ECHELON®

i.LON® 600 LONWORKS®/IP Server User's Guide

078-0272-01

Echelon Corporation
550 Meridian Ave
San Jose, CA 95126, USA

Preface

This document describes how to use the *i*.LON 600 LONWORKS/IP Server and the Echelon LONWORKS/IP Configuration Server.

Purpose

The *i*.LON *600 User's Guide* describes how to configure the *i*.LON 600 and how it can be connected to a LONWORKS network, an IP network, and other devices.

Audience

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

Models

There are four models of the *i*.LON 600 :

- 72601 – FT-10 Transceiver, 90-240VAC, 50/60Hz
- 72602 – TP/XF-1250 Transceiver, 90-240VAC, 50/60Hz
- 72603 – FT-10 Transceiver, 24V VAC/VDC
- 72604 – TP/XF-1250 Transceiver, 24V VAC/VDC

Box Contents

The *i*.LON 600 ships with the following material:

- *i*.LON 600 LONWORKS/IP Server
- *i*.LON 600 CD – This CD contains the *i*.LON 600 embedded image and the LONWORKS/IP Configuration Server as well as Microsoft Internet Explorer 6.0, and documentation.
- *i*.LON 600 Quick Start Sheet – This sheet describes how to install the Echelon LONWORKS/IP Configuration Server software, how to connect the *i*.LON 600 hardware, and how to configure the *i*.LON 600's IP information using the Web interface.

PC Software Requirements

Software requirements to run the Configuration Server and *i*.LON 600 configuration Web pages are given below:

- Microsoft Windows XP or Windows 2000. It is recommended that you install the latest service pack available from Microsoft for your version of Windows.
- Internet Explorer 6 Service Pack 1 or higher.
- Terminal emulator, such as Windows HyperTerminal (optional).

PC Hardware Requirements

Minimum hardware requirements for the computer on which the Configuration Server will run are given below:

- Pentium II 600 MHz or faster
- 128-MB RAM minimum
- 70 MB free hard disk space
- CD-ROM drive
- Super VGA (800 × 600) or higher-resolution display with 256 colors
- Mouse or compatible pointing device

Table of Contents

1

Introduction

This chapter provides an overview of the capabilities of the *i*.LON 600 and the terminology used in this document.

Introduction

The *i*.LON 600 LONWORKS/IP Server is a Layer 3 LonTalk® router that offers fast throughput for process control, building automation, utility, transportation, and telecommunications applications.

The *i*.LON 600 LONWORKS/IP Server improves on the performance of the *i*.LON 1000 with a new generation processor and package that provides reliable, secure Internet access to virtually any electrical device including lights, appliances, switches, thermostats, motors, meters, valves, HVAC, elevators, and security access products. The *i*.LON 600 lets you communicate with devices to monitor, adjust, and reconfigure them as needed.

The *i*.LON 600's LonTalk router application allows IP to be used as a standard LONWORKS channel. **Here, the term "router" is used to signify a LONWORKS router, not an IP router**. From the LONWORKS perspective, the router application has all of the characteristics of a LONWORKS router with one side connected to a twisted pair LONWORKS channel and the other side connected to a LONWORKS/IP channel. The router application can be configured as any of the four standard LONWORKS router types: configured, learning, configured, bridge, or repeater.

The performance of the *i*.LON 600 is derived from a powerful 32-bit RISC processor and Echelon's LONWORKS/IP software architecture. The result is very high packet throughput in networks with large numbers of nodes and/or fast monitoring and display requirements.

The *i*.LON 600:

- Allows the millions of Internet-ready LONWORKS® devices to be monitored, controlled, or configured over the Internet.
- Transforms the Internet (or any IP-based LAN or WAN) into a pathway for carrying LONWORKS control information locally, nationally, or around the world.
- Includes MD5 authentication for secure access.
- Provides Layer 3 routing of LONWORKS control packets.
- Supports TCP/IP, UDP, DHCP, ICMP, SNTP, HTTP and FTP.
- Supports LONWORKS/IP channels with up to 256 devices.
- Supports multiple units behind NAT gateways/firewalls.
- Complies with EIA-852 & ANSI/EIA 709.1.
- Comes in 8TE DIN packaging.
- Available in a 24VAC/DC or 110/240 VAC power input.
- Is CE Mark, U.L. Listed, cUL Listed, TÜV Certified.

Installing the *i*.LON 600 PC Software

To install the *i*.LON 600 Software, follow these steps:

1. Insert the *i*.LON 600 CD-ROM into your PC and follow the instructions in the Setup Wizard. If the installation program fails to start, navigate to your CD-ROM and double click **setup.exe** in the root directory.
2. Make sure you have Internet Explorer 6, SP 1 (or later) installed on your computer. This is available on the *i*.LON 600 CD-ROM in the following location:

\IE\ie6setup.exe

Note: The *i*.LON 600 Configuration Server can open *i*.LON 1000 Configuration Server databases. You cannot, however, re-open the databases with an *i*.LON 1000 Configuration Server.

i.LON 600 Setup Overview

To begin using the *i*.LON 600, you must:

1. *Connect the i.LON 600 Hardware* – This includes connecting the *i*.LON 600 to a power source, LONWORKS network, and an Ethernet network.

WARNING

Connecting the *i*.LON 600 (models 72601 and 72602) to a power source involves handling high-voltage wiring and must be performed by a qualified service person.

2. *Configure the i.LON 600's IP information* – This includes configuring the IP address, host name, etc. using the *i*.LON 600 setup Web pages or console application.
3. Setup a LONWORKS/IP channel using the Configuration Server.
4. *Add the i.LON 600 to a LONWORKS Network* – Using the LonMaker tool, drag a router shape from the stencil to the LonMaker drawing, and then provide the Neuron ID of the *i*.LON 600 using either the service pin or manual entry. Figure 1 shows a flowchart of the *i*.LON 600 setup.

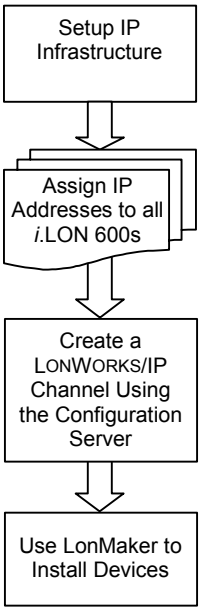


Figure 1. Setting Up a LONWORKS/IP Channel Operational Flow Chart

Section 1

Setting Up and Using the *i*.LON 600 LonWorks/IP Server

2

Mounting, Cabling and Connections

This chapter describes how to mount the *i*.LON 600 hardware and how to attach power, data, a LONWORKS channel, and an Ethernet network to the *i*.LON 600.

i.LON 600 Mounting Options

CAUTION

The high-voltage models (72601 and 72602) of the *i*.LON 600 are intended to be mounted inside of a suitable, safety-agency approved enclosure that is mounted in a restricted access area. High-voltage wiring must be performed only by a qualified service person.

The *i*.LON 600 mounts to a 35mm × 7.5mm or 35mm × 15mm DIN rail. The rear of the *i*.LON 600 enclosure contains a spring-loaded DIN rail lock, which securely attaches the DIN rail onto a permanent fixture. To release the enclosure from the DIN rail, insert a flathead screwdriver into the DIN rail locking tab and gently pull the tab down and away from the enclosure.

The following diagram shows the dimensions of the *i*.LON 600. All units are in millimeters:

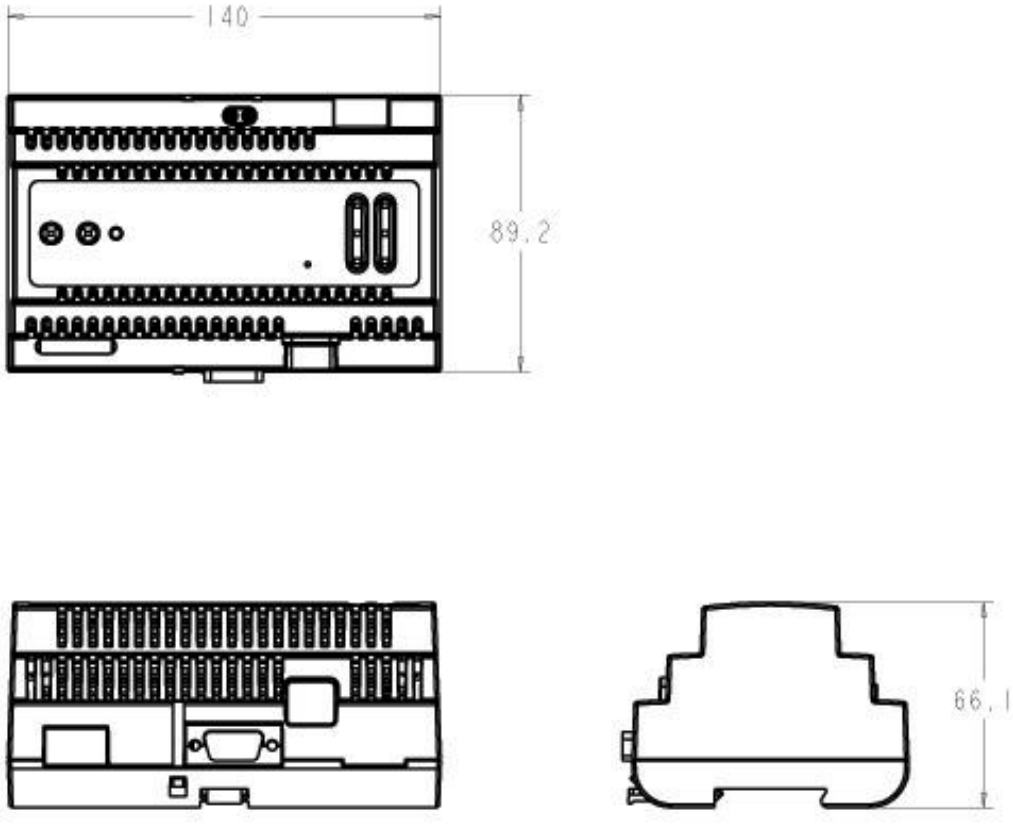


Figure 2. *i*.LON 600 Dimensions

Wiring Connections

The *i*.LON 600 is available in two versions, depending on the type of LONWORKS channel you are using. Models 72601 and 72603 support the FT-10 free topology channel, while models 72602 and 72604 support the TP/XF-1250 channel.

The *i*.LON 600 has two rows of screw terminal wiring connections, an RJ-45 (Ethernet) data connection, and a DB-9 D-connector for connection to a console port. Figure 3 shows the locations of all *i*.LON 600 connectors.

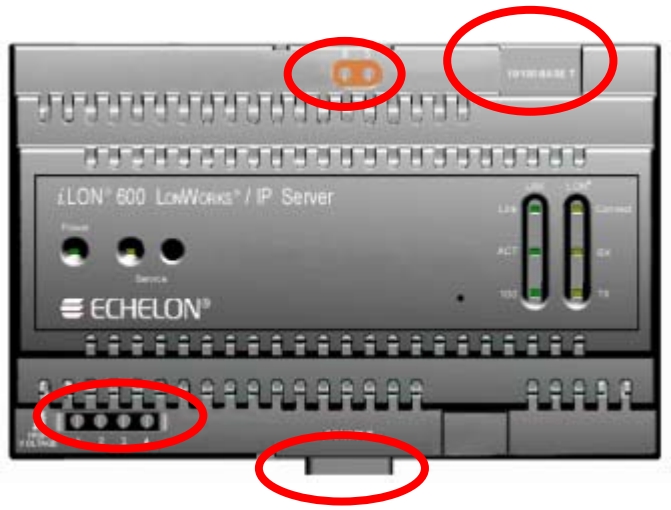


Figure 3. *i*.LON 600 Server Data and Console Connections

Screw Terminal Connectors

The screw terminals are located on the top and bottom edges of the enclosure, and are numbered 1 to 4 (ascending from left to right) on the bottom, and from 5 to 6 (ascending from right to left) on the top.

The screw terminals accept 0.34 – 4.0mm^2 (22 – 12AWG for the power connector and 16 – 26AWG for the LonTalk connector) gauge solid wire. The optimum tightening torque for the screw terminals is 9.217 kg/cm (8 lbs. in.) maximum. For the LonTalk connector, the optimum tightening torque is 6.913 kg/cm (6 lbs. in.). The ideal flathead screwdriver tip width is 3mm (0.12"). Wires should be stripped to a length of 7mm (0.28"). Although not required, it may be useful to use a soldering iron to tin the stripped lengths of any stranded wires to prevent fraying and inadvertent contact with adjacent terminals.

The screw terminal connections can be divided into two groups:

- Power
- LonTalk

The RJ-45 10/100 BaseT Ethernet Port

The RJ-45 connector must be used with an RJ-45 male connector and a suitable Category 5 or Category 6 Ethernet cable connected to a 10BaseT or 100BaseT channel. The *i*.LON 600 automatically adjusts to the speed of the data port. If a 100BaseT network connection is established, the *i*.LON 600 illuminates the "100" LED indicator on the front panel. The *i*.LON 600 automatically detects whether it is connected to an Ethernet hub or directly to a computer and will switch the connection polarity as appropriate, so there is no need to use a crossover Ethernet cable.

The DB-9 Console Port

The *i*.LON 600 contains a console application that is accessed using a terminal emulation program, such as Windows HyperTerminal, via the EIA-232 DB-9 console port. This application allows you to set parameters such as the IP address, subnet mask, and FTP user name and password. The DB-9 is designed to be used with a DB-9 null-modem crossover cable with female connectors on both ends. Connect the cable to the *i*.LON 600 and an available COM port on a computer running the terminal emulation program. The connector pins on the DB-9 console are aligned as shown in Figure 4:

Figure 4. *i*.LON 600 DB-9 Pin Alignment

The connector pins are described in Table 1.

Table 1. *i*.LON 600 DB-9 Pin Assignment

***i*.LON 600 DB-9 (DTE) Pin**	***Description***
1	NC (No connect)
2	RxD (Receive Data)
3	TxD (Transmit Data)
4	NC (No connect)
5	GND (Ground)
6	NC (No connect)
7	NC (No connect)
8	NC (No connect)
9	NC (No connect)
DB-9 Shell	Earth Ground

24V Power for Models 72603 and 72604

i.LON 600 models 72603 and 72604 operate with a supply voltage of 24VAC/DC ±33%. The low-voltage power source must be capable of providing 500 mA (average) of current. The 24V version of the *i*.LON 600 is equipped with a Polyfuse that automatically resets.

Table 2 shows the 24 Volt connector assignments and Figure 5 shows the location of the screw terminals.

Table 2. *i*.LON 600 Server 24 Volt Connections

Screw Terminal	*Enclosure Marking*	*Connections*
1	E	Earth ground
2	24VAC/VDC	24V Connection #1
3	24VAC/VDC	24V Connection #2
4	NC	No connect

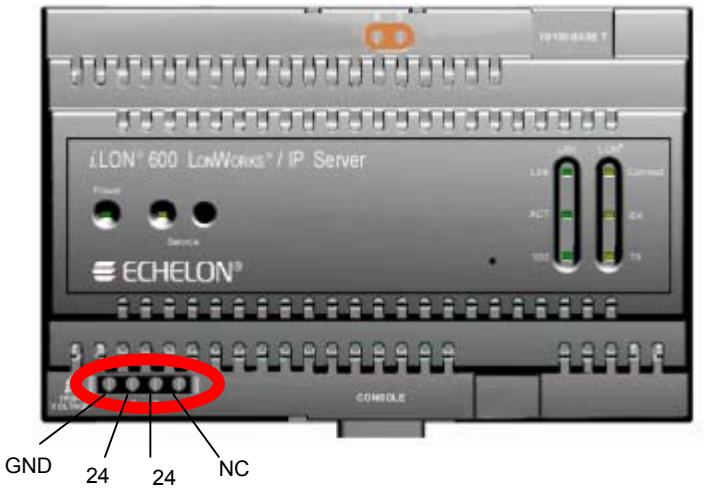


Figure 5. 24V Screw Connectors

SAFETY WARNING

The *i*.LON 600 uses a **non-replaceable** Poly-carbonmonoflouride Lithium Coin battery. **RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF UNUSED BATTERIES ACCORDING TO THE INSTRUCTIONS.**

Connecting High Voltage Models 72601 & 72602

SAFETY WARNING

When connecting the power terminals of an *i*.LON 600, always connect earth ground first, then Neutral, then Line. This minimizes the risk of shock or damage should power inadvertently be present on Line.

SAFETY WARNING

The *i*.LON 600 uses a Poly-carbonmonoflouride Lithium Coin battery. **RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE. DISPOSE OF UNUSED BATTERIES ACCORDING TO THE INSTRUCTIONS**.

SAFETY WARNING

The *i*.LON 600 is not equipped with a power disconnect device. When the device is installed and mounted, the installer must provide a means to safely remove power, such as a power switch or a circuit breaker.

SAFETY WARNING

The terminal block has a plastic cover protecting the screw terminals used to connect the power inputs. This cover **MUST** be placed on the *i*.LON 600 after the power wires are connected and before the power is activated.

The 100-240VAC power mains connection is used to power the *i*.LON 600. The *i*.LON 600 contains an auto-ranging, auto-setting mains power supply.

The high voltage connection is implemented on screw terminals 1 (Earth Ground), 3 (Neutral), and 4 (Line): screw terminal 2 (NC) is not used and should remain unconnected. A solid earth ground via terminal 1 connection is required for proper ESD and EMC performance of the *i*.LON 600 device. Install the power mains in the following order:

1. Insert the earth ground
2. Insert the neutral connection
3. Insert the line connection

DO NOT apply power to the *i*.LON 600 until you have checked all wiring connections, and you are instructed to apply power.

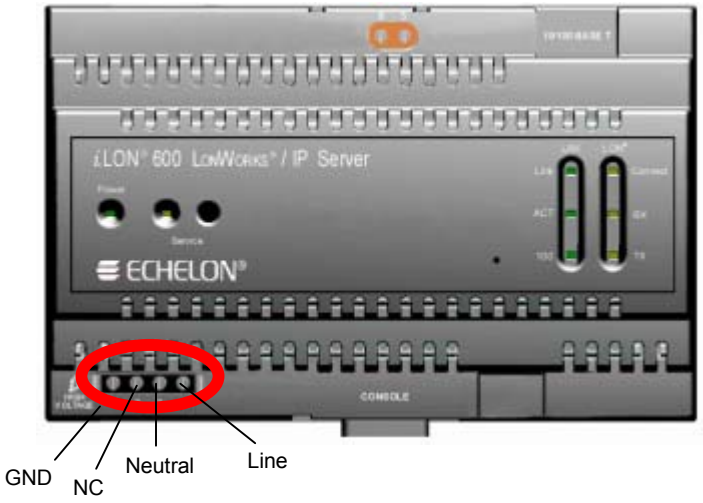


Figure 6. High Voltage Mains Screw Terminals

Table 3. *i*.LON 600 Server AC Power Mains Connections		
Screw Terminal	***Enclosure Marking***	***Mains Connection***
1	E	Earth ground
2	NC	No connect
3	N	Neutral
4	L	Line

SAFETY AND HIGH VOLTAGE WARNING

Ensure that the AC power mains are turned OFF before removing the cover, handling the mains wiring, or connecting any mains cabling to the *i*.LON 600 device.

DO NOT under any circumstances operate the *i*.LON 600 device to mains voltages outside of the range 115/230VAC, -14% to +8%, 50/60Hz ±2.5Hz.

ALERTA DE SEGURIDAD Y ALTO VOLTAJE

Asegúrese que la red electrica de corriente alterna AC este DESENERGIZADA antes de: quitar la cubierta, manipular los cables de alimentacion o conectar cualquier cableado al dispositivo *i*.LON 600.

Bajo NINGUNA circunstancia conecte el dispositivo *i*.LON 600 a redes electricas con voltajes fuera del rango 115/230VAC, -14% a +8%, 50/60Hz ±2.5Hz.

SECURITE ET AVERTISSEMENT HAUTE TENSION

Assurez vous que l'interrupteur Marche Arrêt est dans la position Arrêt avant d'enlever le capot, manipuler les câbles d'alimentation, ou bien quand vous branchez un cordon secteur au *i*.LON 600.

Il ne faut JAMAIS connecter le *i*.LON 600 à une tension d'alimentation hors de la plage 115/230VAC, -14% à +8%, 50/60Hz ±2.5Hz.

SICHERHEITSHINWEIS: VORSICHT NETZSPANNUNG!

Stellen Sie sicher, daß die Netzspannung AUSgeschaltet wurde (Schalterstellung OFF), ehe der Gehäusedeckel entfernt, an der Spannungsversorgung hantiert oder irgendeine Netzverbindung mit dem *i*.LON 600 Gerät hergestellt wird.

AUF KEINEN FALL darf das *i*.LON 600 mit Netzspannungen ausserhalb des Bereichs 115/230V, -14% bis +8%, 50/60Hz±2.5Hz betrieben werden.

AVVERTENZA SULLA SICUREZZA E SULL'ALTA TENSIONE!

Assicurarsi che la rete elettrica sia SPENTA prima di rimuovere il coperchio, maneggiare i cavi di alimentazione, o connettere qualsiasi cavo al *i*.LON 600.

NON connettere mai per nessun motivo il *i*.LON 600 a tensioni al di fuori del range 115/230VAC, da -14% a +8%, 50/60Hz +-2.5Hz.

LONWORKS Network

The *i*.LON 600 is provided with one of two types of LONWORKS channels: TP/FT-10 free topology twisted pair (Models 72601 and 72603), or TP/XF-1250 (models 72602 and 72604). The twisted pair interfaces are polarity-insensitive and require connecting the twisted pair to terminals 5 and 6.

The screw terminals accept 0.34 – 4.0mm^2 (22 – 12AWG) gauge solid wire. The optimum tightening torque for the screw terminals is 0.75mm (6 lbs. in.) maximum. The ideal flathead screwdriver tip width is 3mm (0.12"). Wires should be stripped to a length of 7mm (0.28"). Although not required, you should use a soldering iron to tin the stripped lengths of any stranded wires to prevent fraying and inadvertent contact with adjacent terminals

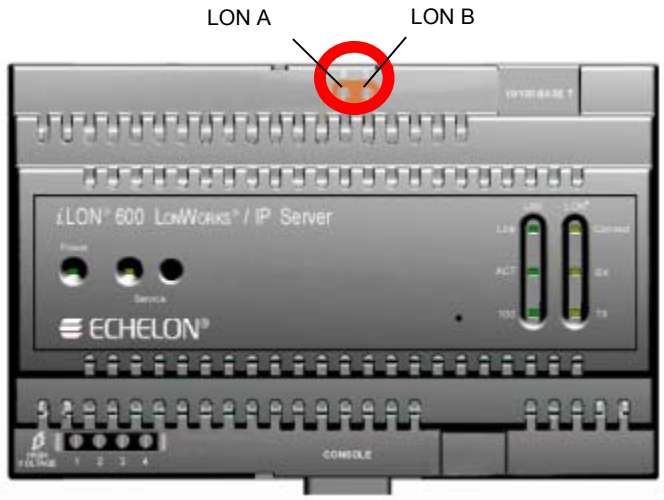


Figure 7. Twisted Pair Terminals

Table 4. LONWORKS TP/FT-10 Network Connections

Screw Terminal	*Enclosure Marking*	*LONWORKS Network Connection*
5	LON B	TP/FT-10 twisted pair, TP/XF-1250 twisted pair
6	LON A	TP/FT-10 twisted pair, TP/XF-1250 twisted pair

Applying Power to the *i*.LON 600

Once you have mounted the *i*.LON 600 and connected all wiring, apply AC mains power to the unit.

The LEDs on the *i*.LON 600 will flash for less than a minute as the unit boots. Once the unit is powered and operational, the green Power LED will stay solid ON.

i.LON 600 LED Displays and Buttons

Once you have applied power to your *i*.LON 600, LEDs will provide you with information on the status of your *i*.LON 600. Table 5 describes each LED and its meaning.

Table 5. LED Status Information

LED	*Description*
Power	This LED is on when the *i*.LON 600 unit has power. When *i*.LON 600 applications are not running, this light blinks rapidly.
Service	This LED is normally off. Blinking indicates the router is not configured. This LED is solid ON when the *i*.LON 600 is in Security Access Mode (see *Setting the i.LON 600 Security* in Chapter 4).
LAN Link	Lights when an Ethernet connection has been established.
LAN ACT	Lights when there is activity on the Ethernet connection.
LAN 100	Lights when the Ethernet connection is at 100 Mbps.
LON Connect	This light is OFF if the *i*.LON 600 has not been configured in a LONWORKS/IP channel by the Configuration Server. If the *i*.LON 600 has been configured in a LONWORKS/IP channel, but needs updating, the light will blink. The light stays solid ON when the *i*.LON 600 has a current configuration for a LONWORKS/IP channel.
LON RX	Lights when a packet is received on the FT-10/TP-1250 port.
LON TX	Lights when a packet is transmitted on the FT-10/TP-1250 port.

The *i*.LON 600 has two buttons: the service pin and the reset switch. The service pin is a recessed pushbutton that sends LONWORKS service pin messages on the LONWORKS channels. You can use this button to commission an *i*.LON 600 with LonMaker or perform a security access reset (described later in this document).

The reset switch is a concealed pushbutton used to reset the *i*.LON 600 server and is located to the left of the LAN 100 LED. You can use a straightened paper clip to access the reset switch. See Figure 8.

