ECHELON®

i.LON™ 1000 Internet Server User's Guide

Version 1.01

078-0184-01B

Printed in the United States of America.

Echelon Corporation
415 Oakmead Parkway
Sunnyvale, CA 94085, USA

Preface

The *i*.LON 1000 Internet Server is a high performance server that provides connectivity between LONWORKS® control networks and Internet Protocol (IP) data networks, while enabling access to network variable information by standard web browsers. This user's guide describes how to install, configure, use, and manage the *i*.LON 1000 as a router and web server.

Purpose

This user's guide describes how to install the *i*.LON 1000 hardware, and configure, use, and manage the *i*.LON 1000 as a router and web server.

Audience

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

Content

The *i.LON 1000 Internet Server User's Guide* includes the following content.

- Chapter 1, *Introduction*, provides an introduction to the *i*.LON 1000 Internet Server.
- Chapter 2, *Shipping Content and Hardware,* describes the contents of the iLON box, the i.LON 1000 hardware, the various ports, and mounting options.
- Chapter 3, *i.LON 1000 Software,* describes the various i.LON 1000 software components, and the PC utilities used to interact with the i.LON 1000 Internet Server. PC software installation, and i.LON 1000 software upgrade procedures are also covered in this chapter.
- Chapter 4, *The i.LON 1000 Console Application,* describes how to use the console application to set up the *i*.LON 1000's IP information such as IP address, subnet mask, default gateway, etc.
- Chapter 5, *LONWORKS/IP Channels Background and Definition,* provides the theoretical basis for using *LONWORKS* /IP channels. This chapter introduces the concept of tunneling *LONWORKS* packets through an IP network.
- Chapter 6, *IP Resources Required to Create LONWORKS/IP Channels,* outlines the IP resources necessary to support *LONWORKS* over IP and provides a simple worksheet of what TCP/IP resources must be provided by the local network administrator.
- Chapter 7, *Creating a LONWORKS/IP Channel,* provides a step-by-step guide (in tutorial form) to setting up a *LONWORKS* /IP channel and using i.LON 1000 Internet Servers in layer 3 routing mode. The tutorial covers *i*.LON 1000 devices as well as LONWORKS/IP devices created on PCs running LNS 3.01 or better.
- Chapter 8, *LONWORKS/IP channel Timing Considerations*, discusses timing parameters and how they should be set up depending on the sort of IP network you are using for your LONWORKS/IP channel (i.e LAN, Internet, etc.).
- Chapter 9, *Creating an i*.LON 1000 *Web Page*, provides a step-by-step guide (in tutorial form) to monitoring and controlling a *LONWORKS* network using the *i*.LON 1000 web server and a standard web browser.
- Chapter 10, *Advanced Usage of the* `<iLonWeb>` *HTML Tag*, contains advanced information on creating HTML web pages.

- Chapter 11, *i*.LON 1000 *Web Page Security*, describes how to add basic web authentication to password protect some or all of the web pages on your *i*.LON 1000 Internet Server.
- Chapter 12, *Advanced Topics*, Contains information on advanced topics, including Aggregation, MD5 Authentication, LonMark Resource Files, DHCP, Event Logs, and SNMP.
- Appendix A, *Console Application*, provides an overview of the Console Application and describes the console commands, the *i*.LON 1000 boot process, and the line editor.
- Appendix B, *Web Page Examples,* explains how to install and use the Web server application example, including a LonMaker network and web pages, that ships with the *i*.LON 1000.
- Appendix C, *Client Side Programming Examples,* contains two examples of using JavaScript to create *i*.LON 1000 web applets.
- Appendix D, *i.LON 1000 Web Server Errors*, contains a list of errors that may be returned by the *i*.LON 1000 web server and some troubleshooting information.

Contents

1

Introduction

This chapter provides an introduction to the *i*.LON 1000 Internet Server, including its applications, hardware, software, and utilities.

Introduction

The *i*.LON 1000 Internet Server provides reliable, secure Internet access to LONWORKS devices.

LONWORKS control networks are the worldwide standard for networking controls and machines in building, industrial, home, transportation, and utility automation applications. Internet Protocol (IP) based data networking is the worldwide standard for moving data over the Internet, Local Area Networks (LANs), and Wide Area Networks (WANs). Echelon's *i*.LON 1000 Internet Server seamlessly links together these control and data networking standards. By allowing the millions of Internet-ready LONWORKS devices already in use to be monitored, controlled, accessed, manipulated, and updated over the Internet, the *i*.LON 1000 opens a new world of applications, markets, and business opportunities.

Figure 1-1 *i*.LON 1000 Front Panel

The *i*.LON 1000 offers unparalleled performance and reliability. Certified under the Cisco Ne*tWork*s™ program, the *i*.LON 1000 integrates Echelon's control networking and routing expertise together with Cisco's Network Foundation Technologies. The result is a Layer 3 LONWORKS router that offers very high packet throughput for demanding process control, building automation, utility, transportation, and telecommunications applications. Cisco certification is your assurance that the *i*.LON 1000 has been both rigorously tested and will meet the needs and standards of Information Technology (IT) managers worldwide. Adherence to the EIA proposed standard for tunneling ANSI/EIA 709.1 packets over IP ensures that communications through the *i*.LON 1000 are both open and interoperable.

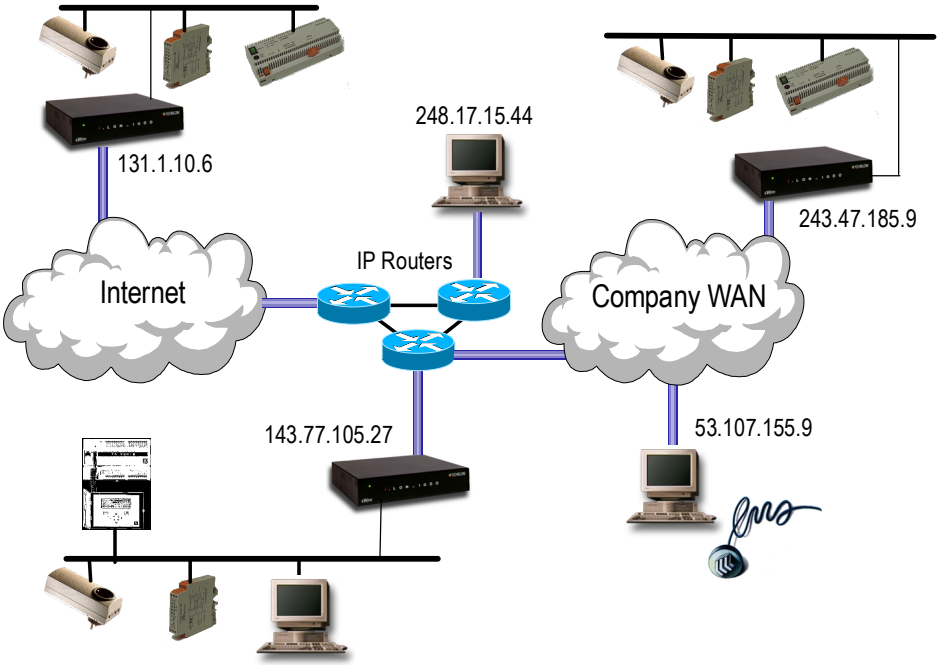


Figure 1-2 *i*.LON 1000 Application

The *i*.LON 1000's built-in Web server allows control information (such as network variables representing temperature, occupancy, speed, etc.) to be accessed easily through a web browser. This password-controlled feature provides access to LONWORKS monitoring and control data from anywhere without the need for special software tools, over LANs, WANs, or the Internet.

The *i*.LON 1000 is unique in its ability to support both peer-to-peer and master-slave network communications. This powerful feature allows remotely located devices to communicate over IP networks in the same way they would if they were co-located. Devices on different floors of a building, scattered across different manufacturing pods, or located in retail branches across the world can be seamlessly and transparently linked together, and connected to far-flung corporate data and ERP networks.

The impressive performance of the *i*.LON 1000 is due to the combination of a powerful 32-bit RISC processor and Echelon's LONWORKS/IP software architecture. The result is very high packet throughput in control networks with large numbers of nodes and very fast monitoring and display requirements.

The *i*.LON 1000 can be installed using standard LONWORKS installation tools. For example, the *i*.LON 1000 is fully supported by tools using Echelon's LNS™ network services architecture (such as the LonMaker™ Integration Tool), which provides quick setup, configuration, and application-level interoperability. From the perspective of the IT network, the *i*.LON 1000 is viewed as a typical IP host. Like other IP hosts, the *i*.LON 1000 supports standard Internetworking protocols: TCP/IP, UDP, DHCP, SNMP (MIB II), ICMP, SNTP, TOS, MD5, HTTP, and FTP. In addition, packet aggregation parameters, addressing, IP bandwidth utilization, and security can all be adjusted via the IP network.

2

Shipping Content & Hardware

This chapter describes the *i*.LON 1000 Internet Server hardware and explains the various mounting and cabling options.

Shipping Contents

Table 2-1 describes the items shipped with the *i*.LON 1000 Internet Server.

Table 2-1 *i*.LON 1000 Shipping Contents

Item	Description
***i*.LON 1000 CD**	The CD contains *i*.LON 1000 PC software utilities and a copy of the *i*.LON 1000 firmware.
***i*.LON 1000 Internet Server User's Guide**	The User's Guide describes how to install the *i*.LON 1000, and configure, use, and manage the *i*.LON 1000 as a router and Web server.
***i*.LON 1000 Internet Server Mounting Template**	A template to accurately measure the placement of the *i*.LON 1000 unit before mounting it onto a wall or panel.
10BaseT Ethernet Cable	This cable connects the 10BaseT cable provided between the *10BaseT* port on the *i*.LON 1000 and an IP network port.
Null-Modem Cable	This cable connects the null-modem cable provided between the *Console* port on the *i*.LON 1000 and a terminal (or an available COM port on a PC running a terminal emulation program).
BLAT Mating Connector Plug	A two-position orange network connector for attachment to a LONWORKS twisted-pair channel. Weidmüller PN 148426.
BL Mating Connector Plug	A two-position black connector for power input. Weidmüller PN 125911.

Optional Accessories

i.LON 1000 accessories include a universal (100-240 VAC input) regulated 24VDC external power supply and 19-inch rack-mounting brackets, which can be purchased separately.

Table 2-2 Optional Accessories

Accessory	Model Number	Description
24VDC External Power Supply	72901-p (where p designates the style of power cord)	*i*.LON 1000 EXTERNAL POWER SUPPLY UNIT. Power Barrel Connector Specifications: ID=2.1mm, OD=5.5mm, L=11mm.
19" Rack Mount Brackets	72951	*i*.LON 1000 19" RACKMOUNT BRACKET ASSY

i.LON 1000 Internet Server Hardware

The *i*.LON 1000 is available in two versions, depending on the type of LONWORKS channel required. The model 72001 supports the TP/FT-10 free topology channel, while the model 72002 supports the TP/XF-1250 channel. All of the *i*.LON 1000 electronics are contained within a single metal enclosure, which provides a front panel power light emitting diode (LED) and rear panel electrical connections, status LEDs, and control switches. The *i*.LON 1000 may be desk, wall, or EIA 19-inch rack mounted. The enclosure is provided with rubber feet to prevent marring furniture when used on a desktop. Two keyhole slots are provided on the bottom of the enclosure for wall or panel mount applications. Optional mounting brackets

(model 72951) may be attached to each side of the *i*.LON 1000 enclosure for EIA 19-inch rack mounting in a single rack height space.

