP-852 device and enter two static mappings into the NAT gateway:

Port 1628 → 192.168.1.102
Port 82 → 192.168.1.102

Consult your NAT gateway documentation for details on how to setup static port mapping for your particular NAT gateway.

Creating a Virtual Wire

LONWORKS networks that do not connect to an IP network may be quite large. A LONWORKS network may contain 255 subnets, with each subnet containing as many as 127 devices. Subnets are linked together using LONWORKS routers. A common implementation is to have many FT subnets connected to a single TP/XF-1250 high speed backbone.

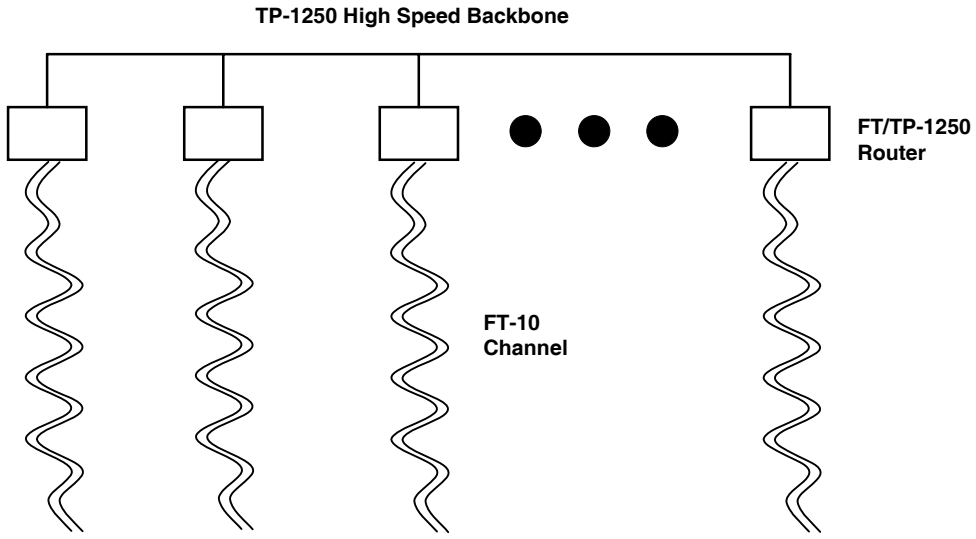

Figure 4.5 Connecting Devices on a Network

The high-speed backbone is a physical wire and, since all TP/XF-1250 to TP/FT-10 routers are connected to the same physical wire, communication proceeds unimpeded.

IP-852 devices are *logically* identical to TP/XF-1250 or TP/FT-10 routers, but use IP as their high-speed backbone instead of a TP/XF-1250 backbone. They may not be connected to the same physical wire.

Two IP-852 devices located in different cities could use the Internet as a high-speed backbone to create a single LONWORKS network. Instead of connecting the two IP-852 devices with one long wire, the Internet is used to create a "virtual wire". The IP-852 Configuration Server creates this virtual wire.

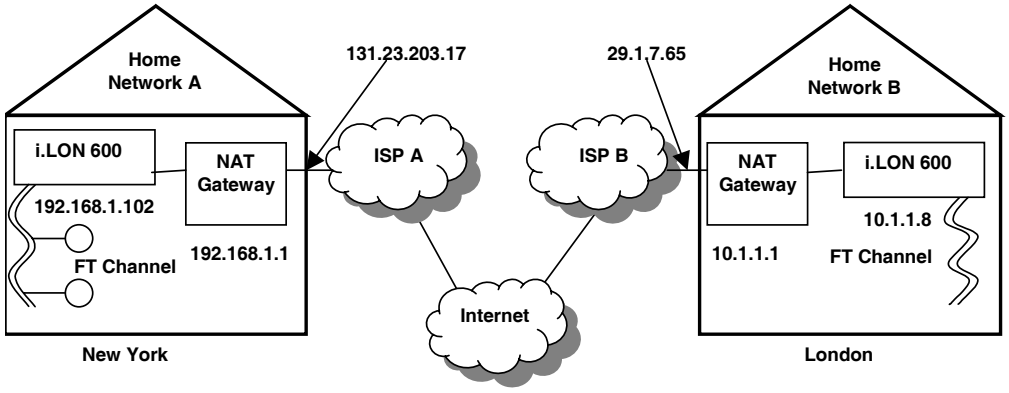

Figure 4.6 Creating a Virtual Wire

The IP-852 Configuration Server is aware of NAT gateways, and you should enter each NAT gateway in your system as you create your IP-852 channel (virtual wire). In Figure 4.6, the IP-852 Configuration Server could be configured as shown below.