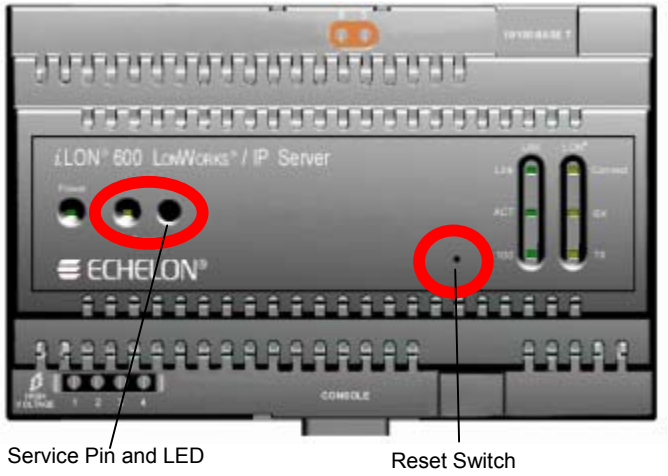


Figure 8. *i*.LON 600 Service Pin and Reset Switch

3

LONWORKS/IP Channels Background & Definition

Traditionally, LONWORKS networks operate over dedicated network wiring such as twisted pair. A given segment of wiring is referred to as a channel. With the introduction of LNS 3.01 and the *i*.LON 1000 Internet Server (and now the *i*.LON 600 LONWORKS/IP Server), a new kind of channel has been created, the LONWORKS/IP channel.

Introduction to the LONWORKS/IP Channel

Unlike traditional LONWORKS channels that use a dedicated physical wire, a LONWORKS/IP channel uses a shared IP network, and is defined by a group of IP addresses. These addresses form a "virtual" wire. *i*.LON 600s and PCs running LNS (version 3.01 or better) use this virtual wire in the same way they use traditional dedicated twisted pair wiring.

The concept is similar to a Virtual Private Network (VPN). Each *i*.LON 600 in the system is aware of its peers and each *i*.LON 600 keeps peer information in its routing tables so it can forward "tunneled" LONWORKS packets to the correct IP address. Figure 9 shows a typical channel configuration.

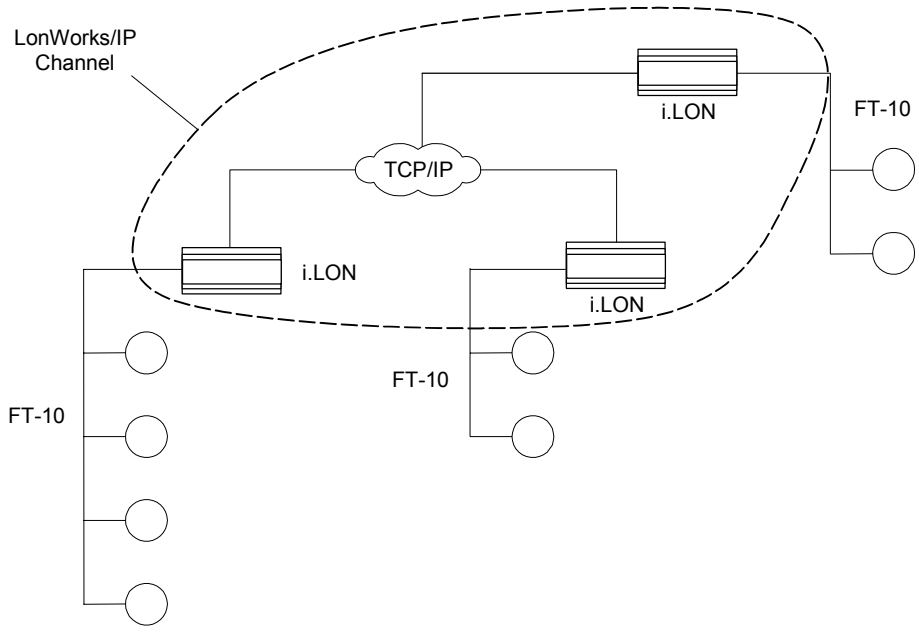


Figure 9. A LONWORKS/IP Channel

Because a virtual wire is created by the *i*.LON 600s, Figure 9 topology is logically the same as Figure 10.

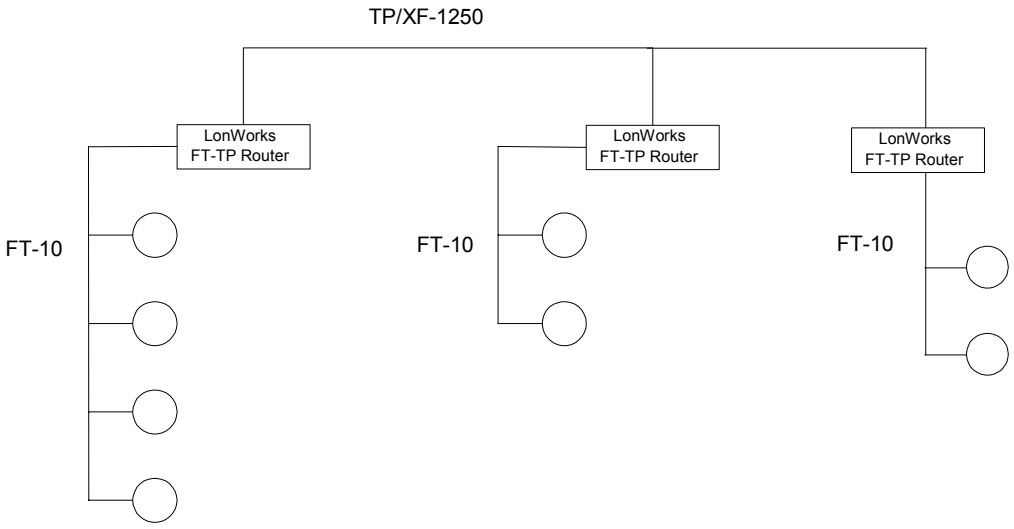


Figure 10. A LONWORKS Network with a Traditional TP-1250 High Speed Backbone

The *i*.LON 600 routing engine is designed to deal with the potentially large latencies introduced by large IP networks such as the Internet. Without this intelligent routing engine, certain LONWORKS network services, such as the ability to detect duplicate packets, could be compromised.

Note that in Figure 9 or Figure 10, a PC running LNS 3.01, MIP, or other mechanism could be attached to any of the FT-10 channels.

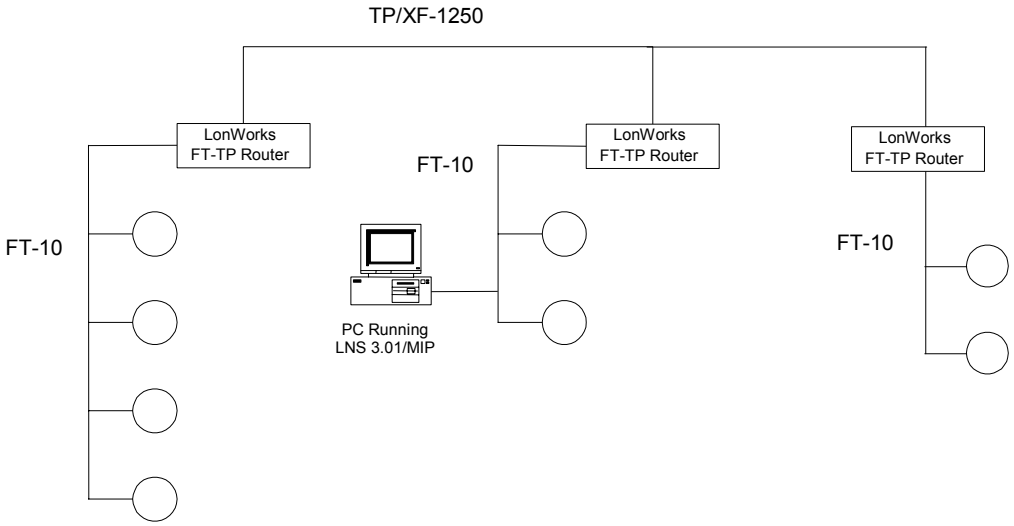


Figure 11. PC Connected to an FT-10 Channel

PCs running LNS 3.01 incorporate the same routing intelligence as an *i*.LON 600. Therefore, PCs running LNS version 3.01 or better can be directly connected as a member of the LonMaker/IP channel side of any *i*.LON 600. This allows topologies like the one shown in Figure 12:

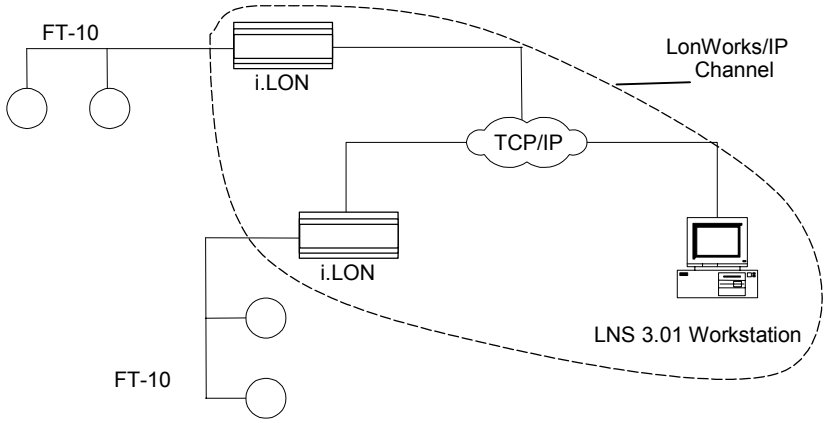


Figure 12. *i*.LON 600 and LNS 3.01 Workstation on a LONWORKS/IP Channel

A complete installation may contain many *i*.LON 600s and PCs – all sharing a LONWORKS/IP channel. Because the LONWORKS/IP channel can exist on any IP network, a system may now span the entire globe as easily as it once spanned a single building, as shown in Figure 13.

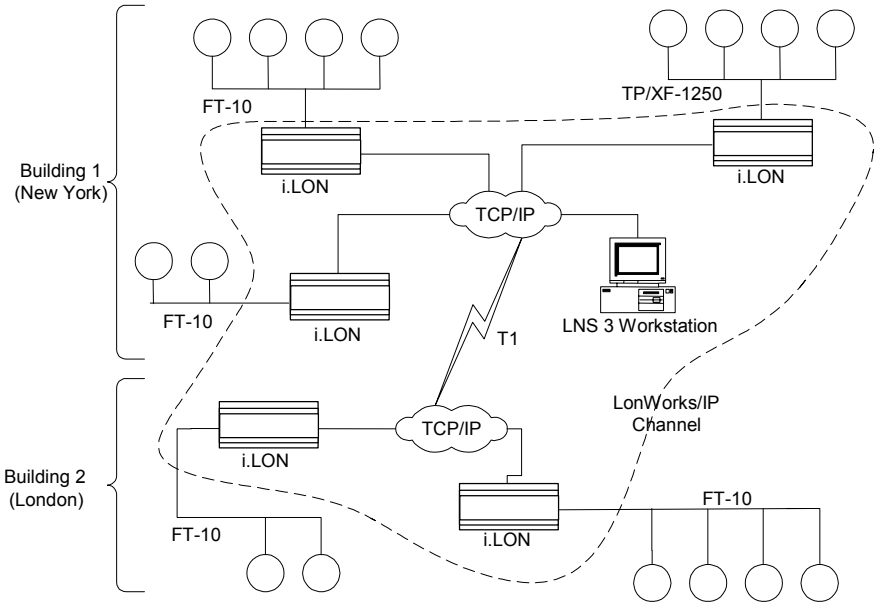


Figure 13. Large LONWORKS Network using a LONWORKS/IP Channel

Note: A single LONWORKS/IP channel may contain up to 256 LONWORKS/IP devices. If your installation requires more than 256 LONWORKS/IP devices, you must create multiple LONWORKS/IP channels and bridge the IP channels using *i*.LON 600s (models 72602 or 72604) configured as repeaters.

4

Configuring the *i*.LON 600 TCP/IP Settings

This chapter describes how to configure the IP information for an *i*.LON 600.

IP Resources Required to Create LONWORKS/IP Channels

Before you install an *i*.LON 600 on an existing IP network, you will need to work closely with the IP network administrator to gather a list of the resources. You must also provide information about your *i*.LON 600 to the network administrator so they can adjust intervening firewalls to allow bi-directional communication with the outside world.

Information/Resources to be Acquired From the Network Administrator

To install one or more *i*.LON 600s on an existing IP network, you must obtain the following information and resources from the network administrator:

- IP Address (preferably static)
- Subnet Mask
- Default Gateway
- DNS Servers
- SNTP Server (optional, but recommended for high latency networks like WANs or the Internet)

In return, you must provide the network administrator with information about your *i*.LON 600s.

- Your i.LON 600s, by default, communicate on ports 1628 (UDP), and they respond to FTP and HTTP protocols. The Configuration Server, by default, uses port 1629 (UDP). See the *TCP/IP Configuration* section in this chapter for more information.
- Depending on your setup, your *i*.LON 600 may also contact an SNTP server (by default on port 123).

If the LONWORKS/IP channel spans a firewall or NAT router, it is important that these ports are open or forwarded to the *i*.LON 600. See Chapter 6 for more information.

The Internet Assigned Numbers Authority (IANA) defines default ports 1628 and 1629 for LONWORKS/IP channels. For more information, visit www.iana.org. You may also want to allow FTP and HTTP traffic to pass through your *i*.LON 600s.

Use a table similar to the one below to plan your installation. The IP address of members within a LONWORKS/IP channel should be static. You can use IP addresses that are not static, but this requires additional configuration (see *Appendix A*). Addresses may be translated using Network Address Translation (NAT), though this also requires additional configuration.

Table 6. Installation Planning

Device	***IP address***	***Port***	***Subnet Mask***	***Gateway***	***Host Name***	***Host Name Reg. Req'd***	***DNS Machine***	***SNTP Server***
Configuration Server PC		1629						
LNS 3 PC		1628						
i.LON 1		1628 (80 & 21 are optional)						
i.LON 2		1628 (80 & 21 are optional)						
i.LON 3		1628 (80 & 21 are optional)						
i.LON 4		1628 (80 & 21 are optional)						
i.LON 5		1628 (80 & 21 are optional)						
i.LON 6		1628 (80 & 21 are optional)						
i.LON 7		1628 (80 & 21 are optional)						

Configuring the *i*.LON 600

After you install the *i*.LON 600 software and connect your i.LON 600, configure it by performing the following steps:

1. Connect the i.LON 600 directly to your PC using an Ethernet cable. If your PC uses DHCP, attach the i.LON 600 to your building's network. See Chapter 7 for more information.
2. Open a DOS command prompt on your PC and enter the following command (this is the exact text of the command):

```
route add 192.168.1.0 mask 255.255.255.0 %COMPUTERNAME%
```

This command allows your computer to communicate with the default IP address (192.168.1.222) even when your computer is on a different subnet. This command will not persist through computer reboots, however, you can add it to your computer's startup script.

Note: You must specify a new IP address for your *i*.LON 600 after you complete the setup. Leaving your *i*.LON setup with the default address could cause communication problems in a multi-device network.

3. Optionally perform a security access reset on the *i*.LON 600 as described in *Security Access Reset* later in this chapter. Set the security options as described in *i.LON 600 Security Web Page*.
4. Launch Internet Explorer 6 or later and point your browser to `http://192.168.1.222`. The *i*.LON 600 Welcome Web page appears:

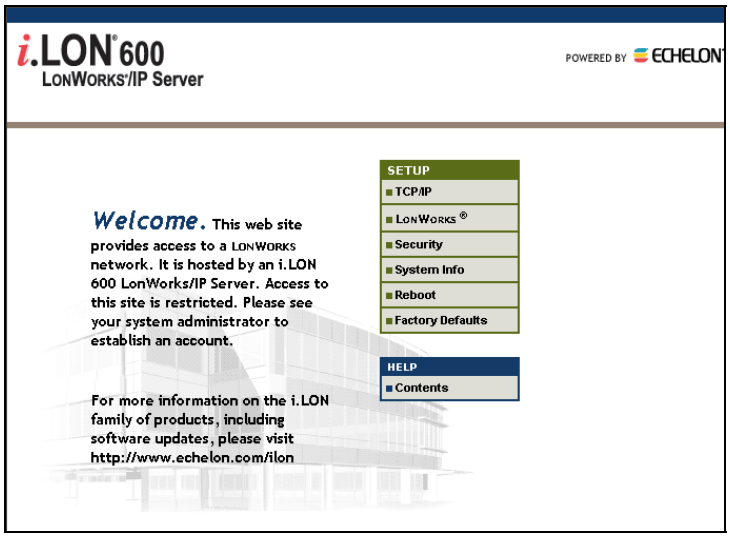


Figure 14. Welcome Screen

5. Click **TCP/IP**.
6. Enter `ilon` in the User Name field and `ilon` in the Password field when prompted. The TCP/IP Configuration Web page opens. The default user name and password is ilon/ilon respectively and is always used after a security access reset is performed. To change the user name and password, run the *i.LON 600 Web Server Security and Parameters* application (see Appendix E).

7. Enter the TCP/IP parameters provided by your network administrator. These settings are described in greater detail in the *Configuring TCP/IP Settings* section below.
8. Reboot your *i*.LON 600 using the Reboot Web page for the parameters to take effect.
9. Connect the *i*.LON 600 to your network.
10. Repeat steps 3-9 for each *i*.LON 600 you wish to install on your network.

Configuring TCP/IP Settings

Set the TCP/IP information for the *i*.LON 600 by following these steps:

1. From the Welcome screen, click **TCP/IP** in the menu. The TCP/IP Web page opens.

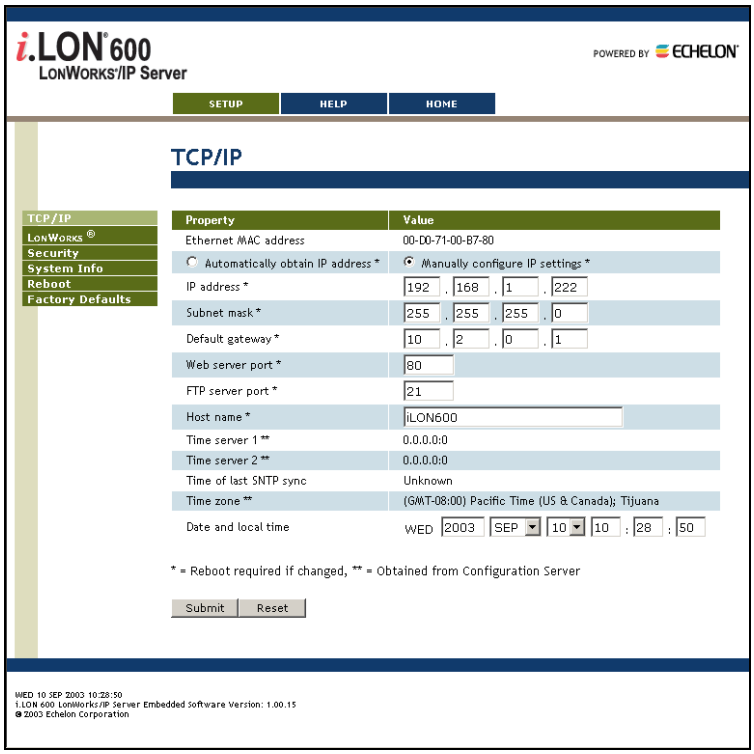


Figure 15. TCP/IP Settings Web Page

2. Enter the following information:

Automatically Obtain IP Address	Set this option to have the *i*.LON 600 obtain its IP address, subnet mask, and default gateway from the local network's DHCP server. If this option is set, you have the option of obtaining the Domain Suffix and/or DNS Server 1 automatically. If you change this value, you must reboot the *i*.LON 600 for the change to take effect. If the DHCP server cannot be contacted, the IP address will be set to `192.168.1.222`, the subnet mask will be set to `255.255.255.0`, and the default gateway will be temporarily set to `192.168.1.222`. As soon as the DHCP server is contacted, the *i*.LON 600 will reboot itself and receive a new IP address. This is not recommended and requires additional configuration of the LONWORKS/IP channel as described in Chapter 7.
Manually Configure IP Settings	Set this option when specifying a static IP address, subnet mask, and gateway for the *i*.LON 600. This is the default (**and recommended**) setting. If you change this value, you must reboot the *i*.LON 600 for the change to take effect.

IP Address	Static IP address used by the *i*.LON 600 if *Manually Configure IP Settings* is set. The default value is `192.168.1.222`. Contact your network administrator for a static IP address.
Subnet Mask	Subnet mask used by the *i*.LON 600 if *Manually Configure IP Settings* is set. By default, this value is `255.255.255.0`.
Default Gateway	Gateway used by the *i*.LON 600 if *Manually Configure IP Settings* is set. By default, this value is `192.168.1.222`.
Host Name	The TCP/IP host name of the *i*.LON 600. By default, the host name is `iLON600`. The URL of the *i*.LON 600 is `Hostname.DNS Suffix` (*i.e.* if Hostname is set to `ilon600Alpha`) and Domain Suffix is set to `Echelon.com`, the URL will be `ilon600Alpha.Echelon.com`. Valid characters are numbers, letters, and the hyphen ('-') character. By default, this value is set to `iLON600`. If you change this value, you must reboot the *i*.LON 600 for the change to take effect. This field has a maximum length of 19 characters.
Web server port	Port used by the *i*.LON 600's web server. The default is the standard web server port number (80). If set to a value other than 80, you need to specify the port number in your browser (e.g. 192.168.1.222:8080) after rebooting the *i*.LON 600.
FTP server port	Port used by the *i*.LON 600's FTP server. The default is the standard FTP server port number (21).
Date and local time	This allows you to manually change the time settings for the *i*.LON 600. Changing the time settings on your *i*.LON 600 will not affect the time settings of the Configuration Server. Note: If SNTP servers are not defined, changing this value can cause the router to not work properly.

3. Click **Submit** to save the changes you made to this Web page. Note that all fields marked with an asterisk require a reboot before the new values take effect. Click **Reset** to leave all fields unchanged. Click **Help** on the Web page for more information about the fields on this screen.

Setting the LonWorks/IP Port

The default port setting for the *i*.LON 600 is 1628. You can set your *i*.LON 600 to reside on any port you wish. See www.iana.org for information on port guidelines or if you want to reserve a special port for your *i*.LON 600.

To specify a new port for your i.LON 600, follow the below steps:

1. Click **LonWorks** from the **Setup** Web page menu. The below screen appears.

Figure 16. Specifying a LONWORKS/IP Port

2. Enter a new port number in the **LonWorks/IP port** field.
3. Click **Submit**.

Rebooting the i.LON 600

To ensure that certain TCP/IP settings take effect, click the **Reboot** button on the Reboot Web page. If the i.LON 600 is located behind an NAT firewall, you should check the **This i.Lon 600 LonWorks/IP Server is located behind a NAT firewall** checkbox. After clicking **Reboot**, a Web page will be displayed telling you that the *i*.LON 600 is rebooting. This process takes approximately one minute. While the *i*.LON 600 reboots, the LEDs on the *i*.LON 600 will flash. Once the reboot is complete, the green Power LED will stay on solidly and your browser will be directed to the Welcome Web page.

If DHCP is enabled, this page may not redirect the Web browser to the **Welcome** page because a new address from the DHCP server is unknown. If this is the case, issue the **show all** command from the console application or ask your network administrator to determine the new IP address of the *i*.LON 600. If your DHCP server has the capability to dynamically propagate newly assigned device IP address and target name to the DNS server (as is the case with the Windows 2000 DHCP server), you should be able to connect to the *i*.LON 600 after reset using its fully qualified hostname. See Chapter 7 for more information on DHCP. See Appendix B for more information on the Console Application.

Note: After you begin a reboot, the *i*.LON 600 Reboot Web page displays a message informing you of how much time is left for the reboot. If you are using popup blocker software, this message may not be displayed.

Restoring Factory Defaults

When in secure access mode (see the *Security Access Reset* section later in this chapter), the Security Web page will display a link to the Restore Factory Defaults Web page. Click the **Restore Factory Defaults** button on this page to reset the configuration of the *i*.LON 600 to its factory default. This will restore the following *i*.LON 600 configuration:

Table 7. *i*.LON 600 Factory Default Settings	
FTP user name:	`ilon`
FTP password:	`ilon`
Automatically obtain IP address:	`false`
IP address:	`192.168.1.222`
Subnet mask**:**	`255.255.255.0`
Gateway:	`192.168.1.222`
Web server port:**:**	`80`
FTP server port:	`21`
Hostname:	`ilon600`
SNTP servers:	`0.0.0.0`
Time zone:	`(GMT-08:00) Pacific Time (US & Canada); Tijuana`
LONWORKS/IP port:	`1628`
LonTalk addresses:	`unconfigured`

This will restore the IP address back to `192.168.1.222`, so you may need to place your computer on that subnet or use the route command to communicate with the *i*.LON 600 after the reboot is complete.

Setting the i.LON 600 Security

The *i*.LON 600 uses a number of security measures:

- *Security Access Reset*. A security access reset is required to access the Security Web page. A security access reset requires physical access to the *i*.LON 600 hardware.
- *Security Web Page*. The *i*.LON 600 Security Web page allows you to password protect or disable FTP and Web server access to the *i*.LON 600.
- *MD5 Authentication.* The *i*.LON 600 can use MD5 authentication for communications on the LONWORKS/IP channel, requiring a 16-byte authentication key.