Figure 1.3 shows the rear panel of the *i*.LON 1000, including the connectors, LEDs, and control switches. The *i*.LON 1000 interfaces with the IP channel through a RJ-45 Ethernet 10BaseT port. The LONWORKS network connection (TP/FT-10 or TP/XF-1250) is effected by way of a removable screw terminal. DB-9 connectors are provided for the console and serial ports. The console port provides a serial connection to a VT-100 terminal or terminal emulation software such as HyperTerminal. The serial port is reserved for future use.

Ports, LEDs, Switches & Wiring Options

Figure 2-1 shows the rear panel of the *i*.LON 1000, including the connectors, LEDs, and control switches. Table 2.4 shows the operation of the control switches on the back panel of the *i*.LON 1000. Table 2-5 describes the LED functionality.

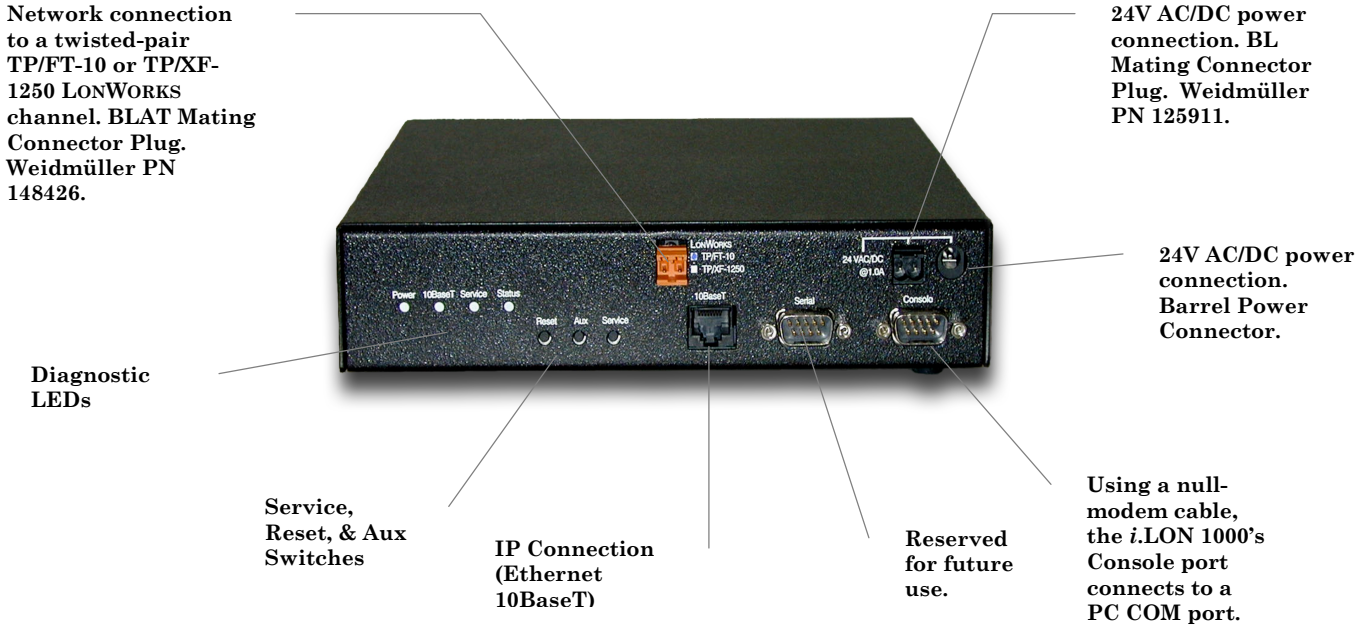


Figure 2-1 *i*.LON 1000 Back Panel

Input Power

The *i*.LON 1000 operates from low voltage 24VAC or DC at 1A. The *i*.LON 1000 may be powered by an optional Echelon 24VDC plug-in power supply (model 72901-p, where p identifies the type of power cord), a customer-supplied 24VAC or DC power supply, or a battery-backed 24VDC rechargeable power supply.

Two connector options are provided for powering the *i*.LON 1000: a 2.1mm barrel connector and a screw terminal connector. Both the barrel connector and the screw terminal connector are *polarity insensitive*. Use either the barrel connector or the screw terminals for input power - **DO NOT power the *i*.LON 1000 through one input power connector and then power another device using the *i*.LON 1000's other input power connector.**

Echelon's 72901 Power Supply includes a compatible 2.1mm barrel connector. Should a different power supply be used, ensure that the barrel connector meets the following specifications: ID=2.1mm, OD=5.5mm, L=11mm.

A black, two-position Weidmüller (PN 125911) BL screw terminal connector is also provided for those preferring to use screw connections. This screw terminal will accommodate wire gauges from 24AWG/0.5mm to 12AWG/2mm: ensure that the selected wire gauge can deliver the voltage and current required by the *i*.LON 1000, taking into account any voltage drop created by wire resistance.

Twisted Pair LONWORKS Network Connection

An orange, two-position Weidmüller PN 148426 BLAT screw terminal connector is provided for connection to the LONWORKS twisted-pair channel. The *i*.LON 1000 model 72001 supports the TP/FT-10 free topology channel, while model 72002 supports the TP/XF-1250 channel.

Suitable cables for LONWORKS channels are listed in Echelon's engineering bulletin, ***Junction Box and Wiring Guidelines***, part number 005-0023-01 (available from Echelon's web site at www.echelon.com).

Use ONLY cables that are listed in this bulletin. The use of unsuitable cables will result in improper network communications.

Ensure that the LONWORKS network is correctly terminated.

TCP/IP Connection

The *i*.LON 1000 connects to any TCP/IP network via the integral 10BaseT Ethernet port. *A standard category 5 Ethernet cable (provided) must be used to connect the i.LON 1000 to a 10BaseT hub*.

Console and Serial EIA-232 Ports

The console port is used to configure the *i*.LON 1000, and provides a serial connection to a VT-100 terminal or terminal emulation software such as HyperTerminal; the serial port is reserved for future use. The format of the console port data is 9600 baud, 8 data bits, 1 stop bit, no parity, and no flow control. *A null-modem cable (provided) is required between the i.LON 1000 and the communication port of the PC used for configuration*.

The cable connection of a null-modem cable is shown in Figure 2-2.

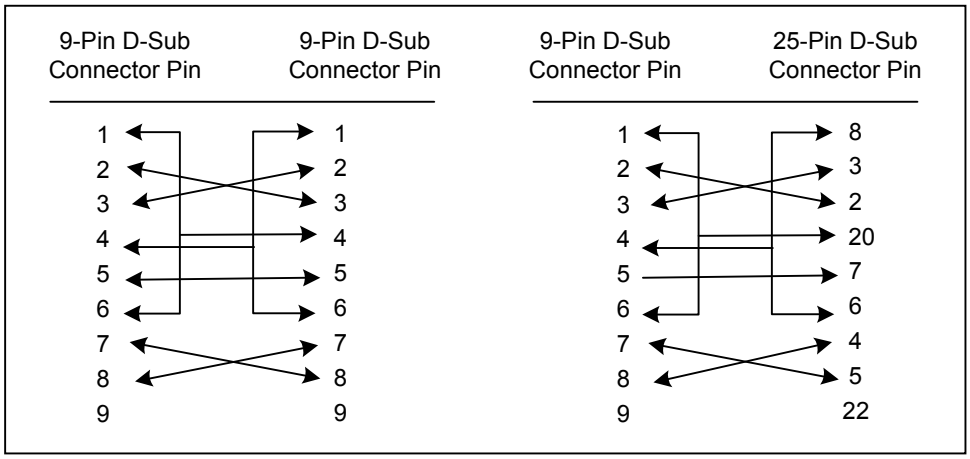


Figure 2-2 Null-Modem Connection for 9-pin and 25-pin Devices

The pinout of the *i*.LON 1000 DB-9 connector is shown in Table 2-3.

Table 2-3 *i*.LON 1000 Console Port DB-9 Pinout

Pin	Function
1, 4, 6, 7,8, 9	Unused
2	Rx
3	Tx
5	GND

Control Switches

Table 2-4 Control Switch Operation

Control Switch	Description
Reset	Resets the *i*.LON 1000 processor, causing it to boot.
Aux	Reserved for future use.
Service	Sends both the Web server and router service pin messages that contain the program ID and LONWORKS Unique ID (Neuron ID) for the nodes. Service pin messages are sent for active applications, only.

Diagnostic LEDs

Four back panel LEDs (Power, 10BaseT, Service, and Status) and one front panel LED (Power) indicate server and network status.

Front Panel LED

A single front panel LED illuminates when the *i*.LON 1000 is receiving power. The front panel power LED indicates that the power supply is active; it is not under software control.

Rear Panel LEDs

Rear panel LEDs provide diagnostic information about the state of the *i*.LON. Table 2-5 summarizes the meaning of the various states of this LED.

Table 2-5 LED Diagnostic Information

Rear Panel LED	Off	Green	Yellow	Blinks Yellow/Green	Blinks Yellow/Off
Power	No power has been applied.	Power applied; Hardware self-test completed successfully.	Power applied; Hardware self-test not yet completed or problem detected during power-up. Check status LED.	N/A	N/A
10BaseT	Ethernet cable not connected; or connected but not terminated at hub.	Ethernet link properly established.	N/A	N/A	N/A
Service	All LONWORKS applications are configured.	N/A	In boot process; or no LONWORKS applications exist.	N/A	Router and/or data server are created but not configured.
Status	No power has been applied.	Booted properly.	In process of booting.	Hardware self-test error. Check power LED. OR Booted but application software failed to start.*	N/A

*This happens if the *i*.LON does not have a valid IP address. 0.0.0.0 (the factory default) is not a valid address.

If all LEDs are off, either the *i*.LON 1000 does not have power or it did not complete the boot process.

i.LON 1000 Internet Server Mounting Options

The *i*.LON 1000 enclosure is designed to be mounted on a wall, in a standard EIA 19-inch rack, or placed on a level surface such as a table or desktop.

Caution! Install the *i*.LON 1000 unit in a room that is adequately ventilated. The operating temperature of the *i*.LON 1000 is 0 to +50 degrees Centigrade (10 to 90% relative humidity at 50 degrees Centigrade). Be certain that adequate ventilation is provided in the area or rack in which the *i*.LON 1000 is operated.

Wall Mount

Mount the *i*.LON 1000 unit on a wall or panel by placing the keyholes on the bottom of the unit over 2 screws installed into a secure wall or panel location as shown in Figure 2.3. Use the mounting template shipped with the *i*.LON 1000 to accurately measure the placement of the unit onto the wall or panel.

To wall mount the unit, follow these steps:

1. Remove the 4 rubber feet on the bottom of the *i*.LON 1000 by pushing up on the side of each foot.
2. Select a wall or panel location supported by a wood or metal stud. The wall or panel undersurface must support the screws and the weight of the *i*.LON 1000.
3. Install 2 screws (No. 8 panhead, 6.4 mm, or equivalent) into the wall or panel surface 5 inches (12.7 cm) apart. Screw height above the wall or panel surface should be approximately 0.25 inches (64 mm).
4. Place the keyholes on the bottom of the *i*.LON 1000 over the wall mounting screws. Push the *i*.LON 1000 toward the surface, then push down to secure the unit into place.