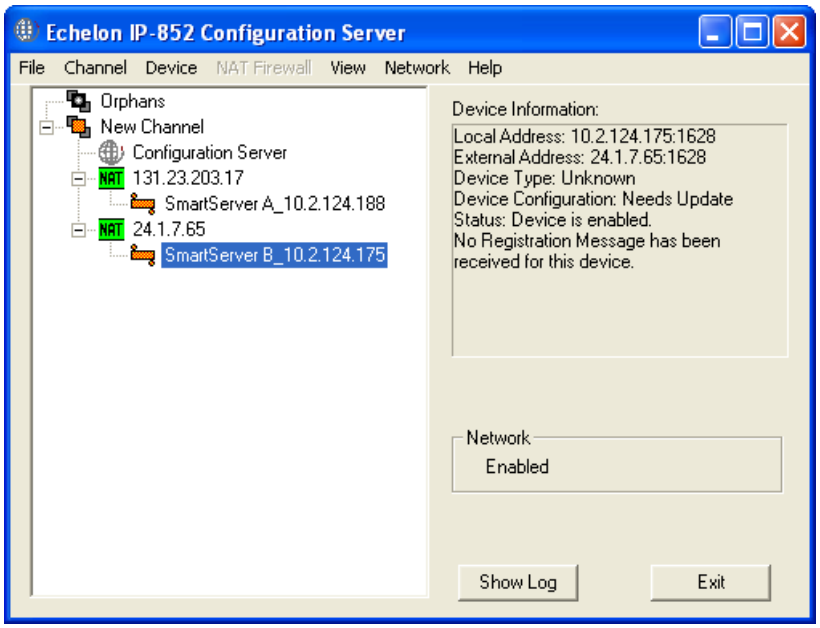

Figure 4.7 IP-852 Configuration Server Setup

Note: The diagnostic information provided about the IP-852 devices (indicated by the varying IP-852 device icon colors) is more complete than the diagnostics provided by the changing colors of the NAT gateways. The IP-852 Configuration Server cannot acquire the same level of diagnostic information about an NAT gateway as it can about IP-852 devices. See Table 2.1 for the descriptions of the different IP-852 Configuration Server icon colors.

The IP-852 Configuration Server acts as a relay station for all information pertaining to channel members, including which LONWORKS subnets are on the far side of which IP address.

Whenever a LONWORKS routing table changes (this can happen while making a network variable connection) or a new member is added to the IP-852 channel, the IP-852 Configuration Server relays this information to all devices on the channel that need to know.

Once all channel devices have been inaugurated into the IP-852 channel, and all LONWORKS device installations and connections have been made, you can shut down the IP-852 Configuration Server software (you can leave it running, however, to ensure it is available as required for future configuration changes).

DHCP

For small networks, manually configuring the IP address of each device on the network is fairly simple. However, as the number of computers on your network grows, assigning each computer on the network its own IP address can be cumbersome. To solve this problem, a system called Dynamic Host Configuration Protocol (DHCP) was created to automatically assign network computers an IP address. Most computers use DHCP.

With DHCP, computers broadcast a message on the local network asking the DHCP server to assign them an address, instead of using a pre-defined address. The DHCP server stores a list of the assigned addresses and makes sure that no two requestors are given the same address. This greatly simplifies the job of the network administrator, but in the case of Web servers (or IP-852 devices), can create some difficulties.