Security Access Reset

The Security Web page of the *i*.LON 600 is only available after performing a security access reset. This Web page allows you to set the user name and password used for FTP access to the *i*.LON 600, the MD5 Authentication Key, and allows you to determine what methods may be used to access the *i*.LON 600.

To perform a security access reset, follow these steps:

1. Remove the *i*.LON 600 from the TCP/IP network and attach it directly to your computer using an Ethernet cable. This step is optional, but is necessary for optimal security. To communicate with the *i*.LON 600, you may need to set your PC's IP configuration if your PC has a different subnet than the *i*.LON 600. See *Setting Your PC's IP Configuration* below for more information.
2. Press and hold the service pin and reset button simultaneously on the *i*.LON 600 using a ballpoint pen, straightened paper clip, or similar device. You can also reboot the *i*.LON by holding down the service pin and clicking **Reboot** from the Reboot Web page (see *Rebooting the i.LON 600*, later in this chapter).
3. Release the reset button. The LEDs will light for about two seconds.
4. Continue holding the service pin down for approximately 10 seconds. During this time, both the Power and Service LEDs will blink rapidly. The Service LED will then illuminate solid orange. You can release the service pin.

The *i*.LON 600 will now be in security access mode. When the *i*.LON 600 is in security access mode, its IP address should be set to the default setting of `192.168.1.222`, the subnet mask should be set to `255.255.255.0`, and the gateway should be set to `192.168.1.222`, the Web server port will be set to 80, and the FTP server port will be set to 21. They are changed back to the values specified on the Setup and Security Web pages once the *i*.LON 600 exits security access mode (*i.e.* when the *i*.LON 600 is rebooted).

You may need to set your PC's IP configuration in order to communicate with the i.LON 600 after performing a security access reset. See the *Setting Your PC's IP Configuration* section below for more information.

When in security access mode, you can access the Security, Reboot, and Factory Defaults Web pages. The *i*.LON 600 Web server is always enabled in security access mode regardless of the Enable Web Server property described in the following section.

Setting Your PC's IP Configuration

This may not work if your PC uses DHCP to obtain an IP address. You may need to set your PC to a static IP address.

The *i*.LON 600's IP address change may place the *i*.LON 600 on a subnet that your computer cannot communicate with. For example: in order to communicate with the *i*.LON 600 after a Security Access Reset, you can either modify your computer's IP configuration to place it on the 192.168.1.* subnet or enter the following command in the Windows Command Prompt:

```
route add 192.168.1.0 mask 255.255.255.0 %COMPUTERNAME%
```

This command allows your computer to communicate with the *i*.LON 600 even when they are not on the same subnet. This command does not persist through computer reboots, but you can include the "–p" switch to make it persistent.

i.LON 600 Security Web Page

To access the Security Web page, perform a security access reset as described above, point your browser to `192.168.1.222`, and click **Security**. The following Web page opens:

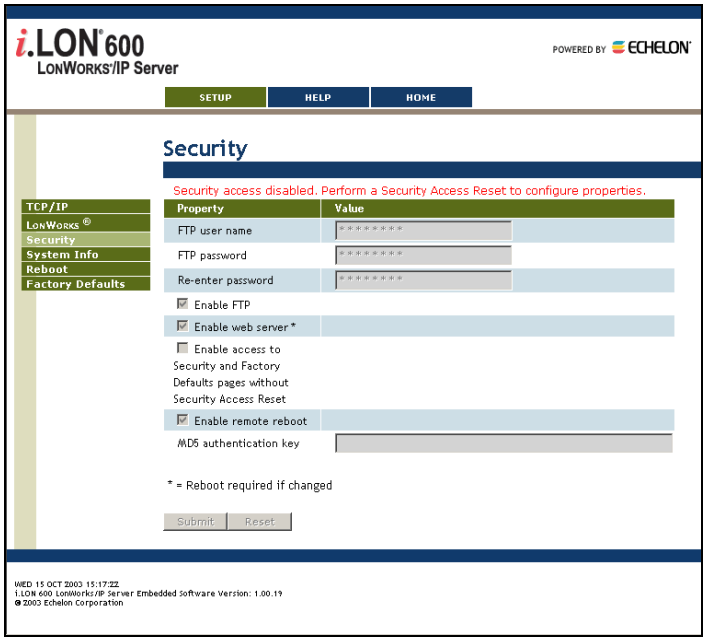


Figure 17. Security Web Page

This Web page allows you to enter the following options (you must click the **Submit** button after changing any options):

FTP User name	The FTP user name for the *i*.LON 600. The default user name is `ilon`. The user name can be up to 20 characters long and may contain letters, numbers, and the underscore character.
FTP Password	The FTP password for the *i*.LON 600. The default password is `ilon`. The password will appear as asterisks. The password can be up to 20 characters long and may contain letters, numbers, and the underscore character.
Re-enter Password	Reenter the FTP Password.
Enable FTP	This option allows FTP access to the *i*.LON 600. This option is enabled by default, but in most cases should be disabled once the system is installed.

Enable Web server	Set this option to allow Web access to the *i*.LON 600. This option is enabled by default. The *i*.LON 600 must be rebooted before this option will take affect. Note: If you disable this option, you will not be able to access the *i*.LON 600 Web pages after a reset. If you need to reenable Web access, you can reset this option by performing a security access reset, as described above.
Enable access to this page without Security Access	If checked, this option allows you access to the security page without first requiring a security access reset. WARNING: Using this option greatly reduces the *i*.LON 600 security.
Raw MD5 Authentication Key	MD5 authentication key is used to secure the LONWORKS /IP channel. This value must match the value specified in the LONWORKS/IP Configuration Server.

MD5 Authentication

You can specify a 16 HEX pair authentication key for all devices on your network. When authentication is enabled and the *i*.LON 600 prepares to send an IP packet, the *i*.LON 600 uses the authentication key and the public MD5 algorithm to compute a digest over each LONWORKS packet in the UDP payload. All authentication keys within a single network must match.

To reset a lost authentication key, you must obtain physical access to the device and reset the key through the setup Web page or the device's serial port. See the *MD5 Authentication* section *Chapter 8* for more information on setting up this feature.

Note: If you are using authentication, you must use an SNTP server. If you lose communication with your i.LON 600, you may need to perform a factory default or use the console application and manually select a different SNTP server.

5

Creating a LONWORKS/IP Channel

This chapter describes how to use the Configuration Server to create a LONWORKS/IP channel. The Configuration Server is installed with the *i*.LON 600 software, so before proceeding, install the *i*.LON 600 software as described in Chapter 1.

Creating a LONWORKS/IP Channel

To create a LONWORKS/IP channel, you must configure each LONWORKS/IP device that will be on the channel and enter information about each device in the Configuration Server. A LONWORKS/IP device can be an *i*.LON 600, *i*.LON 1000, or a PC running LNS 3.01 or higher. The following describes how to setup two *i*.LON 600s on an IP backbone.

In Figure 18, a LONWORKS device on channel 1 is bound to a device on channel 3 across an IP backbone. The PC running the Configuration Server resides on channel 2 and has access to both i.LON 600s through an IP connection. The PC running the LonMaker software is connected to channel 1. To simplify the network, you can run the LonMaker software and the Configuration Server software on a single PC.

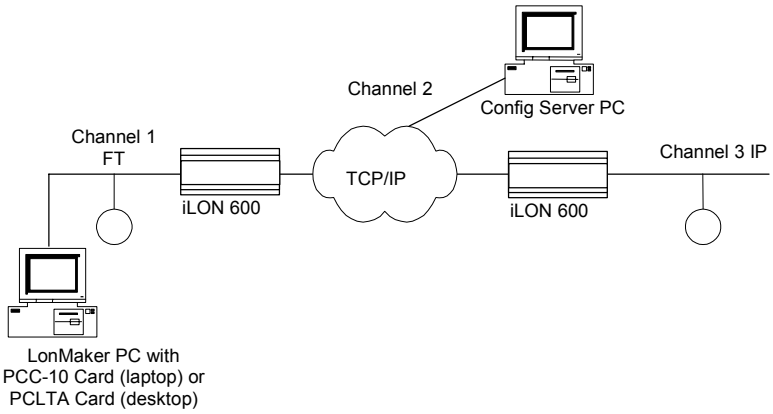


Figure 18. Setting Up a LONWORKS/IP Channel

To create a network like the one illustrated in Figure 18, follow the below steps.

1. Set the IP address, subnet mask, and default gateway for all *i*.LON 600s using the *i*.LON 600 setup web pages as described in Chapter 4.
2. Start the Configuration Server application. From the Windows desktop click on **Start**, choose **Programs**, select **Echelon *i*.LON 600**, and click on **LonWorks-IP Configuration Server**. The Configuration Server main dialog appears:

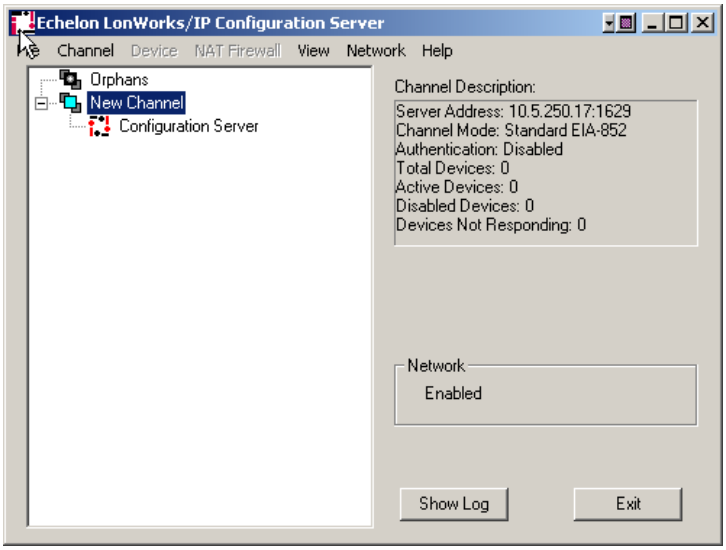


Figure 19. Echelon LONWORKS/IP Configuration Server

3. Verify that the Configuration Server is attached to your IP network. The Network status box should indicate "Enabled". If the Network box does not indicate "Enabled", select **Enabled** from the **Network** menu. The Configuration Server should correctly detect and display the IP address of your PC in the Channel Description window. To verify the Configuration Server PC's IP address, select **Settings** from the **Network** menu and confirm that the Configuration Server's IP address is shown in the Local IP Address or host name field. See Figure 20.

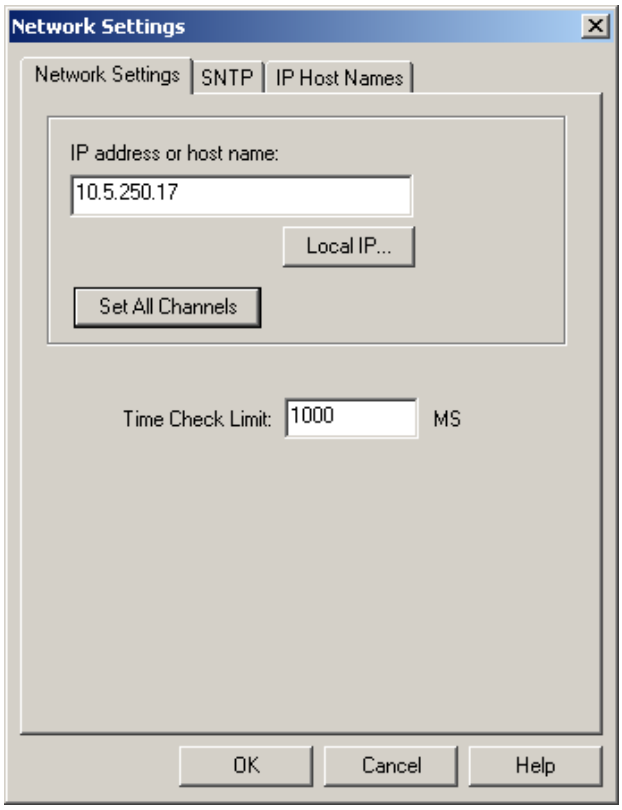


Figure 20. Configuration Server Network Settings

If your PC has more than one IP address assigned to it, you may select which IP address should be used by the Configuration Server using the **Local IP…** button. On the Configuration Server main dialog screen in Figure 20, the New Channel's Server Address is set to 10.5.250.17. This confirms that the Configuration Server is running on a PC with an IP address of 10.5.250.17.

The defaults for the channel properties should 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 may need to adjust the channel property settings and/or use SNTP time servers to synchronize LONWORKS/IP member devices. See the Advanced Topics section for more information.

4. Configure your channel mode by right clicking on the New Channel icon and selecting **Properties** from the menu. Select either **Backward Compatible, Standard EIA-852** or **Extended Firewall Support** mode. See Chapter 8 for more information.
5. From the Configuration Server main dialog, right-click on the new channel, and select **New Device**. An icon representing a LONWORKS/IP device is added to the channel. This device could be either an *i*.LON 600, *i*.LON 1000, or a LONWORKS/IP interface on a PC running LNS 3.01 or higher.
6. Right click on the new device and select **Rename Device** to enter a descriptive name.
7. Right click and select **Device Properties**. The device properties dialog appears.

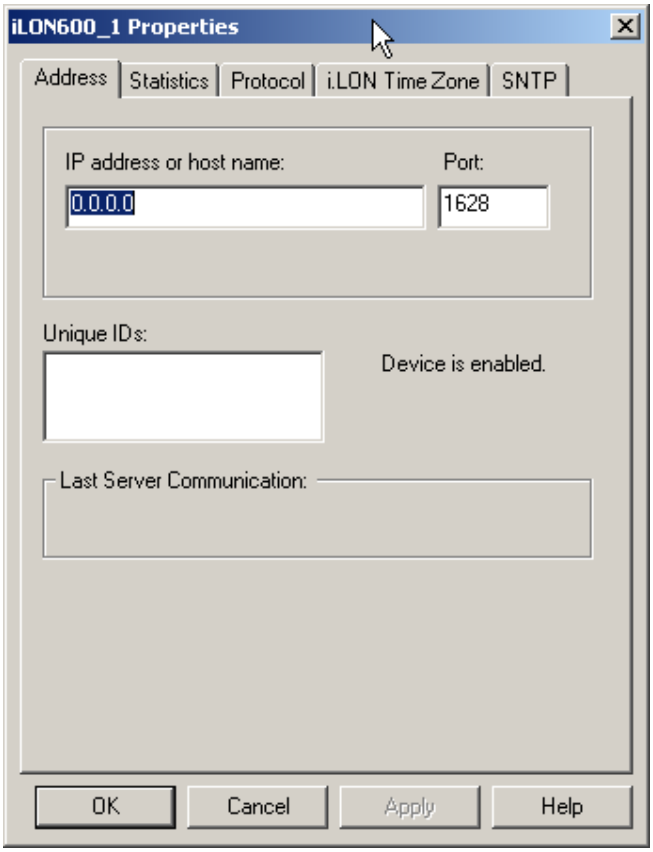


Figure 21. Configuration Server Device Properties: Address Tab

8. Enter the IP Address of the *i*.LON 600 (obtained from your network administrator) and click **Apply**. This is the same address that you assigned to the *i*.LON 600 using the setup Web pages.

If you use a host name, it must be registered in a DNS server that is available to the Configuration Server PC. See Chapter 7 for more information about DNS.

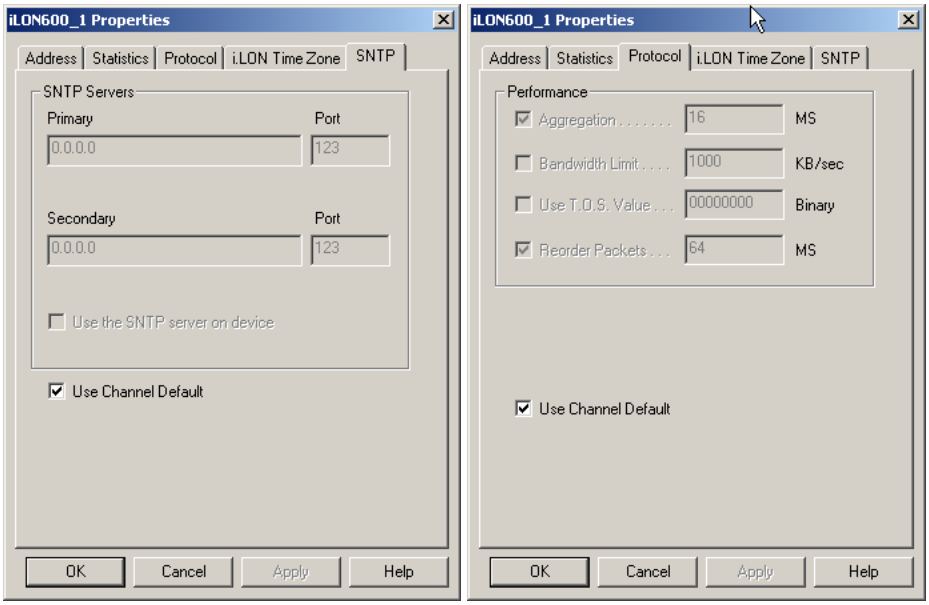


Figure 22. Configuration Server Device Properties: SNTP and Protocol Tabs

9. Click the **SNTP** tab and select the **Use Channel Default** checkbox.
10. Click the **Protocol** tab and select the **Use Channel Default** checkbox.
11. Click the **i.LON Time Zone** tab and set the time zone to correspond with the geographical area of the device.
12. Click **Apply**.
13. Repeat steps 5-10 for each device. As each LONWORKS/IP device is added to the LONWORKS/IP channel.
14. From the Configuration Server dialog, select **Update Members** from the **Channel** menu or **Update Device** from the **Device** menu. The 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.

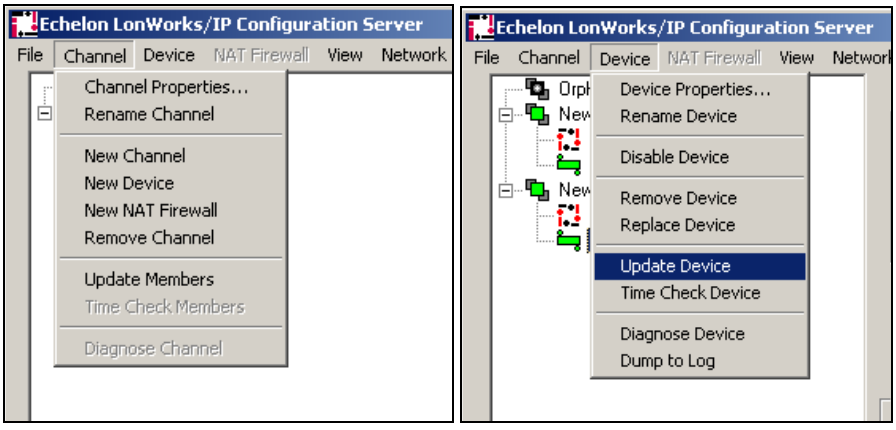


Figure 23. Configuration Server: Update Members and Update Device

When you select **Update Members** or **Update Device,** a communication process starts between the Configuration Server and the selected devices. For channels set up in Standard EIA-852 and Extended Firewall Support modes, this process conforms to the EIA-852 protocol standard. For backward compatible channels, the protocol used is not strictly compatible with EIA-852, although it is very similar. You can view this process by clicking the **Show Log** button.

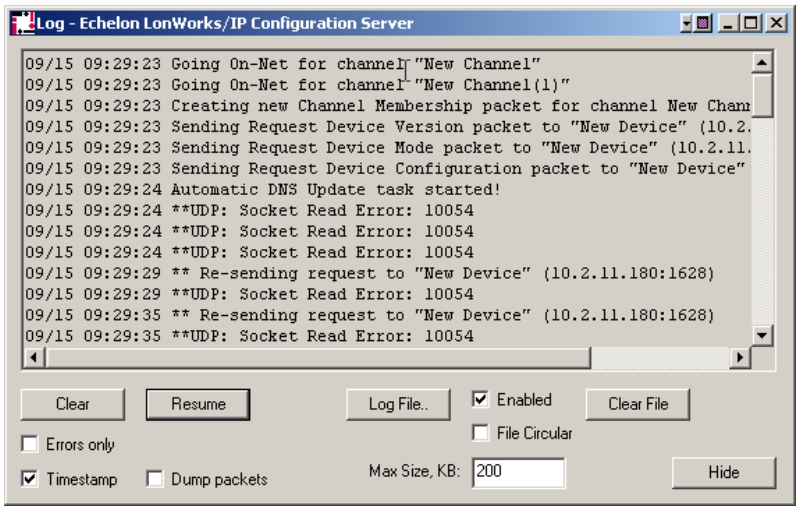


Figure 24. Show Log Screen

If any information between channel members is outdated, the Configuration Server will send updated information to each channel member.

Success or failure of this step is reflected in the Configuration Server log screen and the color of the devices in the tree view on the main dialog. The meaning of each color of the device status is shown in Table 8.

Table 8. Configuration Server Device Status Indicator

Color	***Status Description***
Cyan	No communication has been made with the device during this session.
Green	Normal, and communication has occurred with the device during this session.
Red	Communication with the device has failed after you select Update Members or Update Device. Usually, this occurs when no response is received from a device to which a request was made. Make sure that all security and IP settings are configured properly.
Yellow	Normal, but the Time Check failed for this device.
Orange	The *i*.LON 600's configuration is out of date, incorrect, or incomplete. This normally indicates work in progress. When the Configuration Server updates the *i*.LON 600, the icon will turn green. Note that in a large channel (> 40 devices) this can take several minutes. Also note that changing a bind in LonMaker can require that the routing tables in EVERY *i*.LON 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	Device is disabled.

IMPORTANT:

The Configuration Server must be running when you configure LONWORKS/IP devices using a LONWORKS network management tool such as LonMaker.

i.LON 600 System Information

You can verify the rate at which packets are sent and received by your *i*.LON 600 over the network the network by viewing the **System Info** Web screen. This screen also provides setup information about your *i*.LON 600 including *i*.LON 600 model number, channel type, CPU speed, firmware version, and bootrom version. This information may be helpful in troubleshooting your *i*.LON 600 or optimizing network performance. To access the System Info Web page, point your browser to your *i*.LON 600 and click **System Info** on the right-hand menu bar in the **Welcome** screen. See Figure 25.

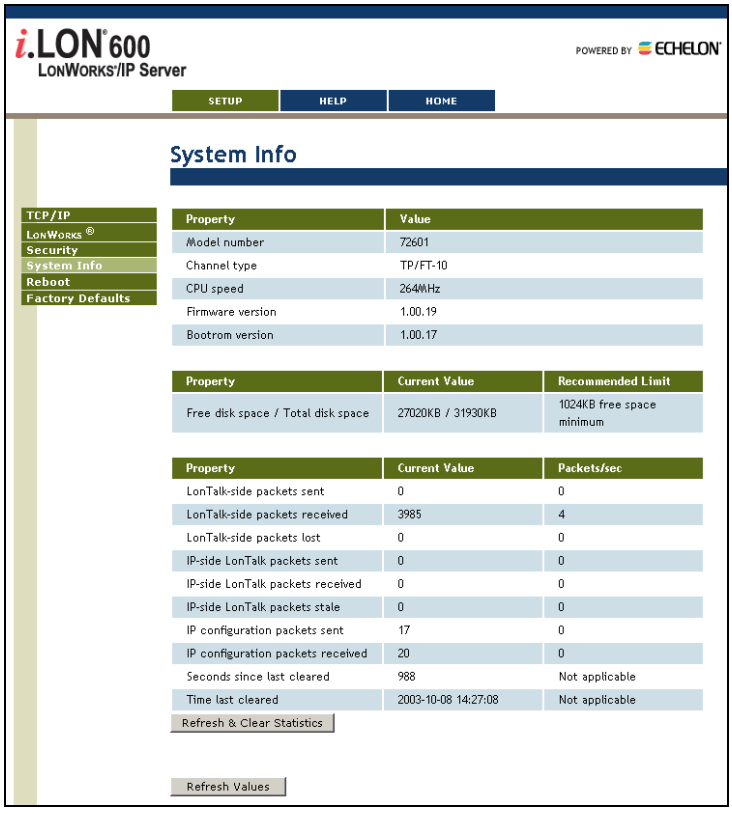


Figure 25. System Info Web Screen

While viewing your system information, you have two options: **Refresh & Clear Statistics** or **Refresh Values**. When you click the **Refresh & Clear Statistics** button, information in the Current Value and Packets/sec columns is set to zero and the **Seconds since last cleared** field resets to zero. Clicking the **Refresh Values** button updates the Current Value and Packets/sec information.

The steps above create a “virtual wire” out of any group of IP addresses. The members of this group can now share information and appear as a standard LONWORKS channel.

Designing a LonMaker Network Containing LONWORKS/IP Channels

i.LON 600s allow you to connect an FT-10 or TP-1250 channel to a LONWORKS/IP channel for transporting LONWORKS packets over IP. Once the LONWORKS/IP channel is established (as described in the previous section), you must define the *i*.LON 600 devices using the LonMaker Integration Tool.