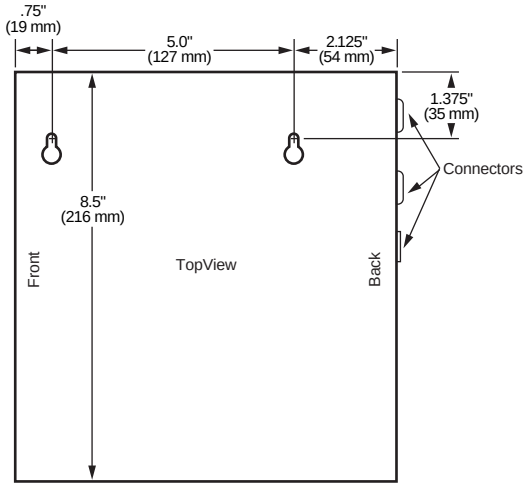


Figure 2-3 *i*.LON 1000 Wall-Mounting Dimensions

EIA 19-inch Rack Mount

Optional rack-mounting brackets are available for mounting the *i*.LON 1000 in a standard EIA 19-inch rack. The *i*.LON 1000 unit occupies 1U space in a standard EIA 19-inch rack. Refer to the following installation guidelines and instructions.

Rack-mounting Guidelines

The rack-mounting brackets (Model #72951) are used with most 19-inch equipment racks. Ensure access to the rear of the *i*.LON 1000 unit once it is mounted.

- Use all of the screws and brackets provided to secure the chassis to the rack posts.
- Install the unit in an open rack if possible.

- Never install the unit in an enclosed rack or room that is not adequately ventilated. Always ensure that the room or rack has sufficient ventilation to maintain the operating temperature range of the *i*.LON 1000.

Required Tools and Materials

- Set of rack-mounting brackets
- Screws (included with rack mount kit)
- Phillips screwdriver

To install the *i*.LON 1000 in the EIA 19-inch rack, follow these steps:

1. Remove all power and signal cables from the *i*.LON 1000.
2. Remove the 4 rubber feet on the bottom of the *i*.LON 1000 by pushing up on the side of each foot.
3. Align the holes on the short side of one bracket with the holes on the side of the *i*.LON 1000. Insert one of the small screws (4/40) into each hole and tighten with the screwdriver as shown in Figure 2-4.

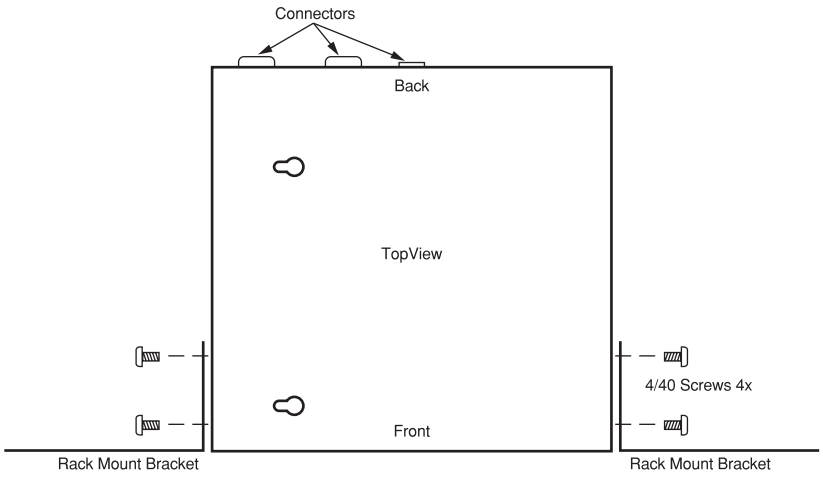


Figure 2-4 Connecting the *i*.LON 1000 Rack-mounting Brackets

4. Repeat step 3 above to attach the second bracket to the *i*.LON 1000 unit.
5. Install the *i*.LON 1000 in the rack as shown in Figure 2-5. Insert a large screw (10/32) in each bracket and tighten.

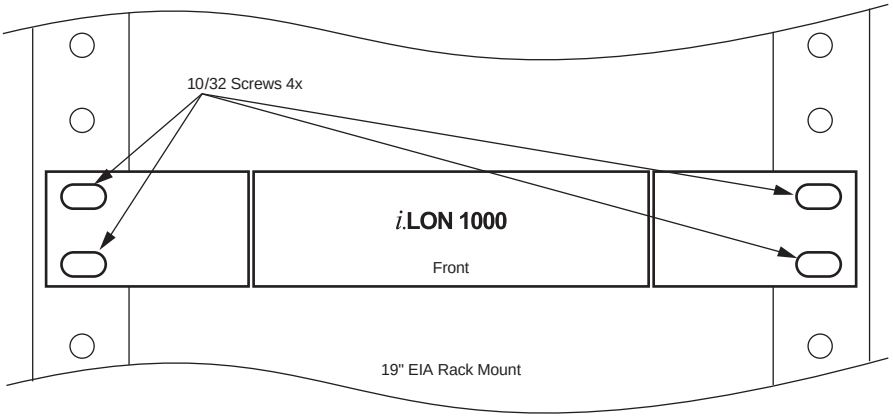


Figure 2-5 Installing the *i*.LON 1000 in the EIA 19-inch Rack

Figure 2-5 Installing the *i*.LON 1000 in the EIA 19-inch Rack

Applying Power and Installation Troubleshooting

Once the *i*.LON 1000 has been mounted and all wiring connected, apply power to the device. The Power LEDs on the front and rear panels should illuminate continuously. If the power LEDs do not illuminate, check that the power barrel connector or screw terminal, as appropriate, are properly seated, and that the power supply is receiving mains power. Also check the output voltage of the power to ensure that the wiring is not shorted, or too long to deliver 24V to the *i*.LON 1000.

Once the Power LEDs are illuminated, continue configuring the *i*.LON 1000 following the software configuration information in subsequent chapters. If at any point the *i*.LON 1000 does not respond as expected, use the LED diagnostic information in Table 2.5 (above) to isolate the problem.

Table 2.6 presents other common troubleshooting symptoms, and associated diagnoses, that may be encountered in the field. These problems might be interpreted as *i*.LON 1000-related, e.g., a malfunctioning *i*.LON 1000 router, when in fact the *i*.LON 1000 is only exhibiting the symptoms of a problem elsewhere in the LONWORKS or Ethernet network.

Table 2-6 – Network Troubleshooting Symptoms and Diagnoses

Symptom	Diagnosis
No LONWORKS communications	Network wiring not correctly connected to *i*.LON 1000. Ensure that the screw terminal connector is firmly seated and the wiring properly stripped of insulation and clamped by the connector screws.
	Network cabling shorted, open, or otherwise damaged. Use continuity meter to check cabling.
	Other network router(s) not commissioned, not powered, or otherwise not functioning correctly.
	Incorrect router channel type installed on channel.
	Inappropriately configured LONWORKS/IP Channel. See Chapters 5-7 for more information on setting up LONWORKS/IP Channels.
	Excessive IP latencies prevent LONWORKS/IP communication. See Chapter 8 for more information on LONWORKS/IP timing considerations.
Erratic or improper network communications	Network wiring not securely connected to screw terminals. The optimum tightening torque for the screw terminals is 4 lbs. in. (0.5Nm) maximum.
	Improper or missing network termination. A free topology TP/FT-10 channel requires one Model 44100 Terminator located anywhere on the channel. A bus topology TP/FT-10 channel requires two Model 44101 terminators, one at each end of the bus. A TP/XF-1250 channel only operates in a bus topology, and requires two Model 44200 Terminators, one at each end of the bus.
	Excessive network cabling. See Echelon's *FTT-10A Free Topology Transceiver User's Guide* (part number 078-0156-01) or *TPT Twisted Pair Transceiver User's Guide* (part number 078-0025-01) for a discussion of the maximum cable distances permissible on the TP/FT-10 and TP/XF-1250 channels. If the channel cabling is too long, install one or more LPR Routers in series with the network cabling.

	Improper network cabling. Suitable cables for the TP/FT-10 and TP/XF-1250 channels are listed in Echelon's engineering bulletin, *Junction Box and Wiring Guidelines*, part number 005-0023-01. In some cases it is possible to correct network communications by installing one or more LPR Routers in series with the network cabling. In other cases the cabling must be replaced with an approved cable.
	Excessive number of nodes on a channel. See Echelon's *FTT-10A Free Topology Transceiver User's Guide* (part number 078-0156-01) or *TPT Twisted Pair Transceiver User's Guide* (part number 078-0025-01) for a discussion of the number of devices that can be installed on a channel. If too many modules are on the channel, install one or more LPR Routers in series with the network cabling.
	Inappropriately configured LONWORKS/IP Channel. See Chapters 5-7 for more information on setting up LONWORKS/IP Channels
	Excessive IP latencies prevent LONWORKS/IP communication. See Chapter 8 for more information on LONWORKS/IP timing considerations.
Ethernet network down	Ensure connectivity to the Ethernet hub, make certain that the hub is powered, and test for the presence of IP packets on the Ethernet channel.

3

i.LON 1000 Software

This chapter describes the various software components within the *i*.LON 1000, and how to install the PC based software utilities.

i.LON 1000 Software and PC Utilities

The single *i*.LON 1000 Internet Server appears as two logical devices on a LONWORKS network: a LONWORKS router and a Web server. A network installation tool, such as the LonMaker™ Integration Tool, is generally used to define and commission the two logical devices. You may configure the *i*.LON 1000 as:

- A Router
- A Web Server
- A Router and Web Server

i.LON 1000 Applications

The *i*.LON 1000's software architecture enables several programs to execute at the same time on the *i*.LON 1000's processor. The *i*.LON 1000 applications include:

- Console Application
- Router
- Data Server
- Web Server

Console Application

The *i*.LON 1000 contains a console application that is accessed using a terminal emulator, such as HyperTerminal connected to the *i*.LON 1000's *Console* port. The Console Application is used to input basic parameters such as the *i*.LON 1000's IP address, subnet mask, and FTP user name and password. A complete description of this application is included in *Appendix A*.

Router Application

The *i*.LON 1000's router application allows IP to be used as a standard LONWORKS channel. Here, the term "router" is used to signify a LONWORKS router. From the LONWORKS perspective, the router application has all of the characteristics of a LONWORKS router with one side connected to a LONWORKS channel and the other side connected to a LONWORKS/IP channel. The router application can be configured as any of the 4 standard LONWORKS router types: learning, configured, repeater, or bridge.

The *i*.LON 1000 does not route IP packets. From the IP perspective, the *i*.LON 1000 is an IP host and must be configured like any other host on an IP network.

Data Server Application

The software component that provides anchor points on the *i*.LON 1000 to which network variables can be bound is called the *data server*. This application works in combination with the *i*.LON 1000's embedded Web server, allowing you to read and write to network variables from web pages using a standard web browser such as Netscape Navigator (versions 4.0 and higher), or Microsoft Internet Explorer (versions 4.0 and higher).