The DHCP server resides on the network and assigns IP addresses. When you enable the **Automatically Obtain IP Address** property in the configuration Web pages for a SmartServer or i.LON device (i.LON 100 e3 Plus Internet Server or i.LON 600 IP-852 Router), you are asking Windows to get its IP address from a local DHCP server. DHCP is commonly used for workstations, but seldom used for Internet-accessible servers. For example, your company's Web server likely has a static IP address instead of a DHCP assigned address.

DHCP addresses are assigned in the order computers are powered on. Computer 1 may be assigned address 100, computer 2 may be assigned address 101, computer 3 may be assigned address 102, and so on. If computers are powered down and then later restarted, there is no guarantee that they will receive the same address. This is a problem if you want to setup a communication channel between a set of computers, as is done when creating an IP-852 channel. In an IP-852 channel, each device knows the addresses of other devices on the network. If those addresses change because a peer was power cycled, then all members of the group need to be updated with the new IP address. This is easily accomplished by updating an entry in the IP-852 Configuration Server, but the process is manual, which makes it impractical for larger networks. **To prevent configuration problems due to changing IP address, assign static IP addresses to all the IP-852 devices on an IP-852 channel.**

However, if you are in control of your DHCP server, you may be able to configure your DHCP server to always assign your SmartServer or i.LON dev ices the same IP address. This is called making a *static reservation*, and is supported by most DHCP servers. Using DHCP with static reservations is acceptable and is similar to using static IP addresses. If you decide to use this technique, each SmartServer and i.LON device can be instructed to acquire its IP address from the DHCP server by enabling the **Automatically Obtain IP Address** on the TCP/IP Web page for your SmartServer or i.LON device. See your device's documentation for how to do this.

DHCP Servers

DHCP servers are configured to assign a range of valid Internet addresses. With a simple NAT gateway, like the one shown in Figure 4.4, the range is often 192.168.1.2 to 192.168.1.254. As an example, the NAT gateway assigns the first computer to request an address 192.168.1.100, the second computer to request an address 192.168.1.101, the next gets 192.168.1.103, and so on. The address a computer is assigned is determined by the order in which the computers are powered up on a network. Computers request an address each time they are powered. This means that by using DHCP you run the risk of losing a previously assigned address for a given computer (or IP-852 device). This usually is not an issue for a home computer that is used to browse the Internet because the computer is always the initiator of the Web page request. However, if you want a computer to act as a Web server, it must have a permanent address so other computers can access it. The same is true for an IP-852 device participating in an IP-852 channel.

The solution is to avoid using DHCP without static IP address reservations for devices whose addresses must be known by external users. This includes FTP servers, time servers, Web servers, database servers, and IP-852 devices.

When a computer does not use DHCP and is assigned an address manually, it has a *static* IP address. It is possible to have a network that defines a range of addresses that will be allocated dynamically by the DHCP server, and a range that will be managed manually. In the NAT gateway mentioned above, 192.168.1.2 to 192.168.1.99 are managed manually.

ISP Address Allocation

Cable or DSL service in the United States costs about $40 - $50 per month for a single dynamically allocated IP address. Depending on your telephone or cable provider, you may be able to purchase a business account that provides one or more static IP addresses at a higher cost.

In the example, if the address provided to your home by the ISP is static, you only need to setup static port mapping and inform outside users to go to 131.23.203.17:80 or 131.23.203.17:81 to view your Web pages. Similarly, if you wanted to include your home IP-852 device in an IP-852 channel, you would enable static port mapping on the NAT gateway and enter 131.23.203.17:1628 in the IP-852 Configuration Server. The packets on the channel would flow unimpeded.

You will run into problems with your network if your ISP does not offer static addresses. Even if static port mapping is enabled on your NAT gateway, you may not be able to access computers within your home because the house IP address (provided by the ISP) may change unpredictably. This is a common problem. **As a result, you should use a static IP address for both your NAT gateway and the SmartServer or i.LON device in your local network.**

DNS

DNS is a mechanism that translates an IP host name like www.echelon.com into a numeric IP address like 205.229.51.8. For example, when you enter www.echelon.com in your Web browser, your Web browser queries a DNS server to find the IP address. It then requests the home page from the numeric IP address—not the IP host name. Because the process is transparent, many people are not aware of the existence of numeric IP addresses.