Figure 26 shows an example of a LONWORKS network that contains a LONWORKS/IP channel. Note that if you are running LonMaker version 3.0 or higher, your LonMaker PC can be a part of the LONWORKS/IP channel by connecting it to the Ethernet rather than an FT-10 channel.

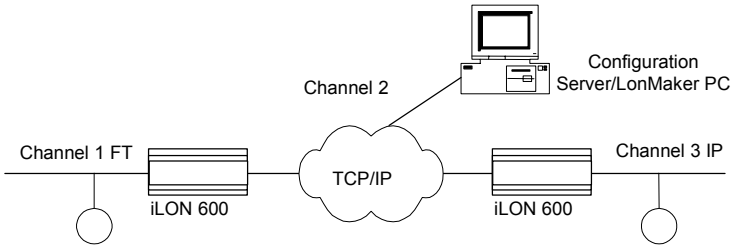


Figure 26. Typical Network Containing a LONWORKS/IP Channel

Defining an i.LON 600 as a LONWORKS Router

The following example illustrates how to create the LONWORKS network described in Figure 26 using the LonMaker Integration Tool. Figure 27 shows the LonMaker drawing created in this example. For more information, see the *LonMaker User's Guide*. To create a LonMaker network which uses *i*.LON 600s, follow these steps:

1. With the Configuration Server running, create a new LonMaker network. Change the name of *Channel 1* to *FT-10 Channel 1* and assign **TP/FT-10** as the transceiver type in the Channel's properties.

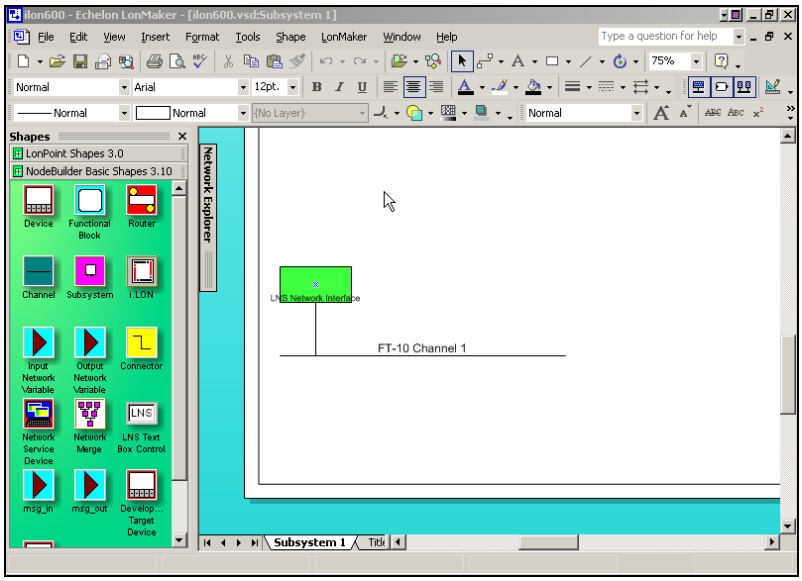


Figure 27. Creating a New Channel Using LonMaker

2. Drop channel shapes onto the drawing representing the *IP Channel* and *FT-10 Channel 2*. For the IP Channel, specify **IP-10L** (if using a local IP network) or **IP-10W** (if using a wide area IP network, such as the Internet) for the *Transceiver Type* in the Channel's properties. For *FT-10 Channel 2*, assign **TP/FT-10** as the *Transceiver Type*.
3. Drop two LONWORKS Router shapes onto the drawing, one connecting *FT-10 Channel 1* to *IP Channel* (*iLONRTR_1)* and one connecting *FT-10 Channel 2* (*iLONRTR_2)* to the IP channel. Follow the LonMaker convention: *Channel A* of a router is the side closest to the LNS Network Interface. *Channel A* of *iLONRTR_1* is attached to *FT-10 Channel 1* and *Channel B* is attached to *IP Channel*; *Channel A* of *iLONRTR_2* is attached to *IP Channel*, and *Channel B* is attached to *FT-10 Channel 2*.
4. Commission the *i*.LON 600 RTR_1 and *i*.LON 600 RTR_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 8.

Be sure the Configuration Server is running when you commission the *i*.LON 600 routers or make any other changes to your LONWORKS network, such as adding or deleting devices or connections.

Once the *i*.LON 600s 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 28 shows the network described above with a *DI-10 LonPoint* 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 connected to channel 3 (switch band to lamp).

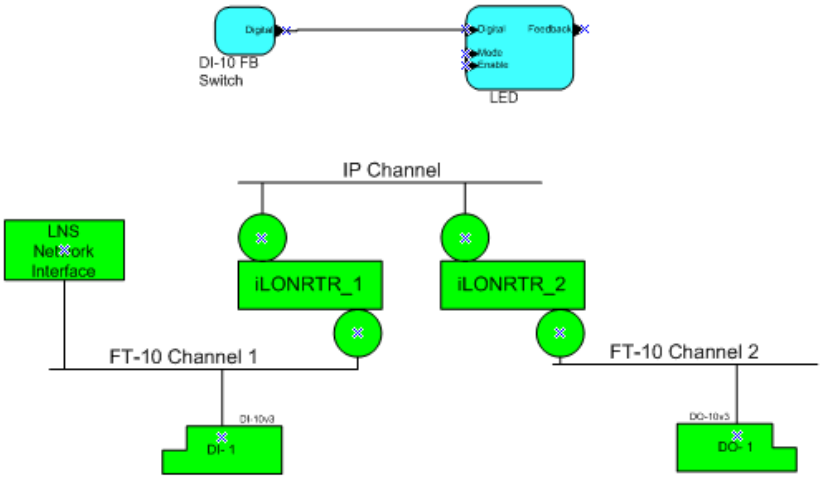


Figure 28. *i*.LON 600 Routers Configured on a LONWORKS Network

Verifying Router Functionality

To verify that the *i*.LON 600 Routers in the network shown in Figure 26 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 fail to see network variable updates reported by LonMaker, there is a problem. Refer to Table 9 for troubleshooting information.

Table 9. Troubleshooting the *i*.LON 600 Router

Symptom	***Probable Cause***	***Corrective Action***
No service pin message is received from the near router (*i*LONRTR_1 in Figure 27).	There is a problem with network connectivity, or the network interface in the PC may not be functioning properly.	Test connectivity between the network interface driver and the network interface card in the PC using the LONWORKS Plug and Play Control Panel applet that came with the network interface. Test to make sure the applet can receive a service pin message from some other node on the same channel as the *i*.LON.
	The *i*.LON 600 may not be physically connected to the network interface.	Check the network wiring between the PC and the *i*.LON 600.
	No IP address has been assigned to the *i*.LON 600.	Configure the IP address in the *i*.LON 600 using the setup web pages and the Configuration Server.
	The router application has not yet been created on the *i*.LON 600.	Create the LONWORKS router application using the Console Application.
	The VNI has not been added to the Configuration Server.	Add the VNI to the Configuration Server.
	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.
The near router (*i*LONRTR_1) commissions successfully, but no service pin message is received from the far router (*i*LONRTR_2).	There is a problem with the LONWORKS/IP channel setup.	Be sure the Configuration Server is running in the background when commissioning *i*.LON 600 routers. Verify that the near router is online and that the Configuration Server reports connectivity among all members of the LONWORKS/IP channel (e.g. all icons are green).
Both *i*.LON 600 routers commission successfully, but the device on the far side of *i*LONRTR_2 (the DI-10 LonPoint device) does not install correctly.	There is a problem with the LONWORKS/IP 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 LONWORKS/IP channel is working, and the improperly working device may not be installed correctly. If no test succeeds, verify connectivity between the *i*.LON 600 devices in the main dialog status window of the Configuration Server.
An *i*.LON 600 added to a LONWORKS/IP channel using the Configuration Server remains red in the device tree.	IP connectivity problem: the Configuration Server is not able to communicate with the *i*.LON 600 on the defined LONWORKS/IP channel.	Verify that the PC running the Configuration Server can ping the *i*.LON 600. To perform a ping, open the Windows Command Prompt (in the Accessories menu) and type “ping 10.2.11.XXX (the device’s IP address)”. You should receive a reply from your device. Examine the Configuration Server trace window for clues as to what may be going wrong.

		Verify that you can ping the Configuration Server PC or members of the LONWORKS/IP channel using the Windows Command Prompt.
The *i*.LON 600 on the LONWORKS/IP 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 *i*.LON 600 device, determined using the Console Application *show* command, matches the IP address defined for it in the Configuration Server. Determine if the router application exists by using the listapp command in the Console Application. Create the router app if it does not exist.

Section 2

Advanced Topics

6

Using the *i*.LON 600 with NAT

Network Address Translation (NAT)

Network Address Translation (NAT) allows multiple computers (hosts) to share one IP address. See Appendix A for a complete description of NAT.

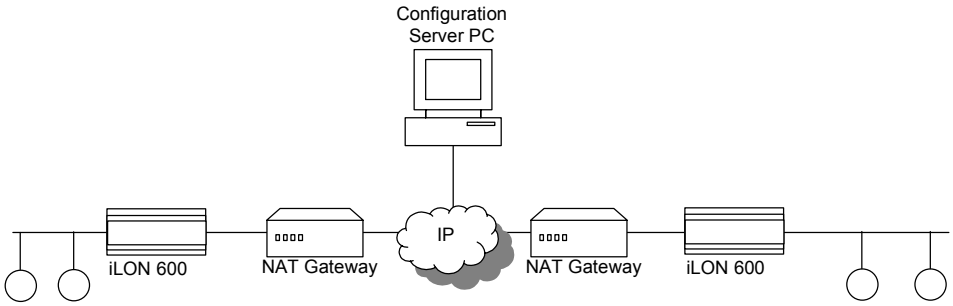


Figure 29. *i*.LON 600s Communicating Through Two NAT Gateways

An *i*.LON 600 may be placed behind an NAT firewall (such as the Linksys router Model BEFSR81DSL or equivalent) and can communicate with another *i*.LON 600 placed behind another NAT firewall. See Figure 29. The ports (by default 1628 and 1629) that the *i*.LON 600 uses to communicate with its peers and the Configuration Server must be opened, mapped, and properly forwarded. See your NAT firewall's user manual for details on how to setup port forwarding (sometimes called static port mapping) on your particular NAT firewall.

Once the ports are mapped on the NAT firewall, setting up a LONWORKS/IP channel is much like the procedure described in Chapter 5 with the exception that additional entries are added to the Configuration Server's device tree to indicate the NAT firewalls.

To setup a LONWORKS/IP channel that spans NAT firewalls, perform the following steps:

1. With the Configuration Server running, select **New NAT Firewall** from the **Channel** menu.
2. Enter a descriptive name for your NAT firewall and press Enter.
3. Double-click the new NAT firewall and enter the IP address of the NAT firewall.
4. Click on the new NAT firewall and select **New Device** from the **NAT Firewall** menu.
5. Double-click the new device and set the new device's IP address.
6. Repeat Steps 1 through 3 to add another NAT firewall and device. The Configuration Server should look like the one in Figure 30:

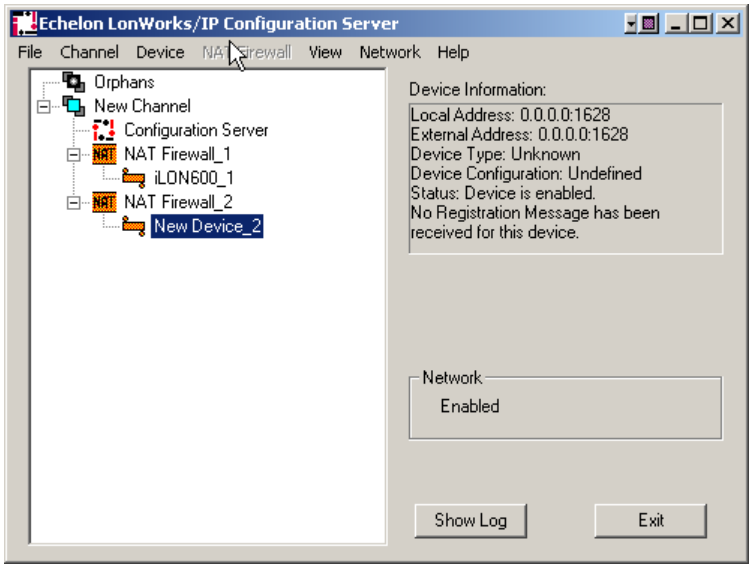


Figure 30. Setting Up Multiple Firewalls with Multiple *i*.LON 600s

7. Right click on the channel and select **Update Members** or right click on the device and select **Update Device**.

7

Using the *i*.LON 600 with DHCP & DNS

DHCP

DHCP (Dynamic Host Configuration Protocol) allows PCs to automatically be assigned an IP address when they are powered. The "DHCP Server" resides on the network and assigns IP addresses. When you select "Obtain IP address Automatically" in the Windows network setup screens, you are asking Windows to get its IP address from a local DHCP server. DHCP is commonly used for workstations, but seldom used for 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 is assigned address 100, computer 2 is assigned address 101, computer 3 is assigned address 102, etc. 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 a LONWORKS/IP channel). In a LONWORKS/IP channel, each device knows the addresses of other devices on the network. If those addresses change because a peer running as a DHCP client 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 Configuration Server, but the process is manual, which makes it impractical.

***Note*:** Echelon recommends that all members of a LONWORKS/IP channel be assigned static IP addresses.

If you are in control of your DHCP server, you may be able to configure your DHCP server to always assign your *i*.LONs the same 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 *i*.LON should be instructed to acquire its IP address from the DHCP server by selecting **Automatically obtain IP address** in the main TCP/IP Web setup screen.

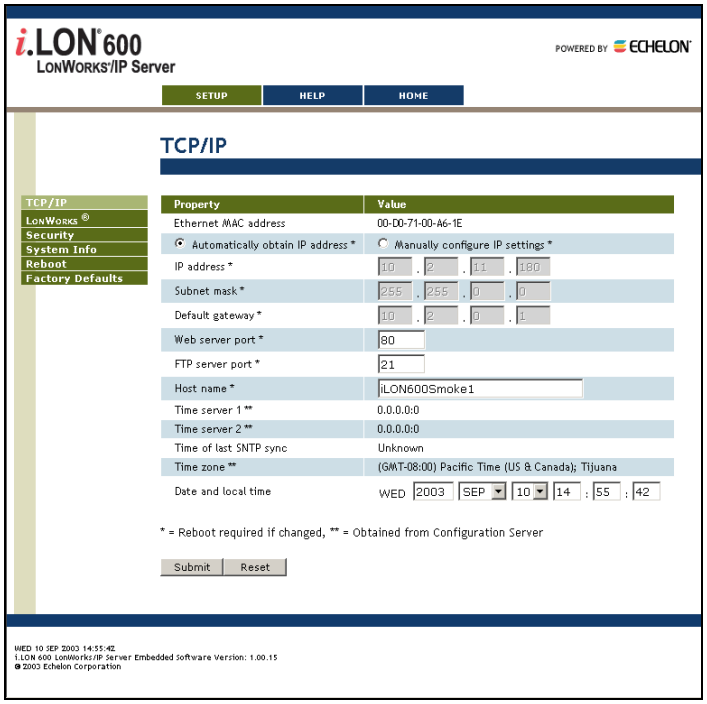


Figure 31. Automatically obtain IP address Setting

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.

Note that 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.

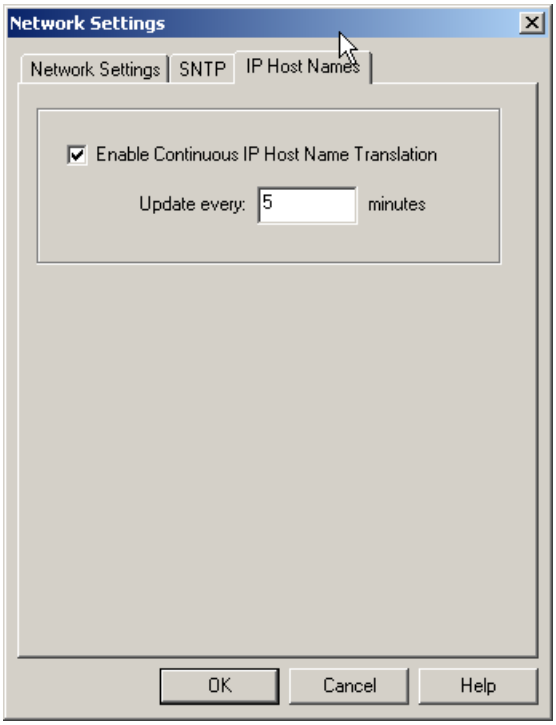
If you are in control of your local DNS server, you should give all participants in your LONWORKS/IP channel static IP addresses and create DNS entries for each participant. This allows you to specify an IP host name when setting up the LONWORKS/IP channel in the Configuration Server instead of numeric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

Note: The *i*.LON 600s themselves do not query DNS servers to resolve addresses, they only work with numeric IP addresses provided by the Configuration Server.

By default, the 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 Configuration Server is first started.

Follow the below steps to set the Configuration Server automatic IP host name address translation.

1. Select **Settings** from the **Network** menu in the Configuration Server and click on the **IP Host Names** tab shown below:



2. Check or uncheck the **Enable Continuous IP Host Names Translation** checkbox and specify an update interval time (if applicable).

To issue an immediate IP host name translation, select **Translate IP Host Names** from the **Network** menu. This will perform a retranslation on all channels.

Note: When using this option, the local DNS server and the Configuration Server must be continuously running.

Linking DNS and DHCP

If your LONWORKS/IP channel implementation is completely under your control, and you have control of all DHCP and DNS servers referenced by the members of your LONWORKS/IP channel, it is possible to assign all addresses using DHCP without static reservations and resolve members using DNS and the Configuration Server. Windows 2000 Server, for example, allows you to link DHCP and DNS records in this fashion.

Echelon does not recommend this method of configuring LONWORKS/IP channels.

See Appendix A or visit http://www.echelon.com/products/internet/ilon10howto/DHCPserver.pdf for more information on DHCP and DNS.

Note: The Configuration Server is an application that defines LONWORKS/IP channels and runs on a PC. The Configuration Server requires a single static IP address for all PCs running LNS (version 3.01 or later) that are connected in the LONWORKS/IP channel. If you leave the Configuration Server attached to the LONWORKS/IP channel, DNS resolvable addresses can be used. If the IP network links its DHCP server and DNS server (a Windows 2000 based server can do this), then *i*.LON 600s can be setup to use DHCP assigned addresses. However, the Configuration Server's ability to resolve addresses through DNS is limited. See the *DNS and the Echelon LONWORKS/IP Configuration Server* section in *Appendix A* for more information. DDNS may also be used with the same precautions.

The EIA-852 specification requires that devices on a LONWORKS/IP channel share IP addresses instead of DNS resolvable names. If an *i*.LON 600 in a channel is aware of a peer at 131.1.23.52, and that peer changes addresses, the *i*.LON will lose communication with the peer until it receives an updated peer list. The Configuration Server can solve this problem by sending out an updated list (using DNS) to all members on the channel. The *i*.LON can not resolve DNS address issues on its own.

- When exchanging messages with the Configuration Server and other devices on the LONWORKS/IP channel, the *i*.LON 600 protocol requires that each device's IP address remain static so it can identify other members of the LONWORKS/IP channel. See note above.

If DHCP will be used to retrieve the IP information for the *i*.LON 600, the network administrator must ensure that a DHCP server is available to provide the IP address, subnet mask, and gateway address. In addition, the network administrator should create individual static address reservations for each *i*.LON 600.

8

LONWORKS/IP Channel Parameters

Channel Mode

You can set the *i*.LON 600 channel mode using one of three radio buttons in the **New Channel Properties** dialog box. To access the **New Channel Properties** dialog box, start the Configuration Server and right click the New Channel icon and select **Channel Properties…** from the menu.

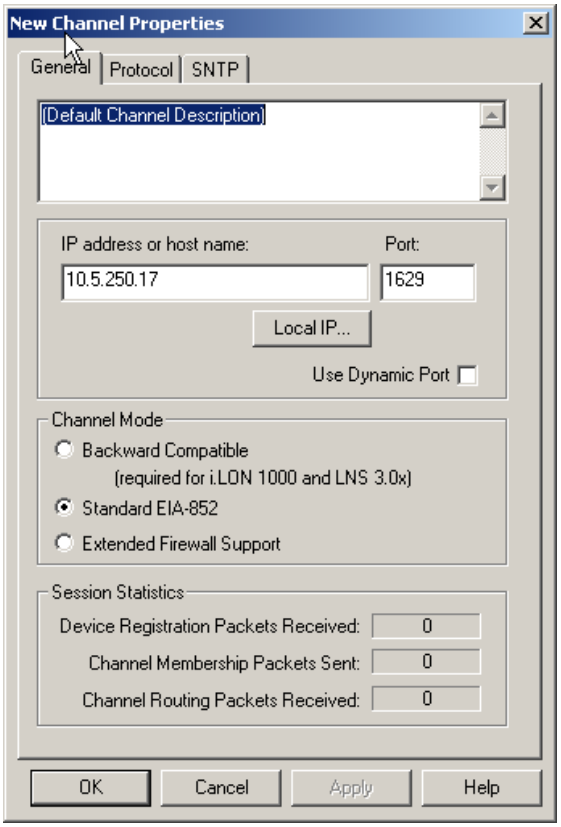


Figure 32. New Channel Properties Dialog Box

A brief description of each mode is described in Table 10.

Table 10. Channel Modes

Setting	*Description*
Backward Compatible (required for i.LON 1000 and LNS 3.0x)	You must enable this option if your channel will contain any i.LON 1000's or LNS 3.0x LONWORKS /IP interfaces. This causes the i.LON 600 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. You can only have one device located behind each NAT firewall. You cannot have duplicate IP addresses.
Standard EIA-852	Select this option when using a standard LONWORKS channel. You can use a maximum of 256 devices per channel in Standard EIA-852 mode. When using this mode, you can only have one device located behind each NAT firewall. You cannot have duplicate IP addresses.
Extended Firewall Support	This option is recommended whenever your LonWorks/IP channel crosses an IP firewall, whether or not 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 LonWorks/IP device behind an NAT firewall, and to

	create multiple LNS LonWorks/IP interfaces in the same channel using the same IP address (but with different ports). Without this option, 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 EIA-852 devices. You can use up to 256 devices per channel in this mode.

Aggregation

The *i*.LON 600 router aggregates LONWORKS packets for transporting over the IP channel. LONWORKS packets are relatively small in size and often arrive at the *i*.LON 600 router in bursts or at a high rate. Aggregating packets decreases the bandwidth necessary to send packets over IP, decreases IP network traffic, and greatly increases the performance of the *i*.LON 600 router.

The *i*.LON 600 router is set through the Configuration Server to use aggregation by default. The aggregation time parameter controls how long the router will wait for packets. The timer operates in multiples of 16.6 milliseconds and defaults to 16 milliseconds.

If the network is idle and a single LONWORKS packet arrives at the *i*.LON 600 router, 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. You can set the *i*.LON 600 aggregation time by double-clicking a selected channel or right clicking and selecting **Channel Properties** and selecting the **Protocol** tab.

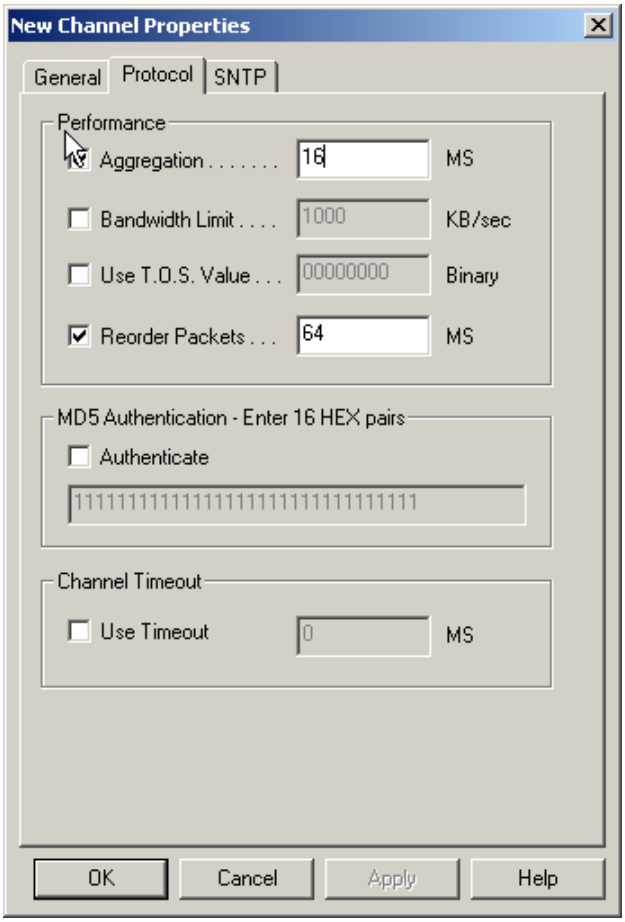


Figure 33. Aggregation Settings

MD5 Authentication

MD5 authentication is a channel-wide property that uses an authentication key to set security on a LONWORKS/IP channel. The authentication key is used to calculate the MD5 digest. When authentication is enabled and the *i.*LON 600 prepares to send an IP packet, the *i.*LON 600 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 APDU is identical to the packets described in the EIA-852 protocol standard for sending LONWORKS packets over IP. The computed digest is appended to the end of the APDU and the packet is sent over the network. Authentication digests are appended to both LONWORKS data packets and Configuration Server control packets. One or more *i.*LON 600 devices receive the packet and use their authentication key to compute a digest over the same payload (not including the appended digest). The receiving *i.*LON 600 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.