Web Server

The *i*.LON 1000's embedded Web server application combined with the data server application work together to serve web pages containing network variables to a standard web browser. The embedded Web and data server applications collectively are referred to as the *i*.LON 1000's *Web server*.

i.LON 1000 PC Utilities

The *i*.LON 1000 utility applications provided for the PC are:

- Configuration Server
- Web Tag Wizard
- Web Server Parameters Application

Configuration Server

The Configuration Server (commonly called the *Config Server*) is an application that creates and maintains LONWORKS/IP channels. The Configuration Server is described in Chapter 7. *Creating a LONWORKS/IP Channel.*

Web Tag Wizard

The Web Tag Wizard creates `<iLonWeb>` HTML tags used to monitor and control network variables in web pages that you create. The wizard steps you through the definition of each parameter necessary to build an HTML tag referring to network variables anywhere in your LONWORKS network.

See Chapter 10 for more information about the `<iLonWeb>` HTML tag.

Web Server Parameters Application

The *i*.LON 1000 Web Server Parameters application allows you to setup security profiles for combinations of users and web pages. This application is covered in Chapter 11, *i*.LON 1000 *Web Page Security*.

i.*LON 1000 Firmware*

The latest version of the *i*.LON 1000 firmware is included with the software. These files are placed in `LONWORKS\iLON\Images\iLON X.xx`, where `X.xx` is the major and minor version number. The directory structure is a duplicate of the directories contained by the *i*.LON 1000 device. If you receive an update of the *i*.LON 1000 firmware, you can update the firmware as described in *Updating the i.LON 1000 Firmware*, later in this chapter.

Installing the *i*.LON 1000 Software on Your PC

The *i*.LON 1000 software requires a PC having the following specifications:

- Microsoft Windows 95, 98, 2000 or NT 4.0 with Service Pack 3 or higher
- Pentium 133 or faster

- 20 MB available hard disk space for minimum configuration
- 48 MB RAM minimum (64 MB recommended) for Windows 95, 98
- 64 MB RAM minimum for Windows NT
- CD-ROM drive
- LonMaker Integration Tool version 2.0 or higher (Optional)
- LonMaker Credits (Optional)
- A terminal emulation program such as HyperTerminal for Windows
- 10 BaseT Ethernet connection with TCP/IP networking installed

The setup program on the *i*.LON 1000 CD will install the *i*.LON 1000 Software and Utilities. To install the software and utilities, follow these steps:

1. Insert the *i*.LON 1000 CD into the CD-ROM drive on the PC.
2. If the *i*.LON 1000 Setup program does not launch automatically, open the Windows Start menu and Select Run. Click OK to run setup.exe on the CD drive. The *i*.LON 1000 Setup window appears and prompts you through installing the PC software and utilities.

Updating the *i*.LON 1000 Firmware

New versions of the *i*.LON firmware may become available on Echelon's web site. To update your *i*.LON hardware with a new firmware version, follow these steps:

1. Download the firmware update to your PC. It is recommended that the update be placed in `LONWORKS\iLON\Images\iLON X.xx`, where `X.xx` is the major and minor version number (the setup program will place the firmware update in this location by default).
2. If the *i*.LON 1000 is currently serving a web site (see Chapter 9), be sure that you have a current back up of all the pages it serves.
3. Upload all the files in the new `LONWORKS\iLON\Images\iLON X.xx` directory to the *i*.LON 1000's flash disk using a standard FTP program. Overwrite any existing files of the same name, maintaining the directory structure that was created when `setup.exe` was run.

4

Using the *i*.LON 1000 Console Application

Before an *i*.LON 1000 can be added to a LONWORKS/IP channel (described Chapters 5-7), basic parameters on the *i*.LON 1000 must be set. At a minimum, the IP address and subnet mask for each *i*.LON 1000 must be specified. The *Console Application*, a built-in application that accepts commands in a manner similar to DOS or UNIX, is used to set the parameters in the *i*.LON 1000.

Setting Up the *i*.LON 1000's IP Information

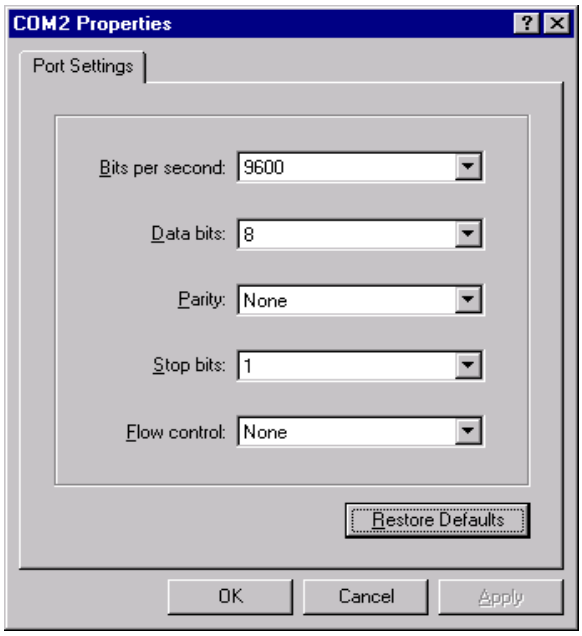
Before an *i*.LON 1000 can be added to a LONWORKS/IP channel (see Chapters 5-7 for more information about LONWORKS/IP channels), basic parameters on the *i*.LON 1000 must be set. At a minimum, the IP address and subnet mask for each *i*.LON 1000 must be specified. The *Console Application*, a built-in application that accepts commands in a manner similar to DOS or UNIX, is used to set the parameters in the *i*.LON 1000.

To set up the *i*.LON 1000 using the Console Application, follow these steps:

1. Connect a PC COM port to the *i*.LON 1000 **Console** port using the null-modem cable that came with your *i*.LON 1000.

   Connect to the Console Application using a VT-100 terminal emulation program such as HyperTerminal. (If using HyperTerminal, set the function, arrow, and control keys to work as Windows keys in Properties/Settings.)

2. Use the port settings shown in the following figure:



   Press the **Enter** key and the *i*.LON 1000 system prompt appears indicating that you have connected.

   ```
   iLON>
   ```

3. Issue the following console commands at the command prompt to set the IP properties of the *i*.LON 1000. Make sure that a static, unique IP address is selected for each *i*.LON 1000 and that the address scheme chosen is valid for the local IP network. See your network administrator if you need help deciding on proper values for the IP settings.

   The syntax for console commands is: **command** *argument*

   ipaddress *address* Sets/Modifies the IP address

   ```
   ipaddress 10.1.0.170
   ```

subnetmask *address*	Sets/Modifies the subnet mask `subnetmask 255.255.255.0`
hostname *name*	Sets/Modifies the host name of the *i*.LON 1000 `hostname myilon`
gateway *address*	Sets/Modifies the gateway address `gateway 10.1.0.1`
ftpuser *name*	Sets/Modifies the FTP user name `ftpuser user1` (Anonymous FTP is not supported.)
ftppassword *password*	Sets/Modifies the FTP password `ftpuser gh5bug`

4. Type **show** at the command line to display the *i*.LON 1000 properties. Verify that the property changes you made to the *i*.LON 1000 are correct. For example:

```
iLON> show

Software Version:   1.01.00
IP Address:         10.1.0.170
Subnet Mask:        255.255.255.0
Host Name:          iLON
Gateway:            10.1.0.1
DHCP:               off
MAC ID:             00-D0-71-00-00-26
LonTalk Unique IDs: 80:00:00:00:12:60 through 80:00:00:00:12:6F
LonTalk Xcvr ID:    TP/FT-10
LonTalk IP Port:    1628
Config Server:      10.1.0.139 (1628)
Authentication:     off
SNTP Servers:       0.0.0.0 (123); 0.0.0.0 (123)
SNTP Synchronized:  no
```

5. Type **reboot** at the command line to reboot the *i*.LON 1000 and apply the property settings.

6. Repeat steps 3 - 5 to configure each *i*.LON 1000.

   Type **help** at the command prompt at any time, or see Appendix A, *Console Application*, for a complete list of console commands.

5

LONWORKS/IP Channels Background & Definition

Traditionally LONWORKS networks operate over dedicated twisted pair wiring. A given segment of wire is referred to as a channel. With the introduction of LNS 3.01 and the i.LON 1000, a new kind of channel has been created, the LONWORKS /IP channel. This chapter provides an overview of the LONWORKS/IP Channel.

Introduction to the LONWORKS/IP Channel

Unlike traditional channels that can easily be identified by tracing a physical wire, a LONWORKS/IP channel is not defined by a physical connection, but a group of IP addresses. These addresses form a "virtual" wire. *i*.LON 1000s and PCs running LNS (version 3.01 or better) use this virtual wire in the same way as traditional dedicated twisted pair wiring.

The concept is similar to a Virtual Private Network (VPN). Each *i*.LON 1000 in the system is aware of its peers and each *i*.LON 1000 keeps peer information in its routing tables so that it can subsequently determine to which IP address a "tunneled" LONWORKS packet should be forwarded. Consider Figure 5-1.

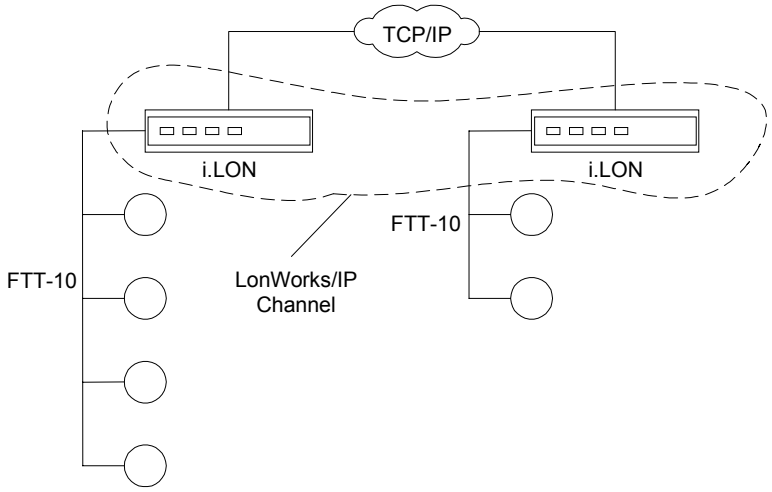


Figure 5-1 – A LONWORKS/IP Channel

The TCP/IP channel may be a single wire carrying TCP/IP packets, or it could be the Internet. Because a virtual wire is created by the *i*.LON 1000s, Figure 5-1 topology is logically no different than Figure 5-2.