IP host names are usually used to reference servers such as a Web server (www.echelon.com), a database server, or a file server. Because these servers are fixed assets, they are usually assigned a static IP address. That static IP address is also entered into a DNS server so that the mapping between the IP host name and the numeric IP address can be made.

If you are in control of your local DNS server, you should give all participants in your IP-852 channel static IP addresses and create DNS entries for each participant. This allows you to specify IP host names when setting up the IP-852 channel in the IP-852 Configuration Server, instead of numeric IP addresses. The IP-852 Configuration Server will translate the IP host name into a numeric IP address and pass that address to all members of the channel.

For example**,** if you had a static IP address at your local network, you could register that IP address with one of the Internet registrars (such as register.com) and associate a name with that static IP address. The registrar will propagate the address/name pair throughout the Internet's DNS servers for you, ultimately allowing you to tell people to go to *www.mynetwork.com* instead of 131.23.203.17.

Note: When a browser tries to view a Web site, it asks the DNS server to translate the name of a Web site into an IP address. It then uses the IP address to contact the Web site. The actual IP packets never contain the proper name of the Web site, only the hard IP address that was resolved by the DNS server. In addition, the IP-852 devices themselves do not query DNS servers to resolve addresses; they only work with numeric IP addresses provided by the IP-852 Configuration Server.

This only works for static IP addresses because each time you change the IP address, you need to contact the registrar to setup the new address/name pair across the Internet. This may take up to two days for an address/name pair to propagate through the entire Internet.

To set the Echelon IP-852 Configuration Server automatic IP host name address translation, follow these steps:

1. In the IP-852 Configuration Server, click **Network**, click **Settings**, and then click the **IP Host Names** tab.

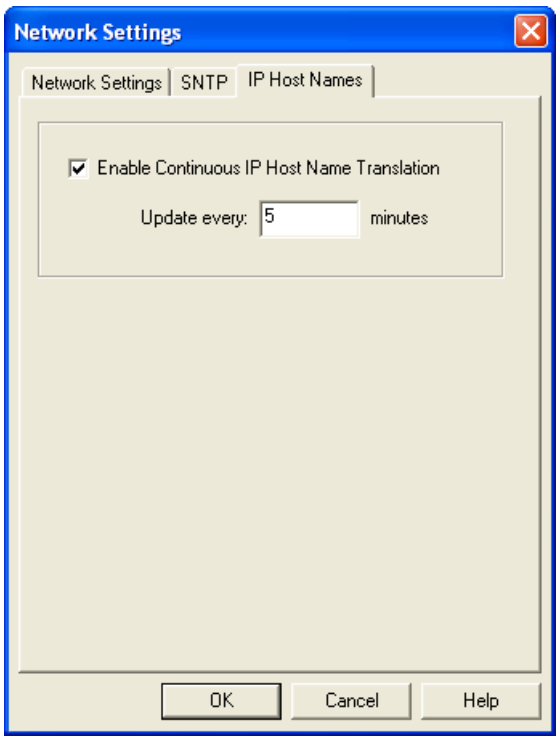

Figure 4.8 IP Host Names Tab

2. Select the **Enable Continuous IP Host Names Translation** check box, and then specify an update interval time (if applicable).
3. To issue an immediate IP word-based address translation, click **Network** and then select **Translate IP Host Names**. This will perform a retranslation on all channels.

   Note: When enabling the **Translate IP Host Names** option, the local DNS server and the Echelon IP-852 Configuration Server must be continuously running.

DNS and the Echelon IP-852 Configuration Server

When you type **myilon.echelon.com:1628** into the IP-852 Configuration Server instead of **205.229.51.11:1628**, the IP-852 Configuration Server goes to the local DNS server defined on that computer to resolve **myilon.echelon.com** to a numeric IP address, and then sends that address to all IP-852 devices on your IP-852 channel. This works until one of the IP addresses changes.