The authentication key, consisting of 16 HEX pairs, is set for each *i.*LON 600 through the Console Application or Web page. Authentication is enabled and the authentication key set for the LONWORKS/IP channel through the Configuration Server. To reset a lost authentication key, you must obtain physical access to the device and reset the key through the device's serial port or use the setup Web page.

To enable authentication and set the authentication key on a LONWORKS/IP channel, follow these steps:

1. Select **Channel Properties** from the Configuration Server's **Channel** menu or right-click on a channel and select **Channel Properties**. Click the **Protocol** tab.

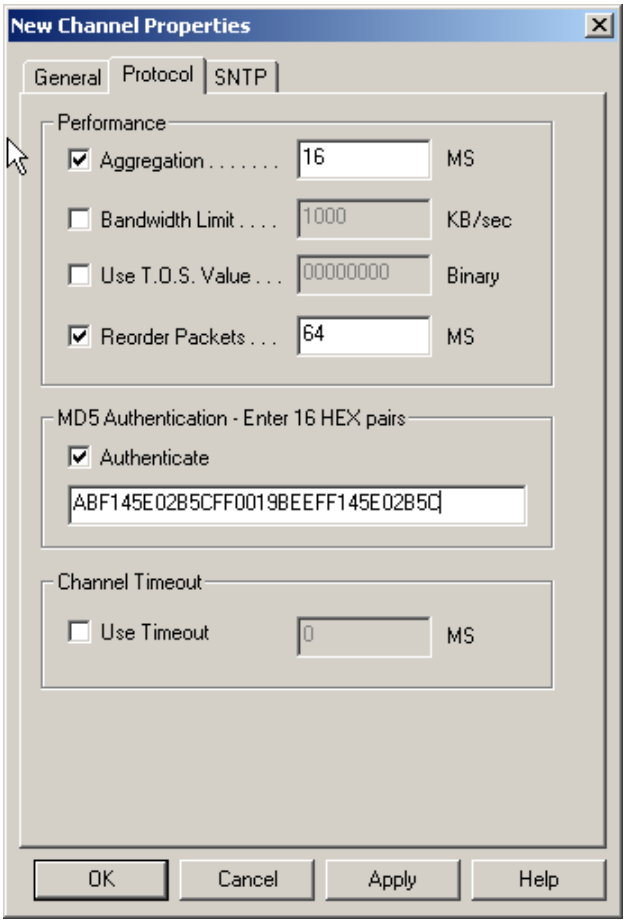


Figure 34. Protocol Tab

2. Select the **Authenticate** checkbox to enable authentication and enter 16 HEX pairs that represent the MD5 authentication key into the entry field.

For example: ABF145E02B5CFF0019BEEFF145E02B5C

3. All authentication keys within a single network must match. Be sure that you have previously entered the same authentication key on the *i*.LON 600 devices defined on this channel using the Console Application or setup Web page. See Figure 35. See Appendix B for more information on changing the authentication key using the Console Application.

Note: To disable authentication on a channel that has authentication enabled, deselect the **Authenticate** check box (shown in Figure 34) and click **Apply**.

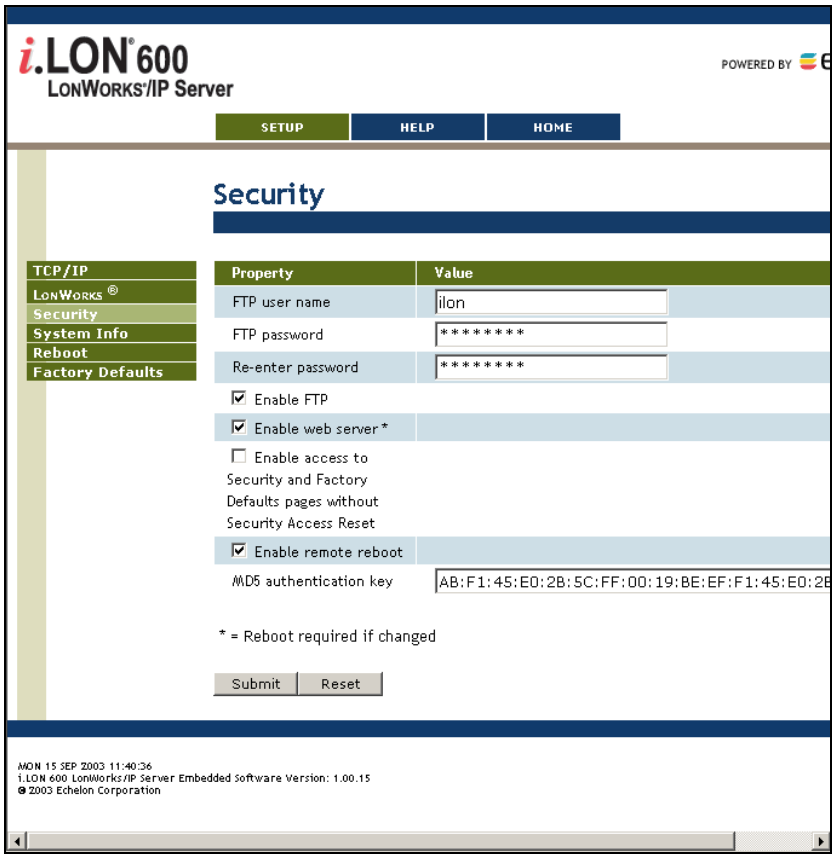


Figure 35. Setting MD5 Authentication

WARNING

MD5 authentication should not be confused with authenticated LONWORKS messaging. MD5 authentication applies to IP packets, authenticated LONWORKS messaging applies to LONWORKS packets.

i.LON 600 System Event Log

The *i*.LON 600 maintains a history of significant system events to track and help troubleshoot any problems that may occur during operation. These system events are logged to the event log, a text file stored in the *i*.LON 600's root directory (`/root/eventlog.txt`). System events are logged to the file when the `eventlog` command is enabled on the *i*.LON 600 through the Console Application. See Appendix B.

To view the event log file, first transfer the file to a PC using FTP, then use a text editor to view the file. If transferred as binary, it may not be readable from a text editor. You may also use the console command `type /root/eventlog.txt` to display it on the console.

Event Types

The event log records different types of event messages. Every event includes a date/time stamp and a message.

The following sections list the event types and include a description of the message.

`Fatal exception reboot; intvec#<vector>;pc:<address>`

A fatal exception has occurred. The event will be followed by a stack trace of the task that took the exception. The device will reboot after a fatal exception.

`Remotely initiated reboot request received`

The Configuration Server sent a remote boot request.

`**********System started***********`

The system started after a reboot. Tracking this event is useful in the case where the system reboots for reasons other than those logged as events. For example, this event could be due to a power cycle or certain program faults.

`******Boot failed/interrupted******`

The bootrom failed to load the system image and entered the bootrom console. The bootrom will also log events to the event log.

`Console command: command line`

A modifying console command was issued through the Console Application. Console commands that affect the state of the machine are tracked as events. For security reasons, the following commands do not log their parameters: `ftpuser`, `ftppassword`, and `authkey`.

`<urgent trace>`

An urgent trace message was generated. The urgent trace messages include:

Table 11. Urgent Trace Messages

Message	*Description*
WebServer Activated/Deactivated (remotely)	Indicates that the WebServer state was changed remotely using the Configuration Server.
NVRAM reset to factory defaults	The NVRAM contents have been reset to the factory default settings.
Web server is unable to open WebParams.dat	The Web server program could not open the WebParams.dat file. Ensure a copy of the file is available.
Time Synchronization disabled, no server	Time synchronization was lost because there are no longer any configured time servers. This will not be logged when the system is first starting.
Time Synchronization failed, server: <address>	Time synchronization was lost because time server at the indicated IP address failed to respond within two seconds. If there is more than one time server configured, resynchronization will be automatically attempted with a different server.
Time Synchronization established, server: <address>	Time synchronization was established with the time server at the indicated IP address. This will not be logged when the system is first starting.
Router: persistent data lost due to <reason> or Suggested action: recommission the router or application instance.	A configuration image or node definition image was lost. This forced the application instance or router to an unconfigured state. It must be commissioned via a LONWORKS network management tool. The reason for the loss is one of the following: “an image corruption” – The image file located in /root/ltConfig was corrupted. “a program ID change" - This might occur when changing the application mix "a signature mismatch" - The image file was corrupted. "a reset or power cycle while updating persistent data" - During or shortly after a LONWORKS network management update, the device was reset.
Persistence Update Failure: File system write error.	The system was unable to write a persistence file for an application or router. The file system could be out of space or corrupted. Verify the amount of free space remaining by running the chkdsk command in the Console Application and then deleting any unused files.
Router Persistence: Unable to write persistent data block.	The system was unable to write a persistence file for an application or router stack. The file system could be out of space or corrupted. Verify the amount of free space remaining by running the chkdsk command in the Console Application and then deleting any unused files.
Router Persistence - discarded due to local IP address change. IP address is x.x.x.x was x.x.x.x	The IP address of the *i*.LON 600 server has changed. This is expected after the IP address has been changed and the server rebooted. The server must be reconfigured with the Configuration Server. The LONWORKS parameters are preserved in this case.
Router - Unable to restart link to Configuration Server.	Communication has been lost with the Configuration Server. Ping the Configuration Server from the *i*.LON 600 using the ping command from the Console Application. If the ping succeeds, verify the necessary ports are open.
Startup - Server start failed	An unforeseen error has prevented a proper startup. Consider setting "factory defaults" through the Console Application or setup web page. This applies only when using VNI.
LONWORKS channel priority lowered to <n> due to transceiver swap.	Unit running with one transceiver type was rebooted with a new transceiver type. The priority slot configured for the old type exceeded the maximum for the new type. Recommend that a new priority slot be assigned, using a LONWORKS network management tool. This applies only when using VNI.

LONWORKS/IP Channel Timing Considerations

When designing a LONWORKS/IP channel over an IP network that might have a large latency, such as the Internet, it is important to be aware of the relationship between the three timing parameters that can be set when configuring the channel. Two of the timing parameters, *Channel Timeout* and *Packet Reorder Timer*, are set for the LONWORKS/IP channel through the Configuration Server. *Channel Delay* is set through an LNS based tool such as the LonMaker tool.

On local area networks, **Channel Timeout** is required only if MD5 Authentication is used. **Packet Reorder Timer** should be disabled on a LAN, and the LonMaker **Channel Delay** for the channel should be set to twice the aggregation timer.

On networks using the Internet, **Channel Timeout** and **Packet Reorder Timer** must consider the value of the LonMaker **Channel Delay** parameter. Table 12 specifies how to approximate the timing values for network implementations using the Internet.

Table 12. Timing Parameter Calculations for Internet LONWORKS/IP 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: ¼ of Channel Timeout Value, or 64 MS
LonMaker Channel Delay	Average Ping Delay + 10%

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

Use the ping command from a DOS window to obtain the average ping delay. Do not use the ping command in the *i*.LON 600 Console Application.

Channel Timeout

Channel Timeout is the LONWORKS/IP channel property that assigns a delay for a packet to travel across that channel. The assigned delay is a time parameter set in milliseconds and 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 response. Synchronize the *i*.LON 600 routers with an SNTP time server.

Set the Channel Timeout parameter to a value in relation with the ping delay specified in Table 12. In a LONWORKS network, each channel is assigned a *cost* defined as the round trip delay for a packet traveling across that channel. Channel Delay is based on a combination of bit rate, packet size, and media access. Generally, you should set Channel Timeout on your LONWORKS/IP channel to more than half the Channel Delay value.

Channel Timeout is **highly recommended** when using MD5 authentication. When using MD5 authentication, set it to 100 MS and the Channel Delay to 200 MS.

Factors in determining Channel Timeout include:

- *Variations on each leg of a round trip*. Your timeout parameter should factor the maximum delay into one leg of the trip.
- *Maximum difference between the times on the LONWORKS/IP devices*. The LONWORKS/IP device stamps its time on a packet when it is sent on the IP network and the target LONWORKS/IP 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 Configuration Server log window log when you run the channel Time Check command.

Packet Reorder Timer

Packet Reorder Timer is a LONWORKS/IP channel property that allows you to set the amount of time that the device will wait for an out-of-order IP packet to arrive. This parameter is important for wide area networks 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 value defaults to 64 milliseconds.

Packets on a local area network do not get out-of-order, so you should not set the reorder packets parameter 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.

Channel Delay

Channel Delay is an LNS property that specifies the value of the expected round trip time of a message (i.e. message and response). This allows expected traffic patterns to be input to the system so that the timer calculations can be affected accordingly. This property can be set using an LNS based tool such as LonMaker. See the LNS and LonMaker documentation for more information on the Channel Delay property.

Using SNTP When Creating LONWORKS/IP Channels

In small IP networks where there is no appreciable latency, it is not necessary to specify an SNTP server for your LONWORKS/IP channel.

However, when creating LONWORKS/IP channels that span large IP networks, like the Internet, where large network delays may be present, you must specify an SNTP time server for the LONWORKS/IP channel. Specifying a time server 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 Configuration Server, select **Settings** from the **Network** menu and click on the **SNTP** tab as shown in Figure 36.

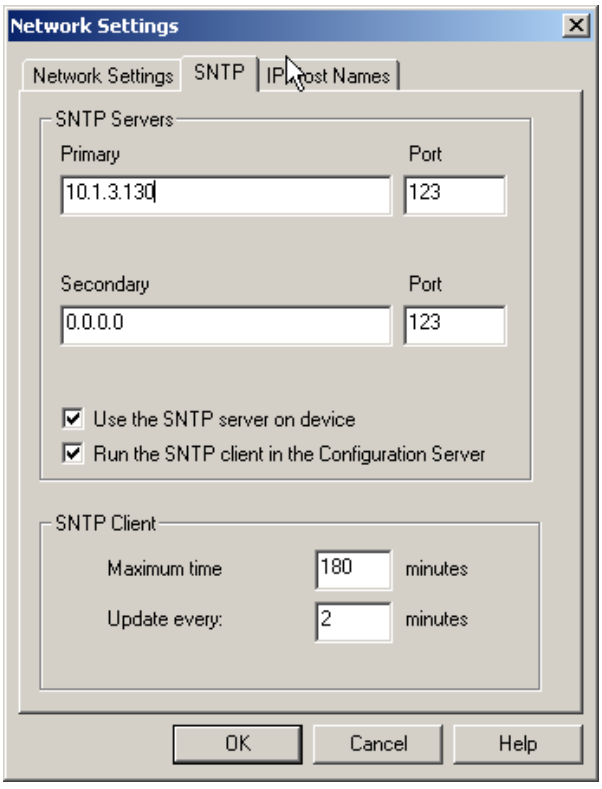


Figure 36. Setting the System SNTP Server

2. Enter the IP addresses or host names of the SNTP servers. Note that the SNTP server IP addresses should be static. Leave the default port numbers of 123. Ensure that the **Use the SNTP server on device** and the **Run the SNTP client in the Configuration Server** checkboxes are checked. The **Use the SNTP server on device** checkbox allows you to specify the default SNTP system server. The **Run the**

SNTP client in the Configuration Server checkbox allows you to run an SNTP client in the Configuration Server. If you are using a third-party SNTP server client on the Configuration Server PC, read the below section before setting your system. The SNTP Client options **Maximum time correction** and **Update every** only apply if the **Run the SNTP client in the Configuration checkbox** is checked. The *i*.LON 600 device SNTP options are self-adjusting and cannot be configured.

3. 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 (i.e. the System SNTP Server if the Channel SNTP server is not changed). Each channel and device in the network may 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 Configuration Server and right-click and select **Properties** or double-click the desired channel or device. Click on the **SNTP** tab.
2. Clear the **Use System Default** or **Use Channel Default** option and enter the IP addresses or host names of the SNTP servers as shown in Figure 37. Leave the default port numbers of 123.

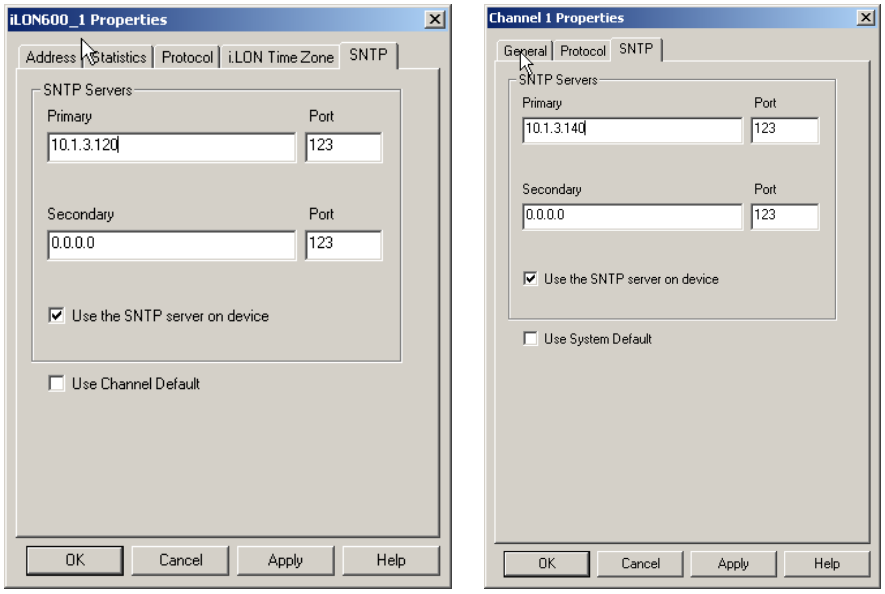


Figure 37. SNTP Server Configuration for a Device and Channel

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

Using a Third-Party SNTP Client on the Configuration Server PC

When the Configuration Server PC is already setup to run a third-party SNTP client, the Configuration Server's system SNTP settings must be set accordingly. The third-party SNTP client will synchronize the PC's clock; therefore, SNTP client should *not* be run in the Configuration Server. Doing so would cause the PC's clock to be synchronized to two SNTP servers—an undesired effect. The Configuration Server's system level SNTP setting is no longer tied with running an SNTP client in the Configuration Server.

Follow these steps to configure the Configuration Server to use a third-party SNTP client to update the PC's clock.

1. Select **Settings** from the **Network** menu and click on the **SNTP** tab.
2. Uncheck the **"Run the SNTP client in the Configuration Server"** checkbox. When cleared, the Configuration Server will not poll a SNTP server to update the PC's clock. The PC will use its third-party SNTP client to synchronize to whatever time server is specified by the third-party client.

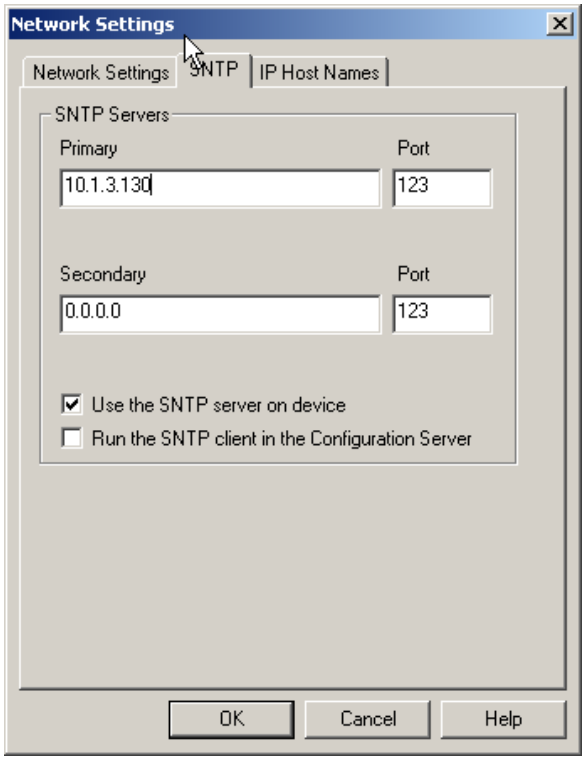


Figure 38. Run the SNTP client in the Configuration Server Checkbox.

3. 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 LONWORKS/IP 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. Available public access servers include:

Table 13. Available Public Access Servers

Site Name	*Site Address*
Ntp.css.gov	148.162.8.3
canon.inria.fr	192.93.2.20

For more information on time and frequency services, log on to www.eecis.udel.edu/~mills/ntp/

- Install an SNTP server on any PC in your LAN. You may use the same PC on which the Configuration Server is installed. One option is Tardis2000 shareware available from www.kaska.demon.co.uk. You can configure the software to synchronize with any other SNTP server, or use local time on the PC by setting Tardis2000 to use the loop back address 127.0.0.1.

9

Using XML to Directly Configure an *i*.LON 600

This section describes how to configure an i.LON 600 using an XML file as the source of the *i*.LON 600 configuration parameters.

Introduction

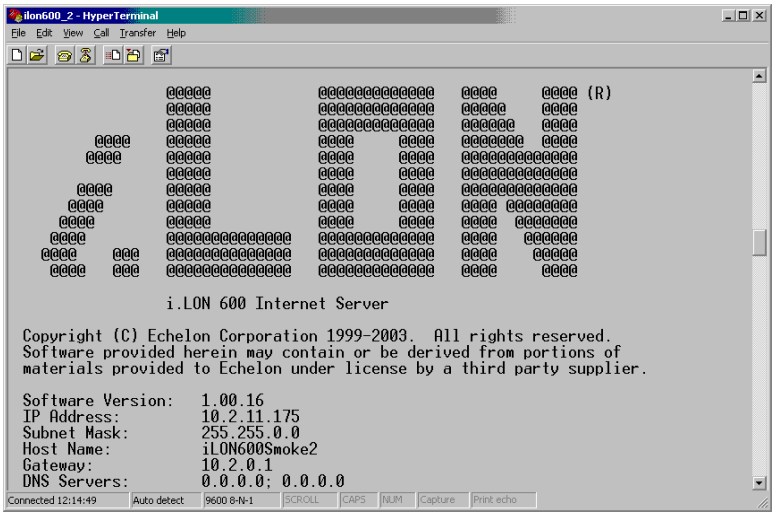
The EIA-852 standard requires that an i.LON 600 devices have a free-standing method of configuration. You can manually configure your *i*.LON 600 without using the Configuration Server software by uploading an XML file (containing configuration data) directly to your i.LON 600.

Echelon recommends using the Configuration Server to setup and specify parameters for your *i*.LON 600. Changes made to your network using a network management tool (such as LonMaker) could invalidate the XML setup file.

Creating and Uploading an XML Configuration File

To create an XML-based configuration file for you i.LON 600, perform the following steps:

1. Connect the console port to your PC (see Chapter 2) and run the console application.



2. Type the command `dump lwipconfig`. This will generate an XML file containing the current LONWORKS/IP configuration of the i.LON 600 called LTIP_Config.xml. The file is located in the /ItConfig/XmlDump directory on the *i*.LON 600.
3. Use FTP to upload the file to your PC.
4. Modify the appropriate XML file fields (such as `<LOCAL_PORT>`, `<CONFIG_SERVER_IP_ADDR>`, and `<CONFIG_SERVER_PORT>`) using a text editor.
5. Using an FTP software program, download the LTIP_Config.xml file to the *i*.LON 600's /ItConfig directory. Note: you may not be able to drag and drop the file directly to the i.LON 600 file folder. If this fails, download the file using the Windows command line FTP client.
6. Reboot your *i*.LON 600 for the changes to take effect. Upon startup, the *i*.LON 600 will use the configuration parameters specified in the XML file.