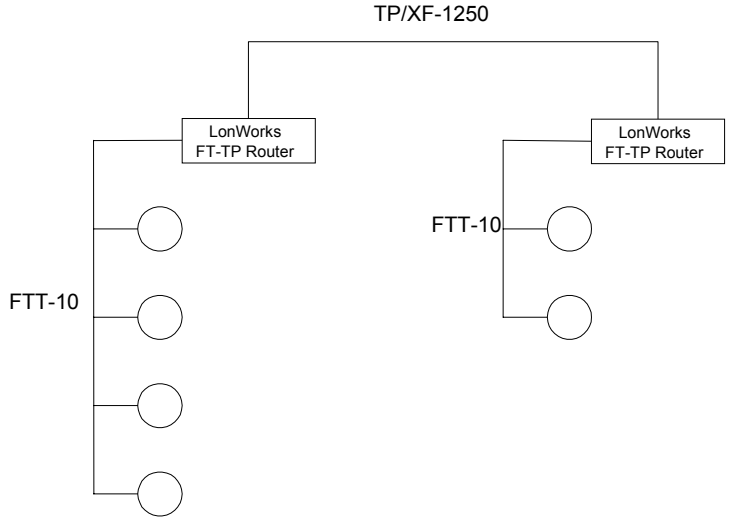


Figure 5-2 – A LonWorks Network with no LONWORKS/IP Channel

The *i*.LON 1000s work together to simulate a wire. The *i*.LON 1000 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 the scenario diagramed above, a PC running LNS 2.0 could be attached to either of the FTT-10 channels.

PCs running LNS 3.01 incorporate the same routing intelligence as the *i*.LON 1000; therefore, PCs running LNS version 3.01 or better can be directly connected to the IP network and communicate with LONWORKS devices on the other side of any *i*.LON 1000. This allows topologies such as that shown in Figure 5-3:

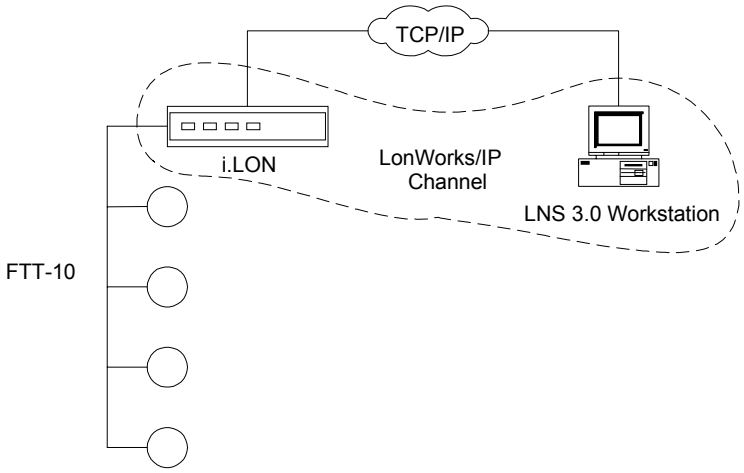


Figure 5-3 – *i*.LON 1000 and LNS 3 Workstation on a LONWORKS/IP Channel

A complete installation may contain many *i*.LON 1000s and PCs – all sharing a LONWORKS/IP channel. Because the LONWORKS /IP channel may be any IP network, a system may now span the entire globe as easily as it once spanned a single building, as shown in Figure 5-4.

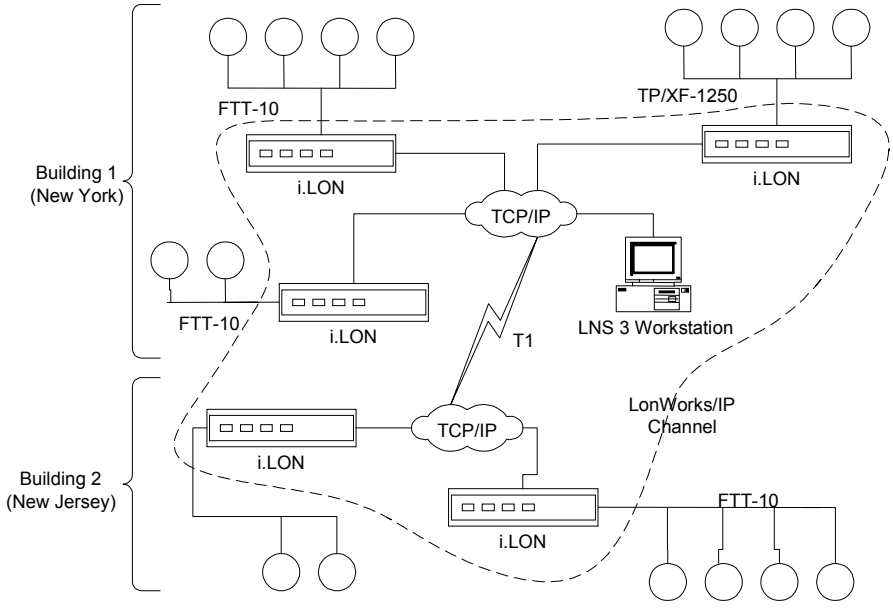


Figure 5-4 – Large LONWORKS Network using a LONWORKS/IP Channel

Note: A LONWORKS/IP channel may contain at most 40 devices. If your installation requires more than 40 LONWORKS/IP devices, you must create multiple LONWORKS/IP channels.

6

IP Resources Required to Create LONWORKS/IP Channels

To install *i*.LON 1000 Internet Servers on an existing IP network, you will need to work closely with the IP network administrator. This section provides a list of the resources you will need to get from the network administrator, and information they will need to adjust any intervening firewalls to allow bi-directional communication with the outside world.

Information/Resources to be Acquired From Network Administrator

To install one or more *i*.LON 1000 Internet Servers on an existing IP network, you must obtain the following information and resources from the network administrator:

- A static, unique IP address and subnet mask for each of the *i*.LON 1000s and the Configuration Server to be connected to the internal IP infrastructure. (The Configuration Server is an application used to define LONWORKS/IP channels; it runs on a PC and requires a single static IP address) You will also need a static IP address for all PCs running LNS (version 3.01 or better) that are connected to the internal IP infrastructure. Additionally, if any PC is to be connected to the Internet, you will need a gateway address and optionally a host name along with the IP address of an appropriate DNS machine.

  When exchanging messages with the Configuration Server and other devices on the LONWORKS/IP channel, the *i*.LON 1000 protocol requires that each device's IP address remain static so it can identify other members of the LONWORKS/IP channel. Using NAT (Network Address Translation) or DHCP without static reservations is incompatible with LONWORKS/IP channels. The *i*.LON 1000 cannot make use of address resolution services such as DNS to re-establish members of a LONWORKS/IP channel when underlying IP addresses change.

  If DHCP will be used to retrieve the IP information for the *i*.LON 1000, 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 might need to create individual static address reservations for each *i*.LON 1000. See *Using DHCP with i.LON 1000* devices in Chapter 12 for more information.

- If any machine is to be referred to externally by its host name (www.myilon.echelon.com for example), you should ask to have the host name added to the Internet domain's zone file. Alternately, you can use host file entries in each machine that needs name resolution, thus avoiding the need to modify the zone file. On a Windows 95/98 machine the host file (host.sam) is typically located in the C:\Windows folder. You must rename it hosts.sam before editing it. On a Windows NT or 2000 machine, the hosts file is typically located in the C:\Winnt\System32\drivers\etc folder. (See your Microsoft Windows documentation for more information on modifying Windows host files.)
- If the LONWORKS/IP channel is to include the Internet (or excessive internal propagation delays will be involved) you will need the address of an SNTP server.

  Use a table similar to the one below to plan your installation (* = optional information):

Device	IP address	Port **	Subnet Mask	Gateway*	Host Name*	Host Name Reg. Req'd	DNS Machine*	SNTP Server*
Config Server PC		1629						
LNS 3 PC		1628						
i.LONs 1-n		1628						

** The port number should taken from the Configuration Server's database

Firewall/Router Configuration Information to be Supplied to the Network Administrator

If any *i*.LON 1000 or PC running LNS 3.01 is to be connected to the Internet (temporarily or permanently), adjustments to the local firewall/router may be required. These adjustments must be made for LONWORKS/IP channels, HTTP access to *i*.LON 1000s, and supporting protocols such as FTP.

WARNING: The IP address of members within a LONWORKS /IP channel must remain static. Addresses may not be translated using Network Address Translation (NAT). The firewall should be configured to make the internal members of the channel transparent to the outside world.

Inspect the table below to determine how the firewall/router needs to be opened up and request the changes from the network administrator. It is advisable to restrict access to source/destination IP groupings rather than open up global Internet access to internal members of a LONWORKS /IP channel. In the table, a member of a LONWORKS/IP channel may be an *i*.LON 1000, a Configuration Server, an LNS Server (version 3.01 or better) or Full Client using an Ethernet connection.

Depending on available IP addresses and your security requirements, it may be possible to locate devices on the dirty side of a firewall, i.e. between the firewall and the serial feed to the ISP. This will avoid any firewall configuration issues at the expense of security.

If an *i*.LON 1000 is to serve web pages to the Internet (described in Chapters 9 and 10), remember to set up access permissions using the *i*.LON 1000 Web Server Parameters utility.

Configuration for LONWORKS/IP Channels						
Condition	Direction	Target IP	Source IP	Protocol	Target Port	Source Port
LONWORKS/IP channel with external members	In	All internal members of the channel	All the external members of the channel	UDP	See Note, below	See Note, below
LONWORKS/IP channel with external members	Out	All the external members of the channel	All internal members of the channel	UDP	See Note, below	See Note, below

Internal SNTP server with external clients	In	The internal SNTP server	All the external members of the channel using the SNTP server	SNTP (UDP)	123	1024-65535
External SNTP server with internal clients	Out	The external SNTP server	All the internal members of the channel using the SNTP server	SNTP (UDP)	123	1024-65535

Note: Traffic in a LONWORKS/IP channel is sent between the members defined in the Configuration Server's database. If for example an *i*.LON 1000 using IP address 10.1.0.10 (*i*.LON 1000s always use port 1628) initiates communication with a Ethernet Iinterface on a PC at IP address 10.1.0.11 that has been configured to use port 1629, the target IP address would be 10.1.0.11 with a target port of 1629 with a source IP address of 10.1.0.10 and a source port of 1628. The source port of a LONWORKS /IP channel member will always be static and will use the port as defined in the device's property listing in the Configuration Server's database.

Configuration for *i*.LON 1000 Web Servers						
Condition	Direction	Target IP	Source IP	Protocol	Target Port	Source Port
Internal *i*.LON 1000 Web Server with external HTTP clients	In	The internal *i*.LON 1000	The external HTTP client	HTTP (TCP)	80	1024-65535

Configuration for *i*.LON 1000 Maintenance						
Condition	Direction	Target IP	Source IP	Protocol	Target Port	Source Port
Internal *i*.LON 1000 with external FTP access	In	The internal *i*.LON 1000	The external FTP client	FTP (TCP)	20 & 21	1024-65535

External *i*.LON 1000 internal FTP client	Out	The external *i*.LON 1000	The internal FTP client	FTP (TCP)	20 & 21	1024-65535

Configuration for LONWORKS/IP Channel Testing						
Condition	Direction	Target IP	Source IP	Protocol	Target Port	Source Port
Ping	In	All internal members of the LONWORKS /IP channel	All external members of the LONWORKS/IP channel	PING (ICMP echo request & echo reply)	N/A	N/A
Ping	Out	All external members of the LONWORKS /IP channel	All internal members of the LONWORKS /IP channel	PING (ICMP echo request & echo reply)	N/A	N/A
Traceroute	In	All internal members of the LONWORKS /IP channel	All external members of the LONWORKS /IP channel	TRACEROUTE (ICMP echo request & echo reply)	N/A	N/A
Traceroute	Out	All external members of the LONWORKS /IP channel	All internal members of the LONWORKS /IP channel	TRACEROUTE (ICMP echo request & echo reply)	N/A	N/A

7

Creating a LONWORKS/IP Channel

This chapter describes how to establish a LONWORKS/IP channel including instructions for setting up networks, channels, and devices using the Configuration Server, and defining and testing the *i*.LON 1000 as a standard LONWORKS router using the LonMaker Integration Tool. The Configuration Server is installed with the *i*.LON 1000 software, so before proceeding, install the *i*.LON 1000 software as described in Chapter 3.