By default, the IP-852 Configuration Server will periodically (once every five minutes) attempt to resolve any IP host name on all channels (including SNTP server) with a DNS server. If a translation is successful, and the resulting IP address is different than what was previously used, the channel members will be updated. This re-translation process also occurs when the IP-852 Configuration Server is first started. Therefore, to reference your IP-852 devices only by DNS name, you must leave the IP-852 Configuration Server running on your network. The IP-852 Configuration Server will periodically query the DNS server to verify that all hard IP addresses are still correct, as described previously.

If a device's IP address changes, the IP-852 Configuration Server will eventually become aware of the change and update its configuration. However, it is still possible that changing a device's IP address could disrupt communication on your IP-852 channel before the IP-852 Configuration Server becomes aware of the change. **To prevent**

channel outages due to IP address changes, use static addresses that do not change.

Linking DNS and DHCP

DNS and DHCP are separate standards. A network can use DNS without using DHCP, and vice versa. You can, however, link DNS and DHCP servers in a single network so that all IP addresses on the network could be allocated dynamically, but still be referenced by name. While this can work for private networks, usually within corporations, it is not practical for the Internet.

If your IP-852 channel implementation is under your control, and you have control of all DHCP and DNS servers referenced by the members of your IP-852 channel, you can assign each device an IP address using DHCP without static reservations, and resolve host names using DNS and the IP-852 Configuration Server. This section describes how you can do so.

Note: The IP-852 Configuration Server requires a single static IP address for all computers running LNS (version 3.0x or later) that are connected to an IP-852 channel.

If you leave the IP-852 Configuration Server attached to the IP-852 channel, DNS resolvable addresses can be used. If the IP network links its DHCP server and DNS server, then IP-852 devices can be setup to use DHCP assigned addresses. However, the IP-852 Configuration Server's ability to resolve addresses through DNS is limited. Dynamic DNS (DDNS) can also be used with the same precautions. For more information on DDNS, see the next section, *Dynamic DNS*.

The ISO/IEC 14908-4 standard requires that devices on an IP-852 channel share IP addresses instead of DNS resolvable names. If an IP-852 device in a channel is aware of a peer at 131.1.23.52, and that peer changes addresses, the IP-852 device will lose communication with the peer until it receives an updated peer list. The IP-852 Configuration Server can solve this problem by sending out an updated list (using DNS) to all members on the channel. The IP-852 device cannot resolve DNS address issues on its own.

If DHCP will be used to retrieve the IP information for an IP-852 device, the network administrator must ensure that a DHCP server is available to provide the IP address, subnet mask, and gateway address.

Dynamic DNS

If your network administrator or ISP does not offer a static IP address service, you can use a third party solution called dynamic DNS (DDNS). Providers include dns2go.com, dyndns.org, and others. Perform a quick Internet search on "dynamic DNS".

How DDNS Works

DDNS operators rely on the fact that your computer's IP address does not frequently change. Depending on your network administrator or ISP, the computer address may change only when you power cycle your NAT gateway. If your NAT gateway is on 24/7, it may be months before your computer's address changes. It is also possible that your network administrator or ISP forces the address to change even if the gateway is not power cycled. The amount of time that a device may keep its address is called its "lease". DHCP servers lease an address for a period of time after which the lessee is required to go back and acquire another lease.

When using DDNS, each time a new DHCP lease is given (for example, each time the computer's IP address changes) the DDNS server is notified. The DDNS server keeps track of each client's current address. To let external users see the Web server in your LAN, instead of telling the registrar that **www.mylan.com** is linked to 131.23.203.17, you tell the registrar that www.mylan.com is linked to **mylan.ddns.org** (for example). When an Internet user types in www.myhouse.com, the Internet DNS server forwards the request to **mylan.ddns.org**, which forwards the request to the current IP address of your home.

The DDNS provider tracks any changes in your computer's address and forwards any request for **mylan.ddns.org** to your house's current IP address.

Because of its potential complications and its reliance on relatively small third party providers, IP-852 channels configured to use devices with DDNS will typically not be as reliable as IP-852 channels configured with devices using static IP addresses.