Sample XML File

Below is an example of an XML file used for configuring the *i*.LON 600.

```
  <?xml version="1.0" encoding="utf-8" ?>
- <LONWORKS_IP_CONFIG>
  <XML_VERSION_MAJOR>1</XML_VERSION_MAJOR>
  <XML_VERSION_MINOR>1</XML_VERSION_MINOR>
  <TIMESTAMP>4008636142</TIMESTAMP>
  <DEVICE_NAME>ICE iLON</DEVICE_NAME>
  <LOCAL_IP_ADDR>10.2.11.153</LOCAL_IP_ADDR>
  <LOCAL_PORT>1628</LOCAL_PORT>
  <CONFIG_SERVER_IP_ADDR>10.2.0.52</CONFIG_SERVER_IP_ADDR>
  <CONFIG_SERVER_PORT>4501</CONFIG_SERVER_PORT>
  <TIME_SERVER1_IP_ADDR>10.2.1.99</TIME_SERVER1_IP_ADDR>
  <TIME_SERVER2_IP_ADDR>0.0.0.0</TIME_SERVER2_IP_ADDR>
  <TIME_SERVER1_PORT>123</TIME_SERVER1_PORT>
  <TIME_SERVER2_PORT>123</TIME_SERVER2_PORT>
  <BANDWIDTH_LIMIT_ENABLED>0</BANDWIDTH_LIMIT_ENABLED>
  <BANDWIDTH_LIMIT_VALUE>1000</BANDWIDTH_LIMIT_VALUE>
  <AGGREGATION_ENABLED>0</AGGREGATION_ENABLED>
  <AGGREGATION_VALUE>64</AGGREGATION_VALUE>
  <CHECK_STALE_PKTS_ENABLED>1</CHECK_STALE_PKTS_ENABLED>
  <CHANNEL_TIMEOUT>0</CHANNEL_TIMEOUT>
  <REORDER_PKTS_ENABLED>1</REORDER_PKTS_ENABLED>
  <REORDER_ESCROW_TIMER>200</REORDER_ESCROW_TIMER>
  <TYPE_OF_SERVICE_ENABLED>0</TYPE_OF_SERVICE_ENABLED>
  <TYPE_OF_SERVICE_VALUE>0</TYPE_OF_SERVICE_VALUE>
  <AUTHENTICATION_ENABLED>1</AUTHENTICATION_ENABLED>

<AUTHENTICATION_SECRET>00000000000000000000000000000000</AUTHENTICATION_SE
CRET>
  <ECHELON_PROTO_VERSION>1</ECHELON_PROTO_VERSION>
  <STRICT_EIA852_ENABLED>1</STRICT_EIA852_ENABLED>
  <HAS_SHARED_IP_ADDRS>0</HAS_SHARED_IP_ADDRS>
  <NAT_IP_ADDR>0.0.0.0</NAT_IP_ADDR>
- <DEVICE_CONFIG_INFO>
  <TIMESTAMP>3272745043</TIMESTAMP>
  <LTIP_PROTO_FLAGS>1</LTIP_PROTO_FLAGS>
  <CN_ROUTER_TYPE>0</CN_ROUTER_TYPE>
  <CN_FLAGS>0</CN_FLAGS>
  <CN_NODE_TYPE>1</CN_NODE_TYPE>
  <CHAN_MEMB_TIMESTAMP>3272745039</CHAN_MEMB_TIMESTAMP>
  <SEND_LIST_TIMESTAMP>0</SEND_LIST_TIMESTAMP>
  <NEURON_ID_BYTES>6</NEURON_ID_BYTES>
  <CHANNEL_TIMEOUT>0</CHANNEL_TIMEOUT>
  <UCAST_PORT>1628</UCAST_PORT>
  <UCAST_IP_ADDR>10.2.11.153</UCAST_IP_ADDR>
  <CONFIG_SERVER_IP_ADDR>10.2.0.52</CONFIG_SERVER_IP_ADDR>
  <TIME_SERVER1_IP_ADDR>10.2.1.99</TIME_SERVER1_IP_ADDR>
  <TIME_SERVER2_IP_ADDR>0.0.0.0</TIME_SERVER2_IP_ADDR>
  <CONFIG_SERVER_PORT>4501</CONFIG_SERVER_PORT>
  <TIME_SERVER1_PORT>123</TIME_SERVER1_PORT>
  <TIME_SERVER2_PORT>123</TIME_SERVER2_PORT>
  <MCAST_ELEMENTS />
- <NEURON_IDS>
  <NEURON_ID>800000001AA1</NEURON_ID>
  </NEURON_IDS>
  </DEVICE_CONFIG_INFO>
- <CHAN_MEMB_INFO>
  <TIMESTAMP>3272745039</TIMESTAMP>
  <SEND_LIST_TIMESTAMP>3272745039</SEND_LIST_TIMESTAMP>
- <MEMBER_ELEMENTS>
- <MEMB_ELEMENT>
  <IP_ADDRESS>10.2.11.151</IP_ADDRESS>
  <IP_PORT>1630</IP_PORT>
  <TIMESTAMP>3264270798</TIMESTAMP>
  </MEMB_ELEMENT>
- <MEMB_ELEMENT>
  <IP_ADDRESS>10.2.11.52</IP_ADDRESS>
  <IP_PORT>10002</IP_PORT>
  <TIMESTAMP>3272743940</TIMESTAMP>
  </MEMB_ELEMENT>
- <MEMB_ELEMENT>
  <IP_ADDRESS>10.2.11.153</IP_ADDRESS>
  <IP_PORT>1628</IP_PORT>
  <TIMESTAMP>3272727405</TIMESTAMP>
  </MEMB_ELEMENT>
```

```
  </MEMBER_ELEMENTS>
  </CHAN_MEMB_INFO>
- <CHANNEL_ROUTING_INFOS>
- <CHANNEL_RTNG_INFO>
  <TIMESTAMP>3264270798</TIMESTAMP>
  <MCAST_IP_ADDR>0.0.0.0</MCAST_IP_ADDR>
  <MCAST_PORT>0</MCAST_PORT>
  <UCAST_IP_ADDR>10.2.11.151</UCAST_IP_ADDR>
  <UCAST_PORT>1630</UCAST_PORT>
  <LTIP_PROTO_FLAGS>0</LTIP_PROTO_FLAGS>
  <CN_ROUTER_TYPE>0</CN_ROUTER_TYPE>
  <CN_FLAGS>1</CN_FLAGS>
  <CN_NODE_TYPE>0</CN_NODE_TYPE>
- <NEURON_IDS>
  <NEURON_ID>080000001B01</NEURON_ID>
  </NEURON_IDS>
- <CN_NODE_ADDRS>
- <CN_NODE_ADDR>
  <SUBNET_ID>2</SUBNET_ID>
  <NODE_ID>4</NODE_ID>
  <DOMAIN_ID_INDEX>0</DOMAIN_ID_INDEX>
  <NEURON_ID_INDEX>0</NEURON_ID_INDEX>
  </CN_NODE_ADDR>
  </CN_NODE_ADDRS>
- <CN_DOMAINS>
- <CN_DOMAIN>

<SUBNET_MASK>40000000000000000000000000000000000000000000000000000000000000
000</SUBNET_MASK>

<GROUP_MASK>00000000000000000000000000000000000000000000000000000000000000
00</GROUP_MASK>
  <DOMAIN_ID>9B</DOMAIN_ID>
  <LENGTH>1</LENGTH>
  </CN_DOMAIN>
  </CN_DOMAINS>
  </CHANNEL_RTNG_INFO>
- <CHANNEL_RTNG_INFO>
  <TIMESTAMP>3272743940</TIMESTAMP>
  <MCAST_IP_ADDR>0.0.0.0</MCAST_IP_ADDR>
  <MCAST_PORT>0</MCAST_PORT>
  <UCAST_IP_ADDR>10.2.11.52</UCAST_IP_ADDR>
  <UCAST_PORT>10002</UCAST_PORT>
  <LTIP_PROTO_FLAGS>1</LTIP_PROTO_FLAGS>
  <CN_ROUTER_TYPE>0</CN_ROUTER_TYPE>
  <CN_FLAGS>1</CN_FLAGS>
  <CN_NODE_TYPE>0</CN_NODE_TYPE>
- <NEURON_IDS>
  <NEURON_ID>FEDC3EF2FB65</NEURON_ID>
  </NEURON_IDS>
- <CN_NODE_ADDRS>
- <CN_NODE_ADDR>
  <SUBNET_ID>1</SUBNET_ID>
  <NODE_ID>127</NODE_ID>
  <DOMAIN_ID_INDEX>0</DOMAIN_ID_INDEX>
  <NEURON_ID_INDEX>0</NEURON_ID_INDEX>
  </CN_NODE_ADDR>
- <CN_NODE_ADDR>
  <SUBNET_ID>1</SUBNET_ID>
  <NODE_ID>126</NODE_ID>
  <DOMAIN_ID_INDEX>0</DOMAIN_ID_INDEX>
  <NEURON_ID_INDEX>0</NEURON_ID_INDEX>
  </CN_NODE_ADDR>
  </CN_NODE_ADDRS>
- <CN_DOMAINS>
- <CN_DOMAIN>

<SUBNET_MASK>00000000000000000000000000000000000000000000000000000000000000
000</SUBNET_MASK>

<GROUP_MASK>00000000000000000000000000000000000000000000000000000000000000
00</GROUP_MASK>
  <DOMAIN_ID>57</DOMAIN_ID>
  <LENGTH>1</LENGTH>
  </CN_DOMAIN>
  </CN_DOMAINS>
  </CHANNEL_RTNG_INFO>
- <CHANNEL_RTNG_INFO>
  <TIMESTAMP>3272727405</TIMESTAMP>
  <MCAST_IP_ADDR>0.0.0.0</MCAST_IP_ADDR>
```

```
  <MCAST_PORT>0</MCAST_PORT>
  <UCAST_IP_ADDR>10.2.11.153</UCAST_IP_ADDR>
  <UCAST_PORT>1628</UCAST_PORT>
  <LTIP_PROTO_FLAGS>0</LTIP_PROTO_FLAGS>
  <CN_ROUTER_TYPE>0</CN_ROUTER_TYPE>
  <CN_FLAGS>1</CN_FLAGS>
  <CN_NODE_TYPE>0</CN_NODE_TYPE>
- <NEURON_IDS>
  <NEURON_ID>800000001AA1</NEURON_ID>
  </NEURON_IDS>
- <CN_NODE_ADDRS>
- <CN_NODE_ADDR>
  <SUBNET_ID>2</SUBNET_ID>
  <NODE_ID>1</NODE_ID>
  <DOMAIN_ID_INDEX>0</DOMAIN_ID_INDEX>
  <NEURON_ID_INDEX>0</NEURON_ID_INDEX>
  </CN_NODE_ADDR>
  </CN_NODE_ADDRS>
- <CN_DOMAINS>
- <CN_DOMAIN>

<SUBNET_MASK>A3B3FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFF</SUBNET_MASK>

<GROUP_MASK>FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FF</GROUP_MASK>
  <DOMAIN_ID>9B</DOMAIN_ID>
  <LENGTH>1</LENGTH>
  </CN_DOMAIN>
  </CN_DOMAINS>
  </CHANNEL_RTNG_INFO>
  </CHANNEL_ROUTING_INFOS>
  </LONWORKS_IP_CONFIG>
```

Echelon XML Tag Description

A few of the Echelon XML tags are described in Table 14.

Table 14. XML Tag Description

Header	***Description***
TIMESTAMP CHAN_MEMB_TIMESTAMP CHAN_RTNG_TIMESTAMP SEND_LIST_TIMESTAMP	These properties show the date and time of the last updated. The ISO time string is read and converted internally into a ULONG (4-byte unsigned integer) and stored in memory in milliseconds counting from January 1, 1900. The default setting is the current date and time.
DEVICE_NAME	Shows the name of the *i*.LON 600. This field is read only.
LOCAL_IP_ADDR	Specifies the *i*.LON 600 router local IP address. It is in IPv4 dotted decimal with null terminated string. This field is read only.
LOCAL_PORT	Specifies the *i*.LON 600 router local IP port.
CONFIG_SERVER_IP_ADDR	Specifies the Configuration Server IP address. It is in IPv4 dotted decimal with null terminated string.
CONFIG_SERVER_PORT	Specifies the Configuration Server IP port.
TIME_SERVER1_IP_ADDR TIME_SERVER2_IP_ADDR	Specifies the primary or alternate SNTP time server IP address. It is in IPv4 dotted decimal with null terminated string.
TIME_SERVER1_PORT TIME_SERVER2_PORT	Specifies the primary or alternate SNTP time server IP port.
BANDWIDTH_LIMIT_ENABLED	Specifies whether or not bandwidth limit setting is used/enabled. Boolean value can be either 1 (true) or 0 (false).
BANDWIDTH_LIMIT_VALUE	Specifies the data limit, in kilobytes per second, that the device will transmit on the IP channel to another device. If selected, the default is 1000 KB per second.
AGGREGATION_ENABLED	Specifies whether or not LonTalk packets aggregation is used/enabled. Boolean value can be either 1 (true) or 0 (false).
AGGREGATION_VALUE	Specifies the amount of time in milliseconds that the device will wait to aggregate LonTalk packets before sending them on the IP channel.
CHECK_STALE_PKTS_ENABLED	Specifies whether or not LonTalk packets are checked against their time limit specified in the channel timeout value. Boolean value can be either 1 (true) or 0 (false).
CHANNEL_TIMEOUT	Specifies the time limit in milliseconds for a single packet to arrive at its destination. Set Timeout if you are sending packets across a virtual private network or any configuration that uses the Internet.
AUTHENTICATION_ENABLED	Specifies whether or not MD5 authentication is used on a LonWorks IP channel. Boolean value can be either 1 (true) or 0 (false).
AUTHENTICATION_SECRET	Specifies the authentication key to set security on a LONWORKS/IP channel. Default is zero.
REORDER_PKTS_ENABLED	Specifies whether or not the device should wait for an out-of-order packet. Boolean value can be either 1(true) or 0 (false).

REORDER_ESCROW_TIMER	Specifies the time limit in milliseconds that the device will wait for an out-of-order packet to arrive.
TYPE_OF_SERVICE_ENABLED	Specifies whether or not the type of service byte in the IP packet for all TCP/IP messages sent by the device is used/enabled. Boolean value can be either 1(true) or 0 (false).
TYPE_OF_SERVICE_VALUE	Specifies the value to use for the type of service byte in the IP packet for all TCP/IP messages sent by the device. The value must be in 1 or 0 for each of the 8 bits.
ECHELON_PROTO_VERSION	Specifies the version of the Echelon device. The value is 1 for the i.LON 1000 and LNS VNI 3.01. Otherwise, the value sets to 2.
STRICT_EIA852_ENABLED	Specifies whether or not it uses the "Standard EIA-852" channel. Boolean value can be either 1 (true) or 0 (false).
HAS_SHARED_IP_ADDRS	Specifies whether or not the device has shared the IP address with other devices. Boolean value can be either 1 (true) or 0 (false).
NAT_IP_ADDR	Specifies the NAT firewall IP address if the *i*.LON 600 resides behind the NAT firewall. It is in IPv4 dotted decimal with null terminated string.

You can find non-Echelon specific XML tags in the EIA-852 specification.

10

Troubleshooting

This appendix can be used to diagnose common problems that occur with the *i*.LON 600.

Common Troubleshooting Problems

The following lists the most common problems encountered when setting up your *i*.LON 600.

Disabled *i*.LON 600s will not configure properly when the Configuration Server is taken off the network (turned off or disconnected). If you reattached the Configuration Server and select Update Members, the *i*.LON 600 is still not configured properly.

- To solve this problem, you must disable your *i*.LON 600 while the Configuration Server is still attached to your network.

If a pre-existing *i*.Lon 1000 installation is uninstalled after installing the *i*.Lon 600, the Configuration Server and supporting files are removed.

- To repair the *i*.LON 600 software installation, follow these steps:
    1. Select **Add/Remove** programs from the **Windows Control Panel**.
    2. Select the Echelon i.LON 600 software from the Currently Installed programs list and click **Change**.
    3. Select the **Repair** option in the Program Maintenance dialog box.

***i*.LON 600 LEDs Do not turn green.**

- This is usually an indication that the Configuration Server cannot communicate with an i.LON 600 on the network. Verify that the NAT gateways are properly setup to forward ports 1628 & 1629 if NAT is used.

I cannot view an *i*.LON 600's setup page.

- *i*.LON 600s have a built-in web server used for setup that communicates on port 80 by default. If you want to access the *i*.LON from outside your NAT gateway, be sure that the NAT gateway is configured to forward port 80 to your *i*.LON 600. A routing problem may exist. Use ping to verify the IP settings.

PCs using DHCP cannot communicate with an *i*.LON 600 using Ethernet direct connect.

- Communication with the *i*.LON 600 may be lost if you use DHCP and direct connect (using an Ethernet cable) and then unplug the *i*.LON 600. When you plug the Ethernet cable back into the *i*.LON 600, Windows communicates with the DHCP server and searches for an IP address. This action will fail. To solve this problem, assign your *i*.LON 600 a static IP address to make any configuration changes. Enable DHCP before re-installing the *i*.LON 600 onto your network.

I cannot access an *i*.LON 600 with FTP.

- *i*.LON 600s have a built-in FTP server that communicates on port 21 by default. If you want to access the *i*.LON using FTP from outside your NAT gateway, be sure that the NAT gateway is configured to forward port 21 to your *i*.LON 600. Perform a security access reset to verify the functionality.

I can access my *i*.LON 600 Web pages but some content seems to be missing.

- The *i*.LON 600 has been designed to work with Microsoft Internet Explorer 6.0 or later. Some pages will not display correctly on other browsers or prior versions of Internet Explorer. You can install Internet Explorer from the *i*.LON 600 software installation CD.

My Service LED is blinking, what does this mean?

- The Service LED blinks when the *i*.LON 600 device is not commissioned. When the *i*.LON 600 is added to a network and commissioned, the Service LED will turn off.

How do I diagnose problems with the Configuration Server?

- Click on the **Show Log** button to display the Configuration Server log. 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.

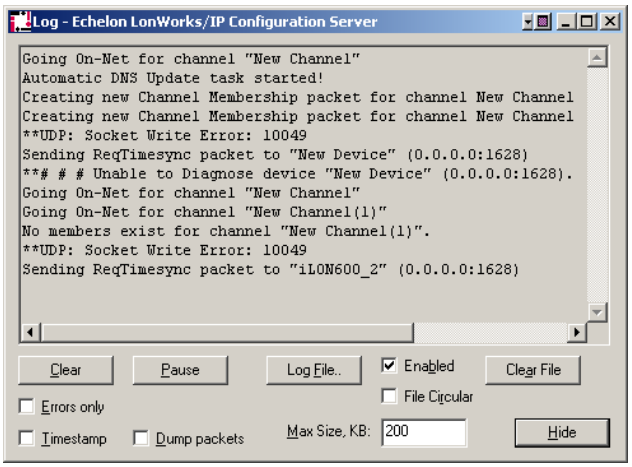


Figure 39. Echelon LONWORKS/IP Configuration Server Log

Table 15 may further help you in troubleshooting the *i*.LON 600 router.

Table 15. Troubleshooting the *i*.LON 600 Router

Symptom	*Probable Cause*	*Corrective Action*
No service pin message is received from the near router (*i*LONRTR_1 in Figure 27).	There is a problem with network connectivity, or the network interface in the PC may not be functioning properly.	Test connectivity between the network interface driver and the network interface card in the PC using the LONWORKS Plug and Play Control Panel applet that came with the network interface. Test to make sure the applet can receive a service pin message from some other node on the same channel as the *i*.LON.
	The *i*.LON 600 may not be physically connected to the network interface.	Check the network wiring between the PC and the *i*.LON 600.
	No IP address has been assigned to the *i*.LON 600.	Configure the IP address in the *i*.LON 600 using the setup web pages and the Configuration Server.
	The router application has not yet been created on the *i*.LON 600.	Create the LONWORKS router application using the Console Application.

	The VNI has not been added to the Configuration Server.	Add the VNI to the Configuration Server.
	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.
The near router (*i*LONRTR_1) commissions successfully, but no service pin message is received from the far router (*i*LONRTR_2).	There is a problem with the LONWORKS/IP channel setup.	Be sure the Configuration Server is running in the background when commissioning *i*.LON 600 routers. Verify that the near router is online and that the Configuration Server reports connectivity among all members of the LONWORKS/IP channel (e.g. all icons are green).
Both *i*.LON 600 routers commission successfully, but the device on the far side of *i*LONRTR_2 (the DI-10 LonPoint device) does not install correctly.	There is a problem with the LONWORKS/IP 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 LONWORKS/IP channel is working, and the improperly working device may not be installed correctly. If no test succeeds, verify connectivity between the *i*.LON 600 devices in the main dialog status window of the Configuration Server.
An *i*.LON 600 added to a LONWORKS/IP channel using the Configuration Server remains red in the device tree.	IP connectivity problem: the Configuration Server is not able to communicate with the *i*.LON 600 on the defined LONWORKS/IP channel.	Verify that the PC running the Configuration Server can ping the *i*.LON 600. To perform a ping, open the Windows Command Prompt (in the Accessories menu) and type “ping 10.2.11.XXX (the device’s IP address)”. You should receive a reply from your device. Examine the Configuration Server trace window for clues as to what may be going wrong. Verify that you can ping the Configuration Server PC or members of the LONWORKS/IP channel using the Windows Command Prompt.
The *i*.LON 600 on the LONWORKS/IP 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 *i*.LON 600 device, determined using the Console Application *show* command, matches the IP address defined for it in the Configuration Server. Determine if the router application exists by using the listapp command in the Console Application. Create the router app if it does not exist.

Section 3

Appendixes

Appendix A

Using NAT, DNS, DHCP and DDNS with a LONWORKS Network

This section describes the advantages of using a static IP address when setting up your network.

Network Address Translation (NAT)

Network Address Translation (NAT) allows multiple computers (hosts) to share one 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.

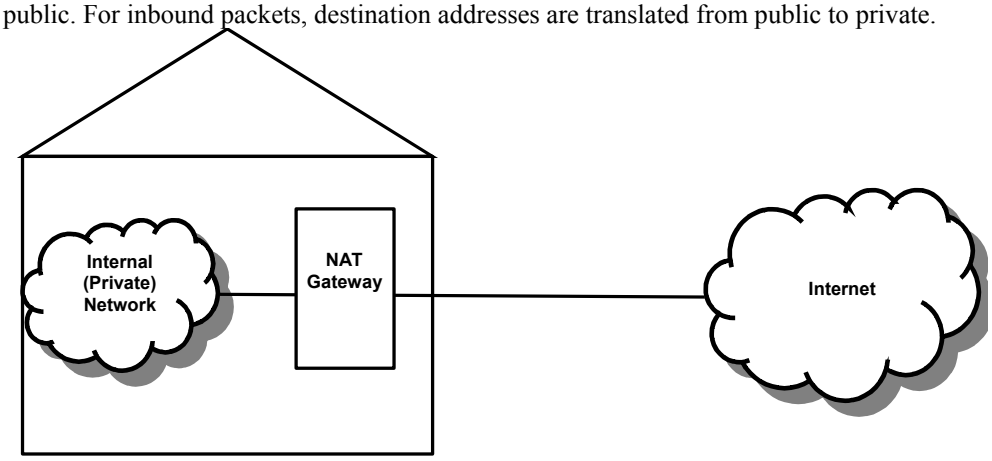


Figure 40. NAT Networking

Simple Home Network Example

If you have a home network, and you have 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 an 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:

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 that the reserved addresses are reusable, not globally unique and therefore 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. See Figure 41.

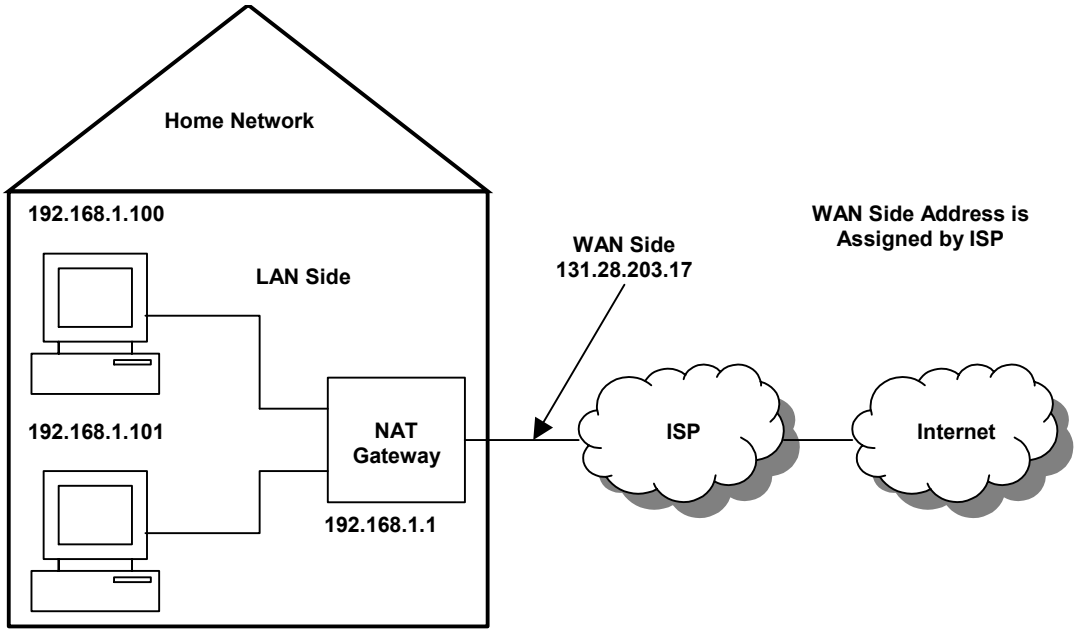


Figure 41. NAT Gateway Structure

The below steps illustrate the NAT process:

1. Using one of your home PCs, open Internet Explorer and type www.echelon.com. Your PC will send a connection initiation (SYN flagged) TCP packet to www.echelon.com (which it has previously resolved to an IP address using DNS). The Ethernet frame containing the packet is addressed to the private interface of the LAN side of the NAT gateway (your PC's default gateway).

Headers contain:

Source IP: 192.168.1.100 (your PC)

Destination IP: 205.229.51.8 (www.echelon.com)

2. The NAT gateway receives the frame and changes the source IP addresses (and checksums) in the packet headers (IP and TCP) from your computer's private address to a public address and forwards the packet to the Internet.

Headers contain:

Source IP: 131.23.203.17 (example global address provided by your ISP)

Destination IP: 205.229.51.8 (www.echelon.com)

3. The Echelon Web site replies with a TCP SYN / ACK flagged packet IP addressed to your home global address. (e.g. 131.23.203.17)

Headers contain:

Source IP: 205.229.51.8

Destination IP: 131.23.203.17

4. The NAT gateway receives this information and changes the destination IP addresses (and checksums) to your PC's private address before sending it to your PC.