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 1000 or a PC running LNS 3.01 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 1000s using the *i*.LON console application as described in Chapter 4.
2. Ensure that the Configuration Server PC can communicate with each *i*.LON 1000 or PC running LNS 3.01 by pinging each *i*.LON 1000 and LNS 3.01 PC.
3. If the LONWORKS/IP channel will contain only *i*.LON 1000 devices, skip to step 7. If the LONWORKS/IP channel will contain one or more PCs running LNS 3.01, open the Windows control panel on the PC and run the *LONWORKS/IP Channels* control panel. This control panel appears in Figure 7-1:

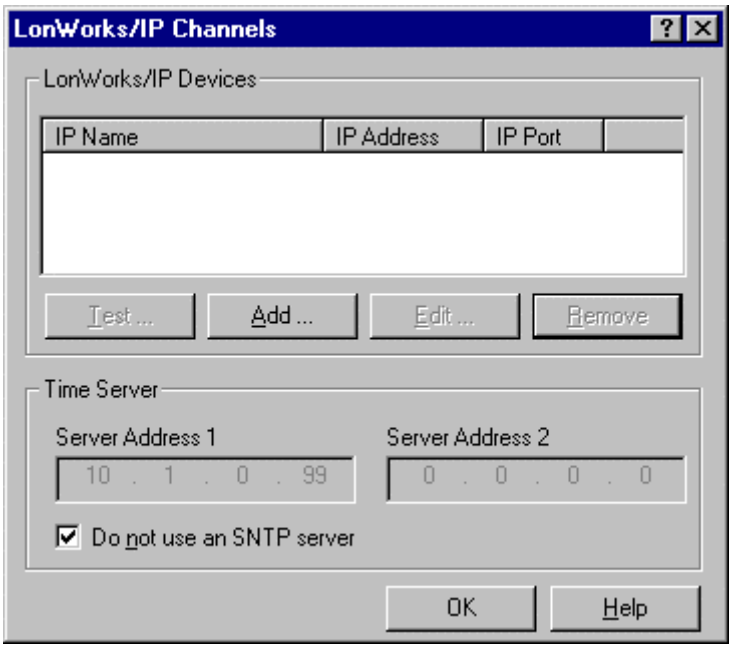


Figure 7-1 LONWORKS/IP Channels Control Panel

4. Click the **Add** button to add a LONWORKS/IP interface to the PC. The dialog shown in Figure 7-2 appears:

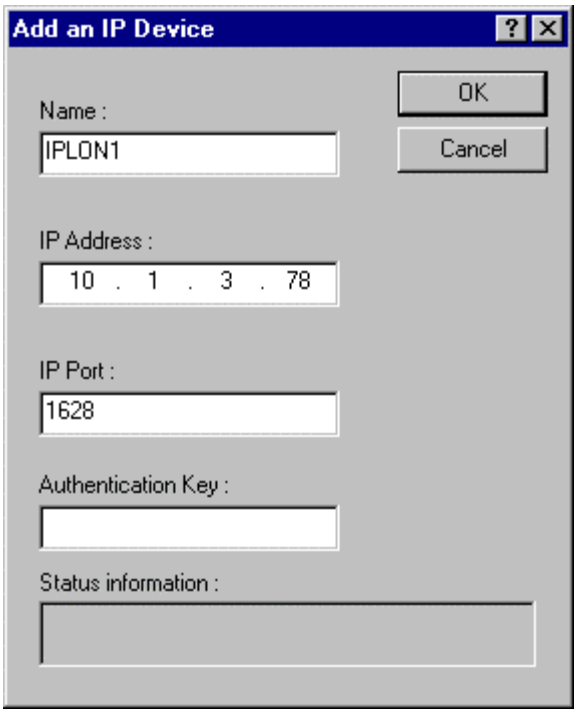


Figure 7-2 Add LONWORKS/IP Device Dialog

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 IP device of the PC (if the PC has multiple Ethernet cards with different IP addresses, you may choose between them).
IP Port	The port that the LONWORKS/IP device will use on the LNS 3.01 PC. By default, this is 1628.
Authentication Key	If the IP channel will be set up to use MD5 authentication, enter the 16 character hexadecimal authentication key in this field.

6. Click OK. The control panel will now look as shown in Figure 7-3:

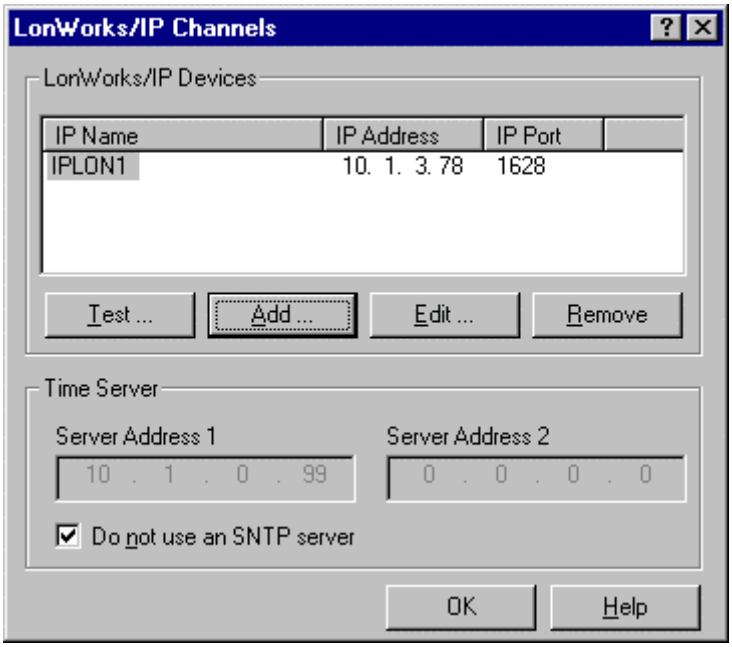


Figure 7-3 LONWORKS/IP Channels Control Panel

7. Start the Configuration Server application. From the Windows desktop click on Start, choose Programs, select Echelon *i*.LON 1000, and click on *i*.LON 1000 Configuration Server. The Configuration Server main dialog appears:

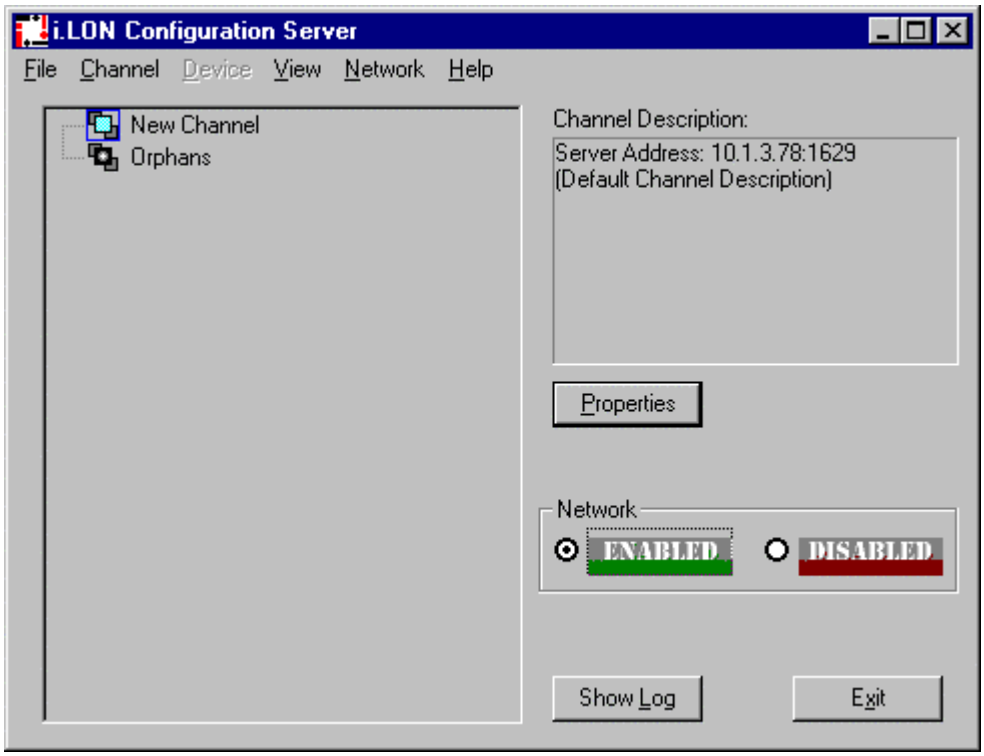


Figure 7-4 *i*.LON 1000 Configuration Server

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

8. 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.

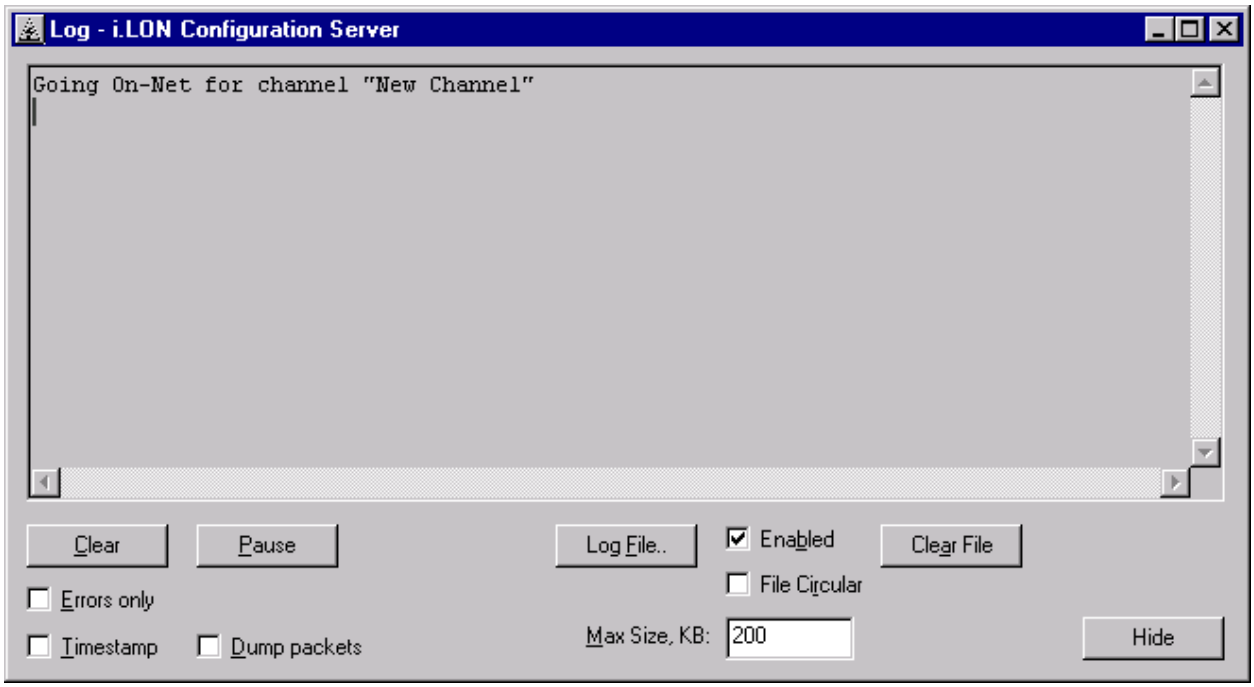


Figure 7-5 *i*.LON 1000 Configuration Server Log

9. Verify that the Configuration Server is attached to your IP network. The **Enabled** radio button on the main Configuration Server dialog (Figure 7-4) should be selected, and the Configuration Server should correctly detect the IP address of your PC. 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 listed in the Host IP Address window. The Host IP address(es) are the available IP addresses to which you may set your network channels. On the Configuration Server main dialog screen in step 7, the New Channel's Server Address is set to 10.1.3.78, 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 channel.