Appendix A

Troubleshooting

This appendix can be used to diagnose common problems that could occur when you create an IP-852 channel with the Echelon IP-852 Configuration Server.

Common Troubleshooting Problems

The following lists the most common problems encountered when creating and configuring an IP-852 channel with the Echelon IP-852 Configuration Server.

Disabled IP-852 devices will not configure properly when the IP-852 Configuration Server is taken off the network. If you reattached the IP-852 Configuration Server and select Update Members, the IP-852 device is still not configured properly.

- To solve this problem, you must disable your IP-852 device while the IP-852 Configuration Server is still attached to your network.

The device icons in the IP-852 Configuration Server do not turn green.

- This is usually an indication that the IP-852 Configuration Server cannot communicate with the device. If any of your IP-852 devices are behind a NAT gateway, verify that the NAT gateway is properly setup to forward ports 1628 and 1629.

I cannot view an IP-852 device's Setup Web page.

- Many IP-852 devices have a built-in Web server used for setup that communicates on port 80 by default. To access the Web page from outside your NAT gateway, be sure that the NAT gateway is configured to forward port 80 to your IP-852 device.

Computers using DHCP cannot communicate with an IP-852 device using Ethernet direct connect.

- Communication with an IP-852 device may be lost if you use DHCP and direct connect (using an Ethernet cable), and then unplug the IP-852 device. When you plug the Ethernet cable back into the IP-852 device, the device communicates with the DHCP server and searches for an IP address. This action may cause the device's IP address to change. To solve this problem, assign your IP-852 device a static IP address and make any configuration changes. Enable DHCP before re-installing the IP-852 device onto your network.

I cannot access an IP-852 device with FTP.

- Many IP-852 devices have a built-in FTP server that communicates on port 21 by default. To access the FTP server on an IP-852 device that is outside your NAT gateway, be sure that the NAT gateway is configured to forward port 21 to the IP-852 device.

The Service LED on my IP-852 device is blinking, what does this mean?

- Many IP-852 devices have a Service LED that blinks when the IP-852 device is not commissioned. When is the device is added to a network and commissioned, the Service LED will turn off.

How do I diagnose problems with the IP-852 Configuration Server?

- Click the **Show Log** button to display the IP-852 Configuration Server log. Right-click a device and click **Diagnose Device** on the shortcut menu. Watch for any error or warning messages that appear in the log window. To simultaneously write the messages to a file, click the **Log File** button and supply a file name.

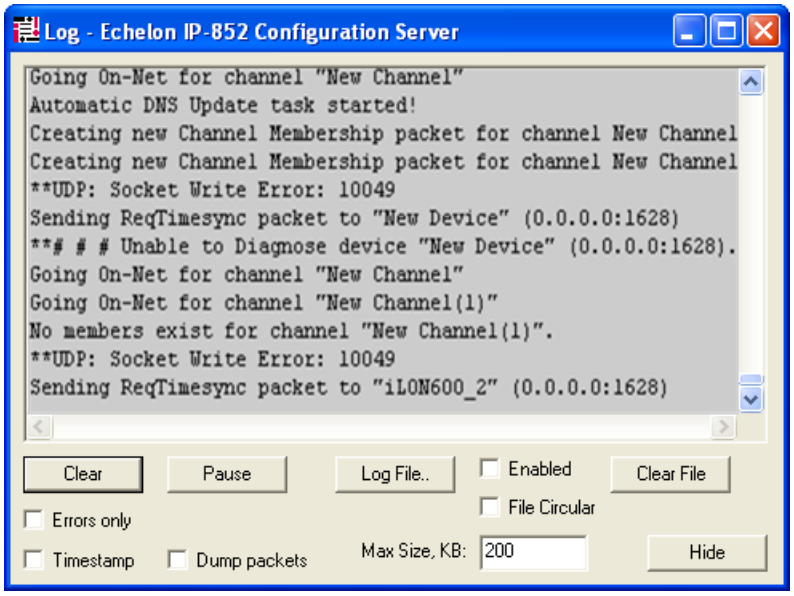

Figure A.1 Echelon IP-852 Configuration Server Log

ECHELON®
www.echelon.com