Headers contain:

Source IP: 205.229.51.8 (www.echelon.com)

Destination IP:192.168.1.100 (your PC)

Note that the process is completely transparent. Neither your PC nor the Echelon Web site are aware the translation has taken place. In this case, two sets of addresses and checksums were replaced. The process is the same for UDP.

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. In the previous example, the connection was initiated from a home network to the destination address 205.229.51.8. Internet Explorer automatically appends 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 may run both a web server and an FTP server. It may additionally run a time server and other applications as well. Each service may be assigned different ports. For example, Internet Explorer uses port 80 as its default when it accesses http://www.echelon.com and maps the address as 205.229.51.8:80. When accessing an FTP client, Internet Explorer will use port 21 so ftp://www.echelon.com will map to 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 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. Note that 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 PCs.

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

In Example 1, two PCs are connected to and communicate through an NAT gateway that accesses the Internet through a single IP address. The NAT gateway forwards the packets to the correct PC using different port settings. To ensure that packets are forwarded to the proper PC, you can setup your NAT gateway to perform static port mapping. Static port mapping lets your NAT gateway forward incoming Internet requests to different PCs in your home using the port settings you specified in your PCs.

For example, if you ran a web server on 192.168.1.100 (see Example 1) you would have to use a port other than 80 since all requests arriving for port 80 are forwarded to 192.168.1.101. To solve this problem, you could run 192.168.1.100’s web server on port 81 and notify people that your secondary web server is located at 131.23.203.17:81. The NAT gateway will forward requests to your web servers depending on which URL is accessed.

i.LON 600 Ports

The *i*.LON 600 uses IANA designated ports for LonWorks traffic (ports 1628 and 1629).

Continuing with the above example, you could connect an *i*.LON 600 to your network with an IP address of 192.168.1.102.

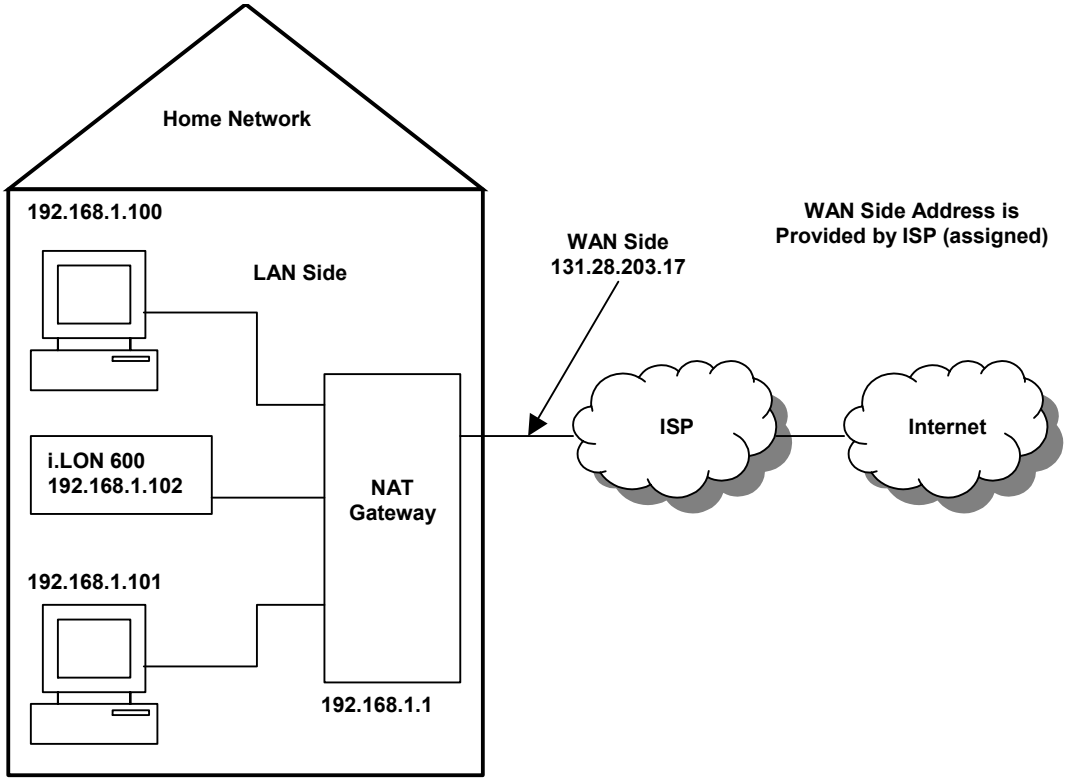


Figure 42. Adding an *i*.LON 600 to an NAT Gateway

To allow Internet access to your *i*.LON 600, you must map the necessary ports on your NAT gateway (as you did for the PCs when setting up web access). Once port 1628 is mapped to 192.168.1.102, the NAT gateway will forward any requests from peer *i*.LON 600s or from the Configuration Server.

i.LON 600s can be configured to use ports other than the IANA defaults. This allows multiple *i*.LON 600s to reside behind a single NAT gateway. The *i*.LON 600 allows you to configure various parameters through the setup Web page using a limited Web server. The default port for this Web server is port 80. In the example, port 80 is already used by 192.168.1.100, so you must change the port on the *i*.LON 600 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 owner's manual 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 each 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-1250 "high speed" backbone.

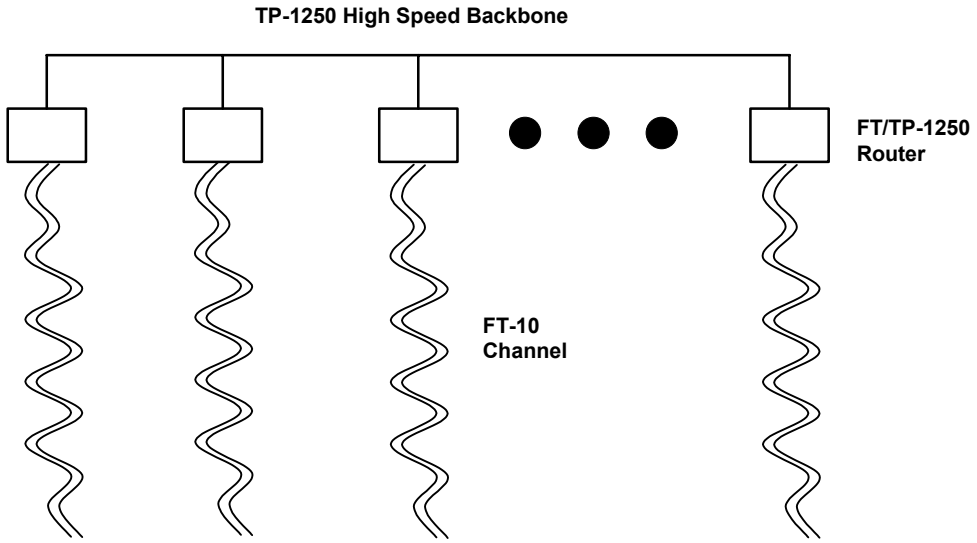


Figure 43. Connecting Devices on a Network

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

i.LON 600s are *logically* identical to TP-1250 or FT routers, but use IP as their high speed backbone instead of a TP-1250 backbone. They may not be connected to the same physical wire.

Two i.LON 600s located in different cities could use the Internet as a high-speed backbone to create a single LONWORKS network. Instead of connecting the two i.LON 600s with one long wire, the Internet is used to create a "virtual wire". The Configuration Server is the software that creates this virtual wire.

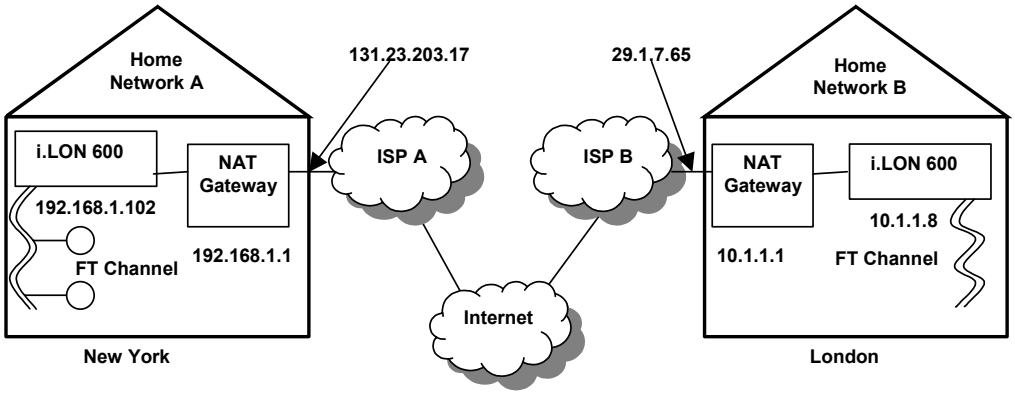


Figure 44. Creating a Virtual Wire

The Configuration Server is aware of NAT gateways and you should enter each NAT gateway in your system as you create your LONWORKS/IP channel (virtual wire). In Figure 45, the Configuration Server might look like the following:

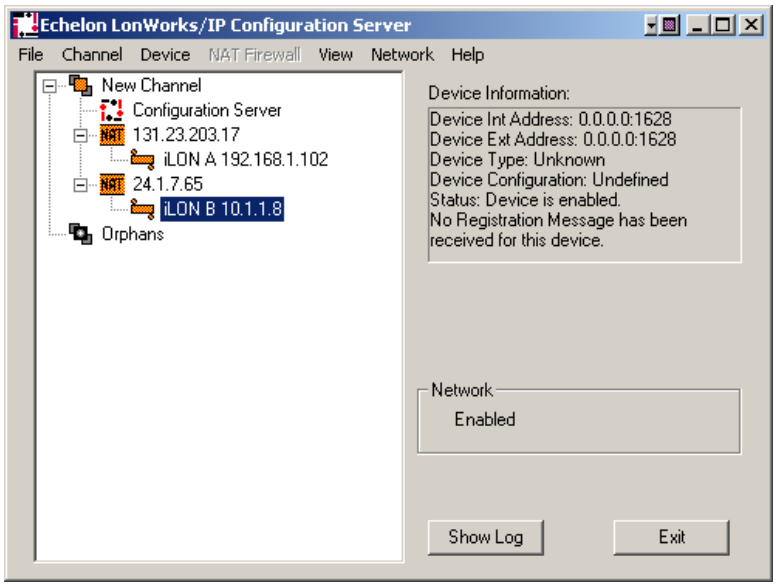


Figure 45. Configuration Server Setup

Note that the diagnostic information provided about the *i*.LON 600s (indicated by the varying *i*.LON 600 icon colors) is more complete than the diagnostics provided by the changing colors of the NAT gateways. The Configuration Server cannot acquire the same level of diagnostic information about an NAT gateway as it can about *i*.LON 600s. Table 16 describes the meanings of the different icon colors.

Table 16. Configuration Server Icon Colors

Color	*Description*
Green	Configuration Server has communicated with the *i*.LON 600 and configuration is up to date.
Yellow	The *i*.LON 600's time differs from the time on the PC running the Configuration Server by more than a few milliseconds. This usually means that either the *i*.LON 600 or the PC 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 should provide an SNTP server to both the PC and the *i*.LON 600 so that their time bases can be synchronized. When synchronized, the yellow icon should turn green.
Red	The Configuration Server can not communicate with the *i*.LON 600. This may happen if the *i*.LON 600 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 *i*.LON 600 as described above.
Orange	The *i*.LON 600'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 Configuration Server updates the *i*.LON 600, the icon will turn green. Note that in a large channel (> 40 devices) this can take several minutes. Also note that changing a bind in LonMaker can require that the routing tables in EVERY *i*.LON 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 *i*.LON 600 in the Configuration Server tree and selected Disable Device from the pop-up menu.
Cyan	The Configuration Server has not yet attempted to communicate with the *i*.LON 600. The Configuration Server may be busy communicating with other channel members (this is common on a large channel). If the Configuration Server appears not to be attempting communication, click on the Show Log button and monitor the progress. Select Update Members from the Channel menu.

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

Whenever a LonTalk routing table changes (this can happen while making a bind) or a new member is added to the LONWORKS/IP channel (virtual wire), the Configuration Server relays this information to all devices on the channel that need to know. Note that some devices on the LONWORKS/IP channel can be unaware of other devices on the channel.

Once all channel devices have been inaugurated into the LONWORKS/IP channel, and all binds have been made, you can shut down the Configuration Server software (though there is no harm in leaving it running).

DHCP

Devices in an IP network have assigned addresses such as 192.168.1.100. For small networks, manually configuring each device's IP address is fairly simple and not very time consuming. As the number of computers on your network grows, however, 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, instead of using a pre-defined address, computers broadcast a message on the local network asking the DHCP server to assign them an 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 *i*.LON 600s), can create some difficulties.

Go back to Figure 41. The addresses assigned to these computers (192.168.1.100 and 192.168.1.101) were most likely assigned manually, but could have been assigned automatically using DHCP. Many NAT gateways, in addition to providing NAT functionality, also provide built-in DHCP servers.

DHCP Servers

DHCP servers are configured to assign a range of valid Internet addresses. With a simple NAT gateway, like the one used in Figure 40, the range is often 192.168.1.2 to 192.168.1.254. As an example, the Linksys Model BEFSR81 NAT gateway assigns the first PC to request an address 192.168.1.100, the second PC to request an address 192.168.1.101, the next gets 192.168.1.103, and so on. The address a PC is assigned is determined by the order in which the PCs are powered up on a network. PCs 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 PC (or *i*.LON 600). This usually is not an issue for a home PC that is used to browse the Internet because the PC is always the initiator of the web page request. However, if you want a PC to act as a web server, it must have a permanent address so other PCs can access it. The same is true for an *i*.LON 600 participating in a LONWORKS/IP channel.

The solution is to avoid using DHCP for devices whose addresses must be known by external users. This includes FTP servers, time servers, web servers, database servers, and *i*.LON 600s.

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 Linksys 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 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 *i*.LON 600 in a LONWORKS/IP channel, you would enable static port mapping on the

NAT gateway and enter 131.23.203.17:1628 in the Configuration Server. The LONWORKS/IP packets 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.

Use a static IP address for both your NAT gateway and the *i*.LON in your home.

DNS

DNS is the Internet's Domain Name System. This system allows you to convert hard (or numeric) IP addresses (for example 131.23.203.17) into one based on letters and words (www.myhouse.com). To be able to use names instead of hard IP addresses to browse the Internet, you must specify at least one DNS server when you setup your PC's TCP/IP networking. If you selected "Obtain an IP address automatically", the DNS server is obtained automatically from the DHCP server at the same time that the PC obtains its IP address.

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.

If you had a static IP address at your home, 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, allowing you ultimately to tell people to go to www.myhouse.com instead of 131.23.203.17.

This only works for static IP addresses because each time you change the 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.

DNS/DHCP Relationship

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

DNS and the Echelon LONWORKS/IP Configuration Server

The Configuration Server can use DNS to resolve a name, but the *i*.LON 600 devices can not. When you type myilon.echelon.com:1628 into the Configuration Server instead of 205.229.51.11:1628, the Configuration Server goes to the local DNS server (defined on that PC) to resolve myilon.echelon.com to a hard address and then sends that hard address to all *i*.LON 600s on your LONWORKS/IP channel. This works until one of the IP addresses changes.

If you want to reference your *i*.LONs only by DNS name, you must leave the Configuration Server running on your network. The Configuration Server will periodically query the DNS server to verify that all hard IP addresses are still correct. If

something changes, the Configuration Server will update all *i*.LONs in the LONWORKS/IP channel.

Do not rely on DNS to resolve *i*.LON IP addresses. Use static addresses that do not change.

Dynamic DNS

If your ISP does not offer a static IP address service, and you still want Internet access to an *i*.LON at your house, 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 home's IP address does not frequently change. Depending on your ISP, the home address may change only when you power cycle the NAT gateway. If the NAT gateway is on 24/7, it may be months before your home's address changes. It is also possible that your 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 supposed to go back and acquire another lease.

When using DDNS, each time a new DHCP lease is given (e.g. each time the PC'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 home, instead of telling the registrar that www.myhouse.com is linked to 131.23.203.17, you tell the registrar that www.myhouse.com is linked to myhouse.ddns.org (for example). When an Internet user types in www.myhouse.com, the Internet DNS server forwards the request to myhouse.ddns.org, which forwards the request to the current IP address of your home.

The DDNS provider tracks any changes in your home's address and maps/forwards any request for myhouse.ddns.org to your house's current IP address.

Because of its potential complications and its reliance on relatively small third party providers, we do not recommend using DDNS when constructing LONWORKS/IP channels.

*Check the terms of service agreement with your ISP before using DDNS. Some ISPs restrict using these services.

Appendix B

The *i*.LON 600 Console Application

This appendix describes how to use the *i*.LON 600's console application through the serial port.

The *i*.LON 600 Console Application

You can use console application to configure and troubleshoot an *i*.LON 600. To access the console application, you must connect a female-to-female DB-9 cable from the **Console** hardware output to a COM port on your computer; then use a terminal emulator, such as Windows HyperTerminal, to communicate on the specified serial port. Set the communications parameters on the terminal emulator to 9600-8-N-1 and turn flow control off. Figure 46 shows a sample startup screen.

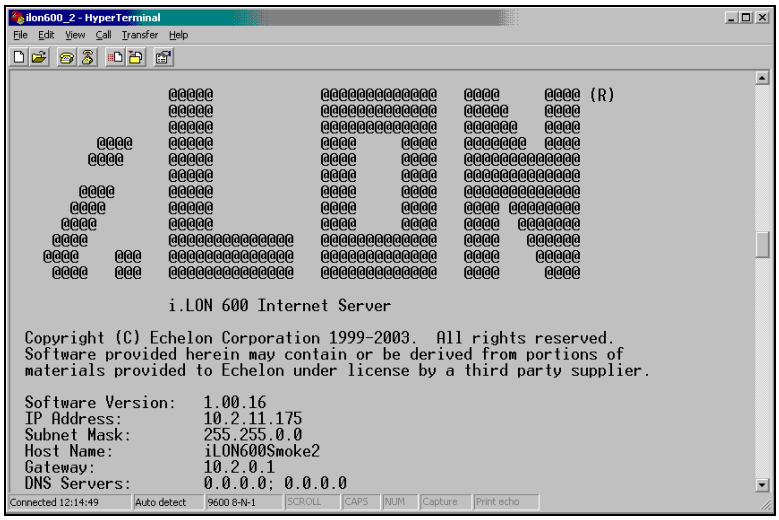


Figure 46. Console Application Startup Screen

Console Command List

Once you have accessed the *i*.LON 600 console application, you can issue commands. You must reboot the *i*.LON 600 (either through the console application or the setup Web page) for any changes to take effect. You can use the following commands with the *i*.LON 600 console application:

Table 17. Console Application Command List

activateapp *index*|*name*	The *i*.LON 600 server uses a multitasking operating system. This command allows you to selectively activate or deactivate processes. Version 1.00 of the *i*.LON 600 server firmware supports the Router (index 1) process.
authkey *key*	Sets the 16 byte MD5 authentication key.
cd [*directory*]	Changes to the specified directory. If no argument is provided, displays current directory.
copy *file1 file2*	Copies *file1* to *file2*.
createapp *name*	Creates an application instance, specified by name, and returns the index assigned to the application. The application is automatically activated after it is created. The user does not generally use this command.
cenelec *on*|*off*	Power line model only. Enables the CENELEC mode (for communicating on European C-band power line networks).
date *mm/dd/yyyy*	Sets the date. This is not allowed if the *i*.LON 600 server is synchronized to an SNTP server.
deactivateapp *index*|*name*	Deactivates an application instance, specified by index or name. See

	activateapp for supported names. This command does not delete the instance of the application; it deactivates the application. This function is primarily used for troubleshooting.
delete *file*	Deletes *file*.
dhcp *on*|*off*	Turns DHCP on and off. If DHCP is on, the *i*.LON 600 DHCP client retrieves its IP address, gateway, subnet mask, primary DNS server (if used), and DNS domain from a DHCP server.

diag *Module subcommand* [*params*]	Performs diagnostic commands on the *i*.LON 600 server. You may be asked to perform these commands by Echelon support personnel to assist them in diagnosing problems with your *i*.LON 600 server. The *module* argument must be set to ConMan (connection manager). Valid *subcommands* are:
	trace [value] – This subcommand sets and views the debug trace level. To view the current trace level, provide no argument (*i.e.* `diag ConMan trace`). To turn on tracing, enter one of the following parameters:
	0x01 – enable MAJOR_EVENT
	0x02 – enable MINOR_EVENT
	0x04 – enable STATE_TRANSITION
	0x20 – enable AUTHENTICATION
	You can enable multiple traces by adding the values of the traces to be enabled. For example, the following command enables MAJOR_EVENT and STATE_TRANSITION tracing:
	`diag ConMan trace 0x5`
	ping IpAddress [count] – Pings the *IpAddress count* times. For example, the following command pings `10.6.8.100` 5 times:
	`diag ConMan ping 10.6.8.100 5`
	If all pings get a response, the console will display:
	`IpAddress` `is alive`
	If the pings get no response, the console will display:
	`No answer from` *`IpAddress`*
	Show [route] – The `diag ConMan show` command displays connection manager configuration information. If the optional *route* parameter is entered (`i.e. diag ConMan show route`), connection manager configuration and IP routing information is shown.

dir [*directory*]	Lists directory contents. If no directory is specified, lists the contents of the current directory.
disable *service*	Disables a service. Available services are: Ftp – FTP access Web – HTTP access Dial-in – Dial-in access DnsServerViaDhcp – Obtaining DNS server from DHCP. DnsDomainViaDhcp – Obtaining DNS suffix via DHCP.
dnsdomain *domain*	Sets the DNS domain name. This command is valid only when DHCP is turned off or Obtaining DNS Suffix From DHCP is disabled while DHCP is enabled (see the enable and disable commands for more information).
dnsprimary *address*	Sets the IP address of the primary DNS server. This command is valid only when DHCP is turned off or Obtaining DNS Suffix From DHCP is disabled while DHCP is enabled (see the enable and disable commands for more information).
dnssecondary *address*	Sets the IP address of the secondary DNS server. This will only be used if the primary DNS server cannot be contacted.
enable *service*	Enables a service. Available services are: Ftp – FTP access Web – HTTP access Dial-in – Dial-in access

	DnsServerViaDhcp – Obtaining DNS Server from DHCP. DnsDomainViaDhcp – Obtaining DNS suffix via DHCP.
eventlog *on*|*off*	Turns the console event log on and off. The event log is kept in `eventlog.txt` in the root directory of the *i*.LON 600 server.
factorydefault	Resets the *i*.LON 600 server to its factory defaults. Files added by the user outside of the `/root/software` directory (*i.e.* Web pages) are not affected. Echelon highly recommends that user run this command from the *i*.LON 600 bootrom console. See *Interrupting the Boot* Process, later in this Appendix, for more information.
ftppassword *password*	Sets the FTP password to *password*; anonymous FTP is not allowed. By default, the FTP password is *ilon*. If the Global password on the Security Web page is changed, the FTP password will be changed to the same value.
ftpuser *name*	Sets the FTP username to *name*. By default, the FTP username is *ilon*. If the Global username on the Security Web page is changed, the FTP username will be changed to the same value.
format	Formats the *i*.LON 600 server's flash disk. Caution! This command deletes all files, including the *i*.LON 600 server's system image file. After using this command, you must upload a new software image to the *i*.LON 600 server. Echelon highly recommends that user run this command from the *i*.LON 600 bootrom console. See *Interrupting the Boot* Process, later in this Appendix, for more information.
gateway *address*	Modifies the gateway address. Enter `0.0.0.0` to specify no gateway. For example, gateway `10.1.10.1`. This command is valid only if DHCP is turned off.
help	Displays a list of typically used commands. `Help all` displays a complete command list.
history [*size*]	If you do not specify the *size* parameter, this command displays a history of console commands issued since the last reboot. You can specify a size from 10 to 100 to determine how far back the command history is kept.
hostname *name*	Modifies the host name. For example, `hostname ilon600`.
install *idx*|*name* [*dmn*]*sn nd*	Installs a LONWORKS domain/subnet/node address for the application specified by *idx*. Caution! This command is provided for backward compatibility to add an *i*.LON 600 server to a pre-installed network. Echelon does not recommend or support using this command. The *i*.LON 600 server should be installed using a standard network installation tool such as the LonMaker tool.
ipaddress *address*	Modifies the IP address. For example, `ipaddress 101.253.100`. This command is valid only when DHCP is turned off.
listapp	Lists the current application instances.
lwipchanmode *1 to 3*	Sets the channel mode (i.e. compat/EIA/firewall) and displays current mode if none is supplied. .1 corresponds to backward compatibility mode, 2 corresponds to Standard EIA 852 mode and 3 corresponds to extended firewall support
lwipport *port number*	Sets the IP port used for the LONWORKS/IP channel.
mkdir *directory*	Makes a directory.
nataddr *IP address*	Sets the NAT address, displays current addr if none supplied.
ping *hostaddr*	Tests communications to another IP host.
reboot	Reboots the *i*.LON 600 server. If the *i*.LON 600 server is currently being used as an RNI, the networks for which it is acting as an interface must be closed and opened.

removeapp *index*|*name*	Deletes an existing application instance, specified by index or name. The user should generally not use this command.
rename *file1 file2*	Renames *file1* to *file2*.
servicepin *index*	Sends a service pin message for the application specified by *index*. See activateapp for supported indexes.

show [*all*| *hwInfo*]	This displays configuration information about the *i*.LON 600 server. For example, show might display:
	`Software Version: 2.00-0024`
	`IP Address: 10.1.253.201`
	`Subnet Mask: 255.0.0.0`
	`Host Name: echeloni600`
	`Gateway: 0.0.0.0`
	`SNTP Server: 0.0.0.0`
	`DHCP: off`
	`MAC Address: 00-D0-71-00-4A-04`
	`Time: MON SEP 13 08:30:02 2003`
	`UTC Time: MON SEP 13 06:30:02 2003`
	`Startup script:`
	`/root/config/startup.scr`
	`Timezone: MET:60:1:5.1.3.2:5.1.10.4`
	Show all displays all parameters. Show hwinfo displays hardware properties.

shutdown	Quits all applications on the *i*.LON 600 device. A reboot is required to restore operation of all modules.
sntpaddress *address*	Modifies the address of the SNTP server. If you have a backup SNTP server, you can enter sntpaddress *address1 address2.*
sntplog *on*|*off*	Enables or disables SNTP logging. The SNTP log file is named `sntp.log` and is located in the root directory of the *i*.LON 600 server. The time logged in the SNTP log file is in universal coordinated time (UTC). The maximum size of the SNTP log file is 50 Kbytes. When the file exceeds 50 Kbytes, logging is automatically disabled. Use this command to diagnose time synchronization problems.
subnetmask *address*	Modifies the subnet mask. For example, `subnetmask 255.255.255.0`. This command is valid only when DHCP is turned off.
time *hh:mm:ss*	Sets the time. This is not allowed if the *i*.LON 600 server is synched to an SNTP server.
timezone *zone*	Sets the time zone with the following format: *nameOfZone*:*timeInMinutes*FromUTC:*dstUsed*:*daylightStart*:*daylightEnd* where *dstUsed* is 0 or 1, and daylight savings start/end times are in the form *rank.day.month.hour*. For example, 1.1.4.2 is the first Sunday in April at 02:00. Rank is a number from 1 to 5 with 5 meaning the last instance in the month. Days are numbered 1 to 7 starting with Sunday. Months are numbered 1 to 12, starting with January.
trace *level* [*stamp*]	Sets the tracing level; 0 = None; 1 = Urgent tracing only (default); 2 = Verbose tracing (for debugging only, not recommended). The optional *stamp* parameter enables time stamping with each trace.
type *file*	Types the contents of *file*.
update *bootrom* [*file*]	Updates the bootrom of the *i*.LON 600 server. By default, this command will look for the `bootrom.upd` file in the /root directory of the *i*.LON 600 server. Echelon highly recommends that user run this command from the *i*.LON 600 bootrom console. See *Interrupting the Boot* Process, later in this Appendix, for more information.