10. 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 Chapter 7 for more information on how to specify SNTP servers. See Chapter 8 for additional information on adjusting channel property settings.

11. From the Configuration Server main dialog, right-click on the new channel (by default, **New Channel)**, and select **New Device**. A new element representing a LONWORKS/IP device is added to the channel. This device could be either an *i*.LON 1000 or a LONWORKS/IP device on a PC running LNS 3.01 or higher. Each channel may contain up to 40 devices. Enter a descriptive name for the new device and press **Enter**. The device dialog appears.

Figure 7-6 *i*.LON 1000 Console Application: Address Tab

12. Enter the **IP Address** of the LONWORKS/IP device. If the device is an *i*.LON 1000, this IP address is the same address that you assigned to the *i*.LON 1000 using the Console Application (see Chapter 4). If the device is on a PC running LNS, this is the IP address specified when the LONWORKS/IP device was added (see steps 4-6, earlier in this section). Be sure that the Port matches the port of the LONWORKS/IP device (1628 by default for *i*.LON 1000s and LONWORKS/IP devices on PCs running LNS 3.01 or higher).

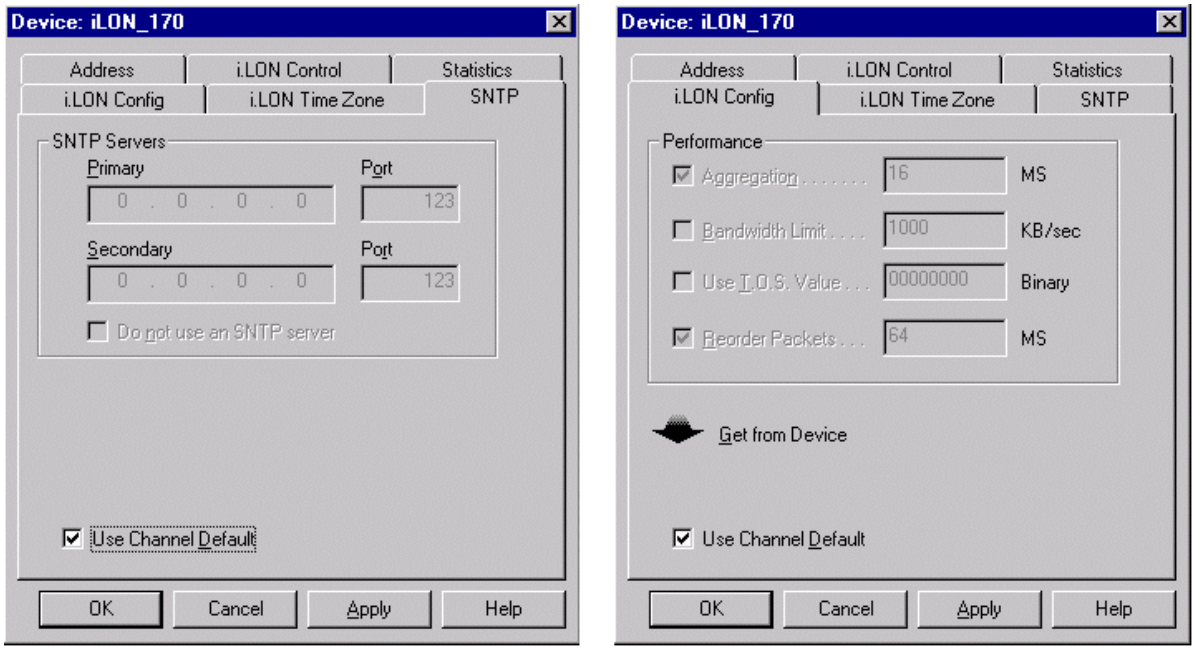


Figure 7-7 *i*.LON 1000 Console Application: SNTP and ***i*.LON 1000** Config Tabs

13. Select the **Use Channel Default** checkboxes on the **SNTP** and **i.LON Config** tabs. Set the time zone to correspond with the geographical area of the device. Click **Apply**.

14. Repeat steps 11-13 for each device. As each LONWORKS/IP device is added to the LONWORKS/IP channel, 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.

15. 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, open the LONWORKS/IP Channels control panel and click the **Test** button as shown in Figure 7-8.

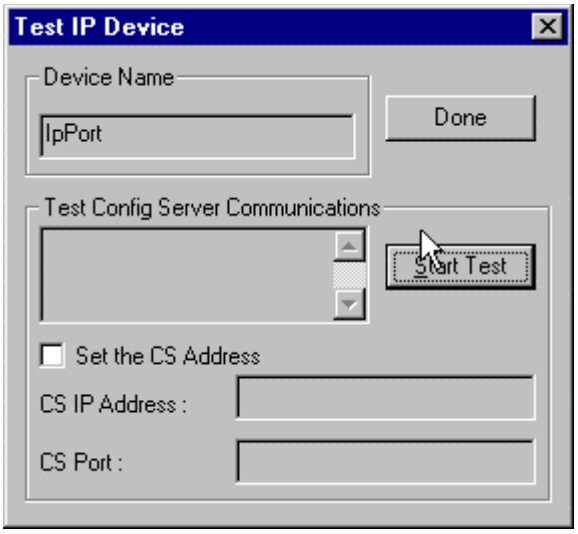


Figure 7-8 Test IP Device Dialog

16. Click **Start Test** to open the LONWORKS/IP device on the PC and allow the Configuration Server to find it. If you still have problems, select the **Set the CS Address** option and enter the Configuration Server's IP address and click the button again (it will now be labeled **ReTest**).

17. From the main dialog, select **Commission Members** from the **Channel** menu. This will attempt to configure all LONWORKS/IP devices that are listed under the selected channel entry.

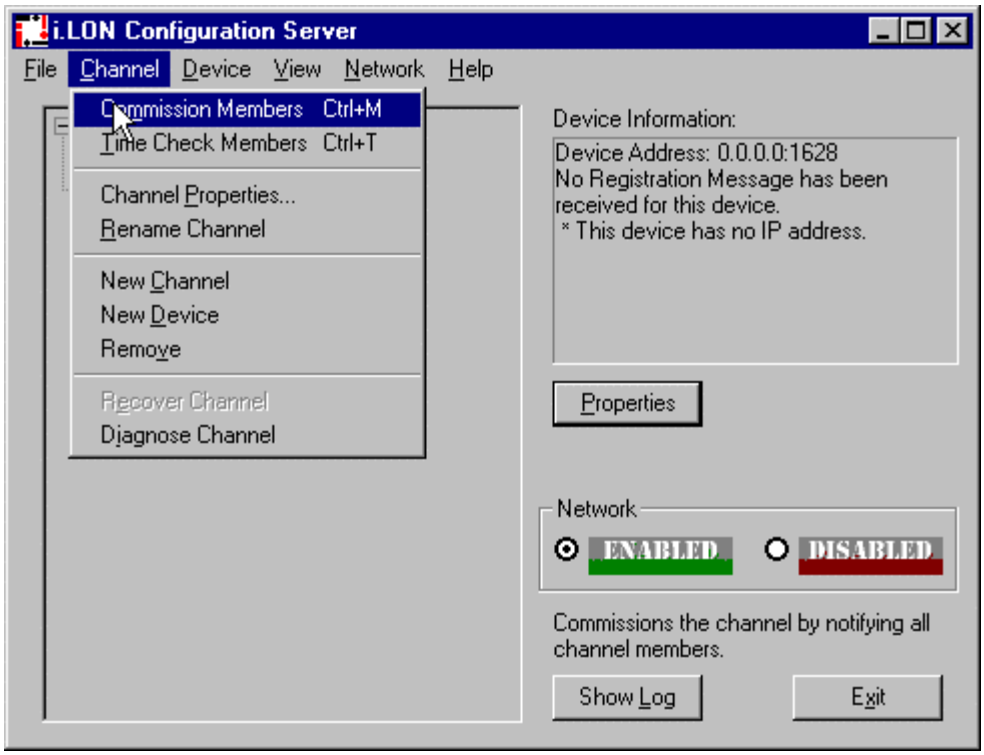


Figure 7-9 Configuration Server: Commission Members

When you select **Commission Members,** a communication process starts between the Configuration Server and members of the targeted channel. The process begins with a "Request for Device Registration" message to all members of the selected channel from the Configuration Server. Each member responds to the Configuration Server with a Device Registration message. The Configuration Server receives the messages, fills in device configuration information such as the Configuration Server's IP address, SNTP information, and the date/time of the current Channel Membership information, and sends Device Configuration messages back to the devices. The devices update their configuration information. Each device also checks the Channel Membership date/time included in the Device Configuration message. Based on this date and time, devices determine whether more recent Channel Membership information is available. If so, the devices request the new information and the Configuration Server provides it. When devices receive a Channel Membership message, they compare Channel Routing date/times stored in that message against similar information that they store about other devices in the channel. If any information is outdated, the devices request updated information from the Configuration Server.

Success or failure of this step is reflected in the Configuration Server Log screen, and by the color of the devices in the tree view on the main dialog. The color of the device reflects its current status, as shown in Table 7-1:

Table 7-1 – Device Status Indicator

Color	**Status Description**
Cyan	Normal, but 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. Usually, this occurs when no response is received from a device to which a request was made.
Yellow	Normal, but the Time Check failed for this device.
Red/White	Device is disabled.

Important: Leave the Configuration Server running. It must be running when you configure LONWORKS/IP devices using a LONWORKS network management tool.

The steps above create a "virtual wire" out of any group of IP addresses. The members of this group can now share information seamlessly, and appear as a standard LONWORKS channel to the LONWORKS network. In the following section we describe how to use the LonMaker™ Integration Tool to bind two nodes together across this new "virtual" wire. If you're experienced with connecting LONWORKS devices together, you'll notice that the procedure below is exactly the same as if we were using standard LONWORKS routers.

Designing a LonMaker Network Containing LONWORKS/IP Channels

The *i*.LON 1000's router application allows you to connect a LONWORKS channel to a LONWORKS/IP channel for transporting LONWORKS data packets over IP. Once the LONWORKS/IP channel is established (as described in the previous section), you should define the *i*.LON 1000 devices using a network installation tool such as the LonMaker Integration Tool (version 2.0 or higher). This will allow information to pass from the LONWORKS/IP channel to the LONWORKS channel on the other side of the *i*.LON 1000 router.