Interrupting the Boot Process

The *i*.LON 600 server undergoes an extensive boot process upon power-up and when reset by the reset button or a reboot command issued in the Configuration Server, reboot web page, or console application. During the boot process, the *i*.LON 600 server's disk structure is automatically checked to ensure that any structural errors on the disk are repaired (similar to running a `chkdsk` command in DOS), and a message is displayed on the screen if any corrections are made to the disk. Additional information about the corrections is written to the event log file. The boot process then loads the *i*.LON 600 server's system image. Successful completion is indicated when the *i*.LON 600 server displays its normal command-line prompt.

If the *i*.LON 600 server repeatedly fails to boot up, you are unable to FTP files to it, or you suspect the image is corrupted, you may interrupt the boot process to troubleshoot the *i*.LON 600 server.

To interrupt and bypass the boot process, press the exclamation point (!) key when the "Press the '!' key to stop auto-boot…" message appears on the console. This message displays for approximately 4 seconds at the beginning of the boot process (following self-test and memory initialization). If the auto-boot is interrupted, the boot image is then loaded from ROM, and the *i*.LON 600 server enters the bootrom state.

The Bootrom State

When the boot process is interrupted or fails (*e.g.*, if the iLonSystem image is corrupt or not available, perhaps due to a power cycle during image download), the *i*.LON 600 server loads its system image from ROM and starts a console application similar to that run by the normal iLonSystem image. This state, called the bootrom state, is indicated by a command-line prompt prefixed with [Bootrom]. If caused by a boot failure, you may need to reload or upgrade the *i*.LON 600 server software to restore proper operation.

While in the bootrom state, only a subset of the normal console commands are available. The *i*.LON 600 server provides the minimal functionality required to troubleshoot and recover its system image. The FTP server runs, and the console provides commands needed to recover the image; however, application commands, such as `listapp` and `createapp`, are not available and certain attributes are not displayed.

Updating the Bootrom

Echelon may provide you with updates to the *i*.LON 600 server bootrom. The bootrom can be updated using the console application. To update the bootrom, follow these steps:

1. Obtain the updated bootrom file from Echelon. The default name for this file is `bootrom.upd`.
2. Reboot the *i*.LON 600 server using the console application. When the console reads "`Press the '!' key to stop auto-boot`", press '!'. The *i*.LON 600 server will reboot to the bootrom state, halting all applications.
3. FTP the `bootrom.upd` file into your *i*.LON600 /root directory.
4. Update the bootrom by executing the `update bootrom` command. If the bootrom file name is different than the default (`bootrom.upd`), specify the actual file name as an additional parameter. When the update completes, it will automatically reboot your *i*.LON600 system.

WARNING:

Do not interrupt the bootrom update process. Doing so will render the *i*.LON 600 server unable to boot. If this happens, you will need to ship your *i*.LON 600 server back to Echelon to be repaired.

Appendix C

i.LON 600 Firmware

The latest version of the *i*.LON 600 firmware is included with the software on the CD. These files are installed on the PC `LonWorks\iLON600\Images\iLON600 1.00`, where `1.00` is the major and minor version number. The directory structure is a duplicate of the directories contained by the *i*.LON 600 device. If you receive an update of the *i*.LON 600 firmware, you can update the firmware as described in *Updating the i.LON 600 Firmware*, later in this chapter.

Updating the *i*.LON 600 Firmware

New versions of the *i*.LON firmware may become available at www.echelon.com/ilon. To update your *i*.LON hardware with a new firmware version, follow these steps:

1. Log onto www.echelon.com/ilon.
2. Download the firmware update to your PC. It is recommended that the update be placed in the `LonWorks\iLON600\Images\iLON X.xx` folder where `X.xx` is the major and minor version number (the setup program will place the firmware update in this location by default).
3. Download all the files in the new `LonWorks\iLON600\Images\iLON X.xx` directory to the *i*.LON 600's flash disk using a standard FTP program. Overwrite any existing files of the same name, maintaining the directory structure that was created when you copied the firmware to your PC.

The *i*.LON 600 Directory Structure

The *i*.LON 600 contains a file system with a directory structure as described in this section. This directory structure is replicated on your computer in the `LonWorks\i.LON600\Images\iLON600 1.00` directory. You can access the *i*.LON 600 file system using an FTP client such as Internet Explorer. The top level of the *i*.LON 600 directory structure appears as shown in Figure 47:

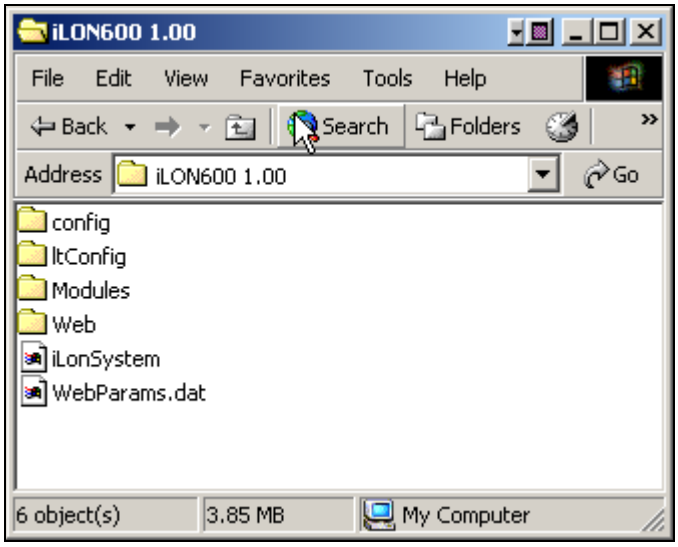


Figure 47. *i*.LON 600 Directory Structure

The folders contain the following information:

Table 18. Device Status Indicator	
Directory	***Description***
Config	Contains the configuration files for the *i*.LON 600 .
ltConfig	Contains LonTalk configuration data. Do not modify the files in this folder.
Modules	Contains executable modules. Do not modify the files in this folder.
Web	Contains the web pages used for setting up the *i*.LON 600.
Webparams.dat	This file is used to set *i*.LON 600 web security.
iLonSystem	This is the *i*.LON 600 system image. Do not modify or move this file.

Appendix D

Using Your *i*.LON 600 to Access a Remote Network

Creating a LONWORKS/IP Channel

Creating a LONWORKS/IP channel involves configuring each LONWORKS/IP device that will be on the channel and informing the Configuration Server of all LONWORKS/IP devices on the channel. A LONWORKS/IP device can be an *i*.LON 600 or a PC running LNS 3.0 or better. To create a LONWORKS/IP channel, follow these steps:

1. Set the IP address, subnet mask, and default gateway for all *i*.LON 600s using the *i*.LON web interface, as described in Chapter 4.
2. Ensure that the Configuration Server PC can communicate with each *i*.LON 600 or the LNS 3.0 PC.
3. If the LONWORKS/IP channel will contain only *i*.LON 600 devices, skip to Step 7. If the LONWORKS/IP channel will contain one or more PCs running LNS 3.0 or later, select Start/Settings/Control Panel on your PC and run the *LONWORKS/IP Channels* control panel. This control panel appears in Figure 48.

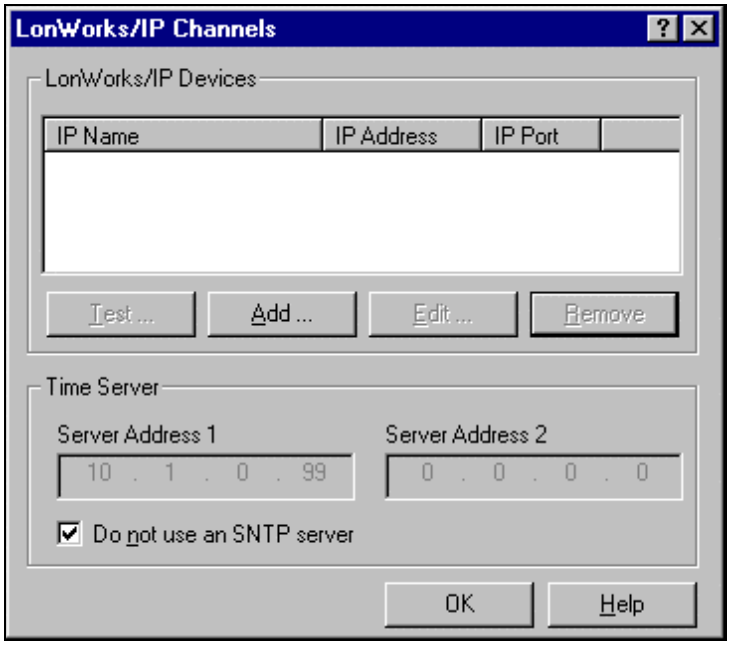


Figure 48. LONWORKS/IP Channels Dialog Box

4. Click the **Add** button to add a LONWORKS/IP interface to the PC. The dialog shown in Figure 49 appears:

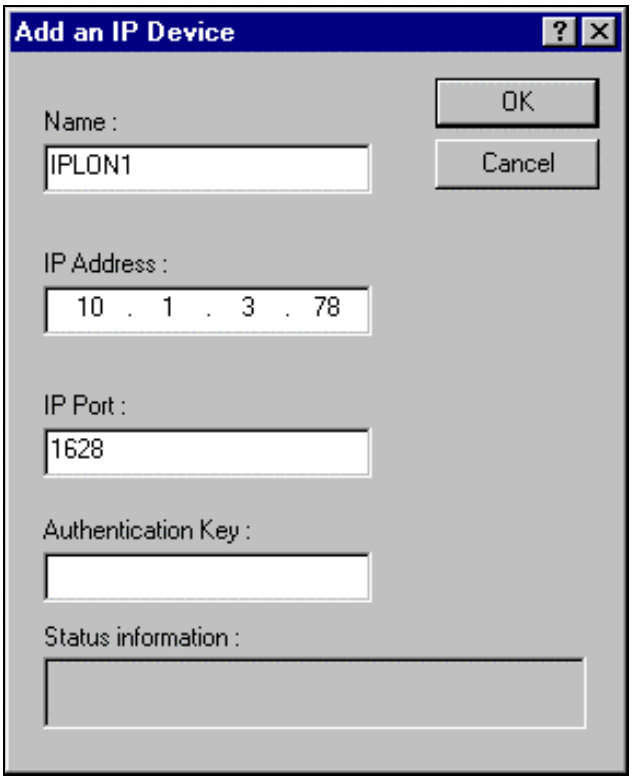


Figure 49. Add LONWORKS/IP Device Dialog

5. Fill in the following information:

Name	The name of the LONWORKS/IP device.
IP Address	The IP address of the device will be automatically set to the PC's IP address (if the PC has multiple Ethernet cards with different IP addresses, you may select the specific address you want to use).
IP Port	The port that the PC communicates with other LONWORKS/IP devices. By default, this is 1628.
Authentication Key	If the LONWORKS/IP channel will be set up to use MD5 authentication, enter the 16 pair hexadecimal authentication key in this field.

6. Click **OK**. The control panel will now look as shown in Figure 50.

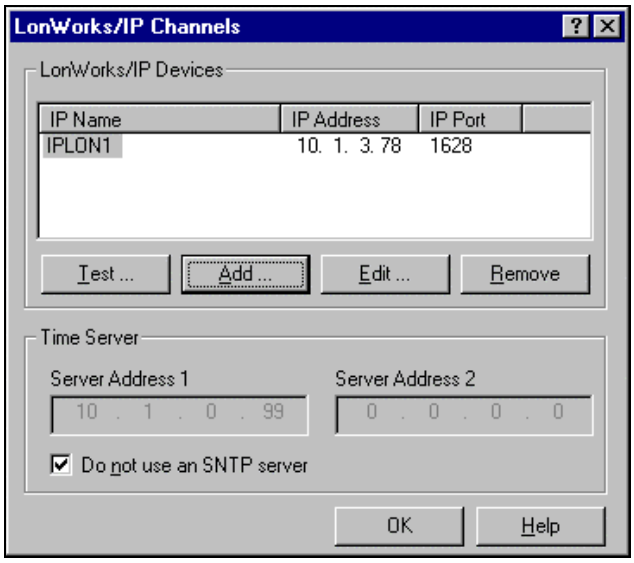


Figure 50. LONWORKS/IP Channels Control Panel

7. Start the Configuration Server application. From the Windows desktop click on Start/Programs/Echelon *i*.LON 600/LonWorks-IP Configuration Server. The Configuration Server main dialog appears:

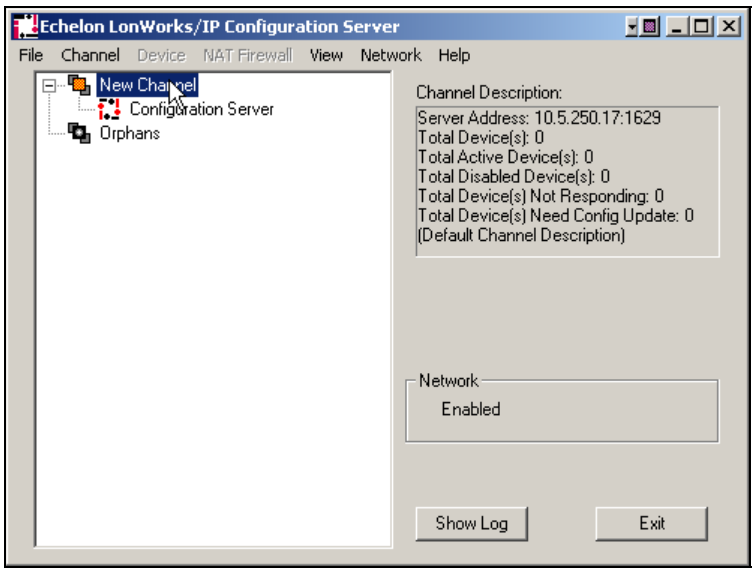


Figure 51. Configuration Server

8. To rename **New Channel** to a more descriptive name, right-click on **New Channel**, select **Rename Channel**, and enter the descriptive name.

9. Click on the **Show Log** button to display the Configuration Server log. 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.

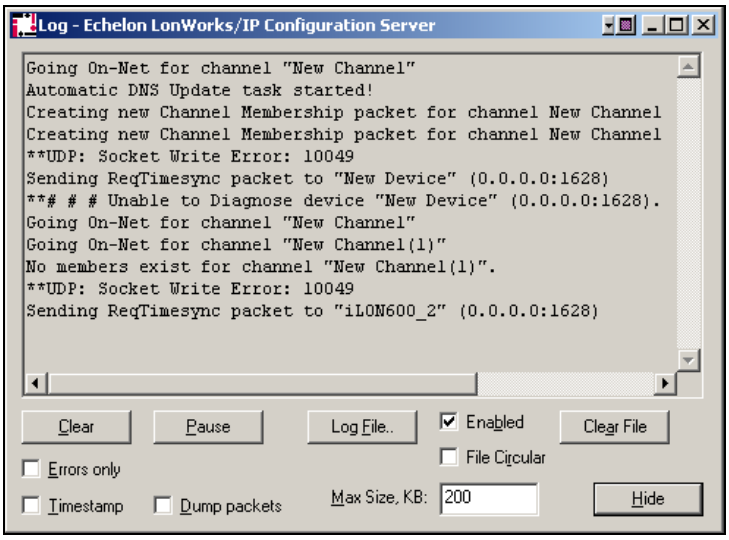


Figure 52. Configuration Server Log

10. Verify that the Configuration Server is attached to your IP network by checking the **Enabled** in the **Network** menu. The Configuration Server should detect the IP address of your PC.

11. Verify your PC's IP address by selecting **Settings** from the **Network** menu and confirming that the Configuration Server's proper IP address is listed in the **TCP/IP address or host name** field. The **Local IP** button shows the available IP addresses for your network channels. On the Configuration Server main dialog screen in Step 7, the **New Channel's Server Address** is set to 10.5.250.17, port 1629. This confirms that the Configuration Server is running on a PC with an IP address of 10.1.3.78, and the utility is using port 1629 to create the LONWORKS/IP devices on PCs running LNS 3.01 or later only respond to Configuration Server setup messages when the LONWORKS/IP device is open. To force a LONWORKS/IP device to open, run the LONWORKS/IP Channels control panel and click the **Start Test** button as shown in Figure 32.

Appendix E

i.LON 600 Web Server Parameters Application

This section contains information about modifying the *i*.LON 600 Web page security.

Overview of i.LON 600 Web Page Security

The *i*.LON 600 Internet Server supports a Web page security feature that allows you to restrict access to files under the *i*.LON 's `/root/Web` directory. Access may be secured by user name/password, source IP address, or location of the resource (URL).

Web page security is defined using the *i*.LON Web Server Security and Parameters software. This is a standard utility that is included in all *i*.LON software products.

To start this program, click **START/PROGRAMS/Echelon i.LON 600/i.LON 600 Web Server Security and Parameters** or from the Configuration Server select **i.LON Web Server Security and Parameters** from the **Network** menu. The *i*.LON 600 Web Server Security and Parameters software creates a file called WebParams.dat. This file must be uploaded to the *i*.LON 600's root directory (/root/WebParams.dat) using a standard FTP program overwriting a default WebParams.dat.

The WebParams.dat file is parsed by the *i*.LON 600 on startup to restrict access to Web pages. Note that the WebParams.dat file is stored as plain text with no encryption or password protection. This means that *i*.LON 600 security is protected from inspection by FTP security (user name and password) only. Be sure to set the proper user name and password for FTP access to prevent the WebParams.dat file from being viewed. Also, be sure to secure the PC on which you generated the WebParams.dat file. See *Chapter4, i.LON 600 Security Web Page* to set the FTP user name and password.

The default WebParams.dat files allow access to all files under the root/Web directory from any location. The default user name is *ilon* and the default password is *ilon*. To modify the user name and password fields, you must create a new (or edit an existing) WebParams.dat file. This updated file must be uploaded to the *i*.LON 600 and the i.LON 600 must be rebooted for the new security settings to take effect. To update the settings, perform the following steps:

1. Download the existing WebParams.dat file from the i.LON 600 using an FTP application.
2. Start the *i.LON Web Server Security and Parameters* application, select **Open** (**File** menu) and open the `WebParams.dat` file.
3. Click the `ilon` user name in the list.

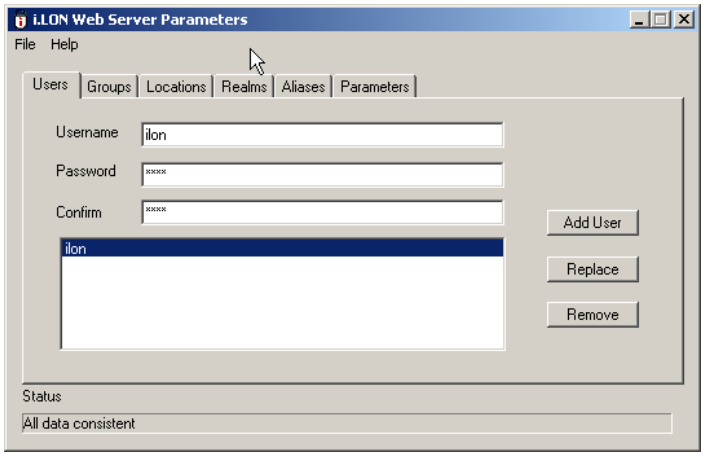


Figure 53. Opening the WebParams.dat File

4. Enter the desired user name and password (in this example, the passwork is myilon) and click the **Replace** button. The new user name is now shown on the user list. See Figure 54.

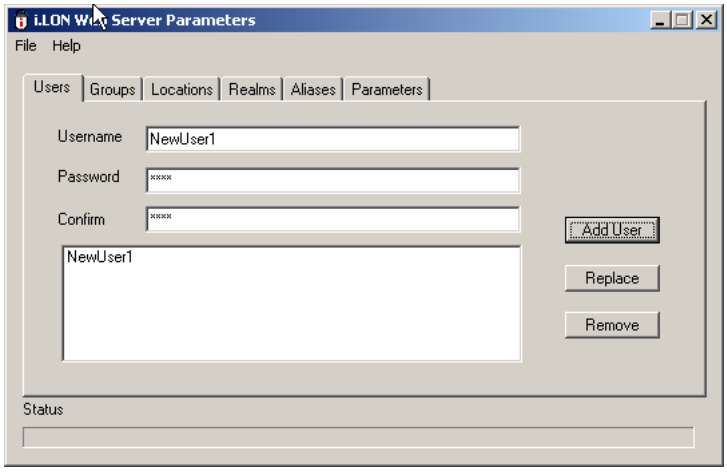


Figure 54. Creating a New User

4. After editing or replacing the default user name and password, click the **Groups** tab. Select `all` from the **Groups** list. All members of the list appear. Remove *ilon* user from the list by clicking the **Remove** button (located next to the **Add User** button).

5. Finally, add the new user that you created in Step 3 to the *all* group by clicking **Add User** as shown in Figure 55.

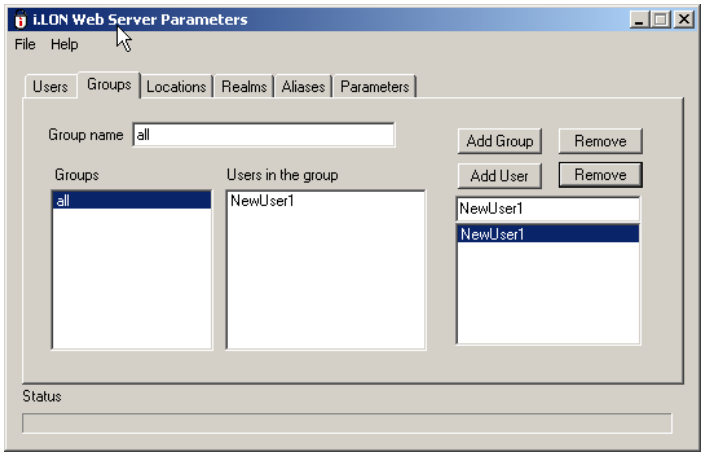


Figure 55. Adding a New User

6. Save the WebParams.dat file by clicking **Save** (**File** menu).

7. Using FTP application, upload WebParams.dat to the i.LON 600's /root directory.

8. Reboot the i.LON 600 to activate the security changes.

See the *i*.LON Web Server Security and Parameters help file for detailed information on each setting.

Sample WebParams.dat File

The following is an example of a WebParams.dat file using the above example.

```
iLonSecurity 1.3 600
GlobalMemoryBytes:16384
RequestMemoryBytes:16384
TaskStackBytes:307200
NumTasks:1
TaskPriority:240
MaxSymbols:100
MaxUrlSize:1024
(Users)
all:NewUser1:myilon
(Locations)
everywhere:*.*.*.*
(Realms)
/forms/Echelon/*:all:everywhere
(Aliases)
```