Figure 7-10 shows an example of a LONWORKS network which 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 as well (i.e. it could be connected to the IP channel rather than the FTT-10 channel).

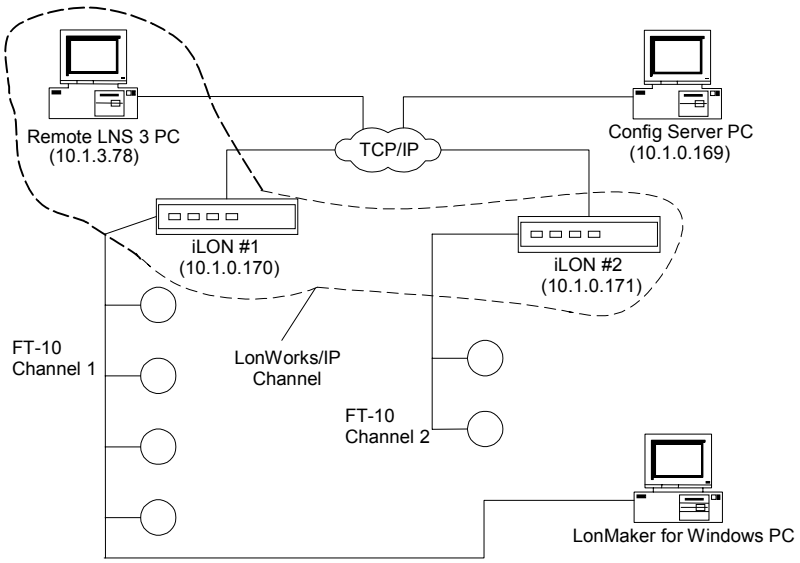


Figure 7-10 Typical Network Containing a LONWORKS/IP Channel

Defining an i.LON 1000 as a LONWORKS Router

The following example illustrates how to create the LONWORKS network described in Figure 7-10 using the LonMaker Integration Tool. Figure 7-11 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 1000s as routers on a LONWORKS network, 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.
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* (*iLON #1*) and one connecting *IP Channel* to *FT-10 Channel 2* (*iLON #2).* Follow the LonMaker convention: *Channel A* of a router is the side closest to the LNS Network Interface. *Channel A* of *iLON #1* is attached to *FT-10 Channel 1* and *Channel B* is attached to *IP Channel*; *Channel A* of *iLON #2* is attached to *IP Channel*, and *Channel B* is attached to *FT-10 Channel 2*.
4. Commission the *i*.LON 1000 Routers and leave them in the Online state.
5. If your IP network contains large latencies, change the network timing properties as described in Chapter 9.

Be sure the Configuration Server utility is running when you commission the *i*.LON 1000 routers.

Once the *i*.LON 1000s have been installed and commissioned, you can create 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 7-11 shows the network

described above with a *DI-10 LonPoint* device added to *FT-10 Channel 2*, and one of the digital output network variables from the DI-10 device bound to the *LNS Network Interface*.

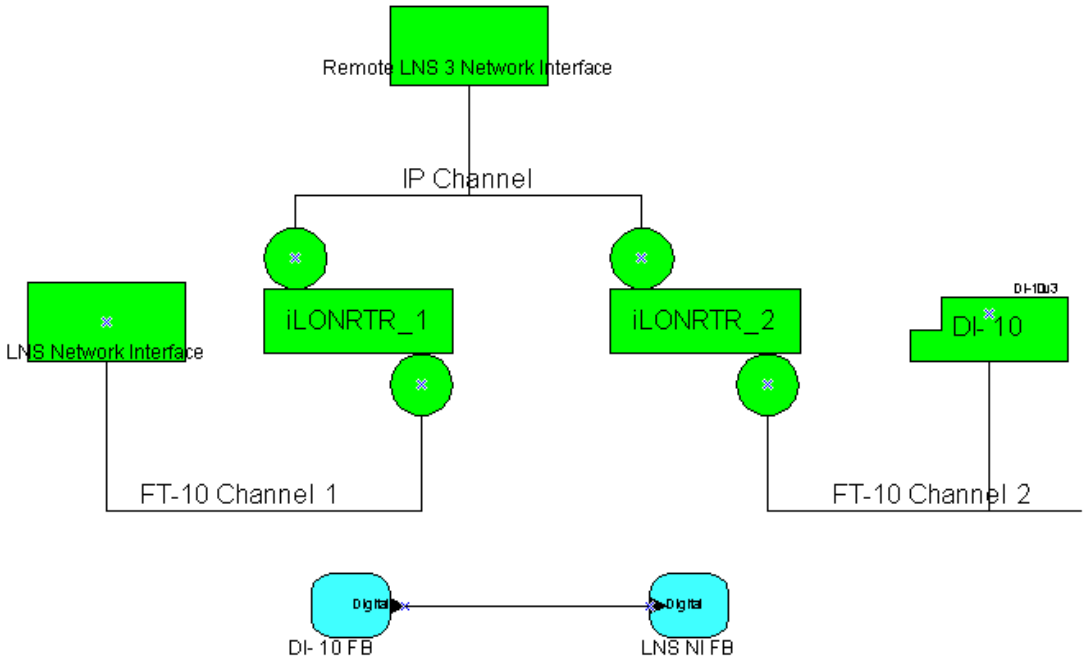


Figure 7-11 *i*.LON 1000 Routers Configured on a LONWORKS Network

Verifying Router Functionality

To verify that the *i*.LON 1000 Routers in the network shown in Figure 7-11 are working correctly, follow these steps:

1. Right-click on the network variable connection between DI-10 FB and LNS NI FB 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 FB*.
2. If you fail to see network variable updates reported by LonMaker, there is a problem. Refer to Table 7-2 for troubleshooting information.

Table 7-2 – Troubleshooting the *i*.LON 1000 Router

Symptom	**Probable Cause**	**Corrective Action**
No service pin message is received from the near router (*i*LON #1 in Figure 7-11).	There is a problem with network connectivity, or the network interface 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.
	The *i*.LON 1000 may not be physically connected to the network interface	Check the network wiring between the PC and the *i*LON 1000.
	No IP address has been assigned to the *i*.LON 1000.	Configure the IP address in the Console Application and Configuration Server.

	The router application has not yet been created on the *i*.LON 1000.	Create the LONWORKS router application using the Console Application.
The near router (*i*LON #1) commissions successfully, but no service pin message is received from the far router (*i*LON #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 1000 routers. Verify that the near router is online and that the Configuration Server reports connectivity among all members of the LONWORKS/IP channel.
Both *i*.LON 1000 routers commission successfully, but the device on the far side of *i*LON #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, so the problem must reside with the device being installed. If no test succeeds, verify connectivity between the *i*.LON 1000 devices in the main dialog status window of the Configuration Server.
A device (*i*.LON 1000) added to a LONWORKS/IP channel using the Configuration Server remains red in the device tree.	The Configuration Server is not able to communicate with the *i*.LON 1000 on the defined LONWORKS/IP channel.	Verify that the PC running the Configuration Server can ping the *i*.LON 1000. Make sure that you attached side A and side B of the *i*.LON 1000 to the correct channels. 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 *i*.LON 1000 Console Application.
The *i*.LON 1000 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.	Ask your IT department if the two *i*.LON 1000 devices are on different sides of a firewall, on a NAT box, or on a router that translates IP addresses. Make sure that the IP address of the target *i*.LON 1000 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.

8

LONWORKS/IP Channel Timing Considerations

This is an advanced topic which is only required when using *i*.LON 1000s in layer 3 routing mode over IP networks with unusually large latencies such as the Internet. This information does not apply to the *i*.LON 1000's web server. In networks where the layer 3 routing function is contained within a local LAN, you may safely ignore this chapter and use the Configuration Server default for the LONWORKS/IP channel configuration.

LONWORKS/IP Channel Timing Considerations

When designing a LONWORKS/IP channel over an IP network which might have a large latency, such as the Internet, it is important to be aware the relationship between the 3 timing parameters that can be set when configuring a network to send packets across the IP network. 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 8.1 specifies how to approximate the timing values for network implementations using the Internet.

Table 8.1 – Timing Parameter Calculations for Internet LONWORKS/IP Channels

Timing Parameter	**Set to:**
Channel Timeout	(Average Ping Delay / 2) + 20%
Packet Reorder Timer	The lesser of: ¼ of Channel Timeout Value, or 64 MS
LonMaker Channel Delay	Average Ping Delay + 10%

If using aggregation (see *Aggregation* in Chapter 12), 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 1000 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 delay. Synchronize the *i*.LON 1000 routers with a SNTP time server.

Set the Channel Timeout parameter to a value in relation with the ping delay as indicated in the table 7.1. 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. As a guideline, 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:

1. The delay can vary on each leg of a round trip. Your timeout parameter should factor the maximum delay into one leg of the trip.

2. The 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 receiving LONWORKS/IP device compares the stamp to its own time. If the time has expired, (i.e., (time of device – time stamp in packet) > channel timeout)), the IP packet is discarded by the receiving 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 the channel Time Check command is issued.

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 a 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 a 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 3 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 8-1.

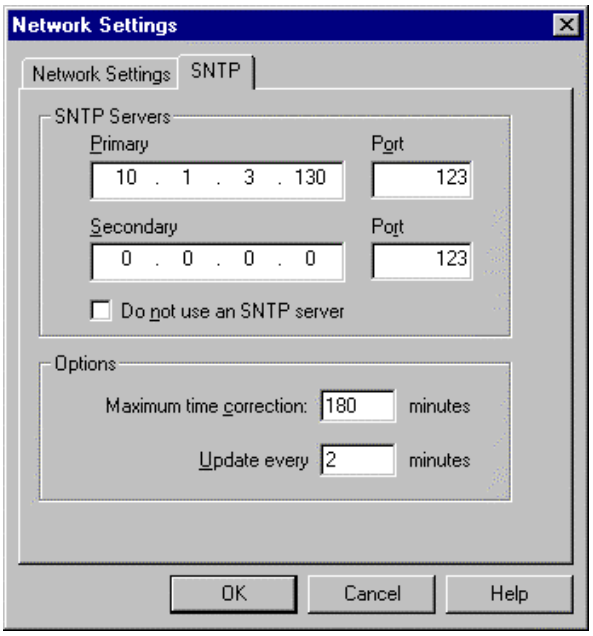


Figure 8-1 – Setting the System SNTP Server

   The Options specified in this dialog, *Maximum time correction* and *Update every*, apply to the Configuration Server only. The *i*.LON 1000 device SNTP options are self-adjusting and cannot be configured.

2. Enter the IP addresses of the SNTP servers. Note that the SNTP server addresses should be static IP addresses. Leave the default port numbers of 123. Ensure that the **"Do not use an SNTP server"** checkbox is cleared.

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

Specifying SNTP Servers for a Channel or Device

By default, 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). If desired, 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. Highlight the channel or device in the main dialog of the Configuration Server and click on **Properties**. Click on the **SNTP** tab.

2. Clear the **Use System Default** or **Use Channel Default** option and enter the IP addresses of the SNTP servers as shown in Figure 8-2. Leave the default port numbers of 123.

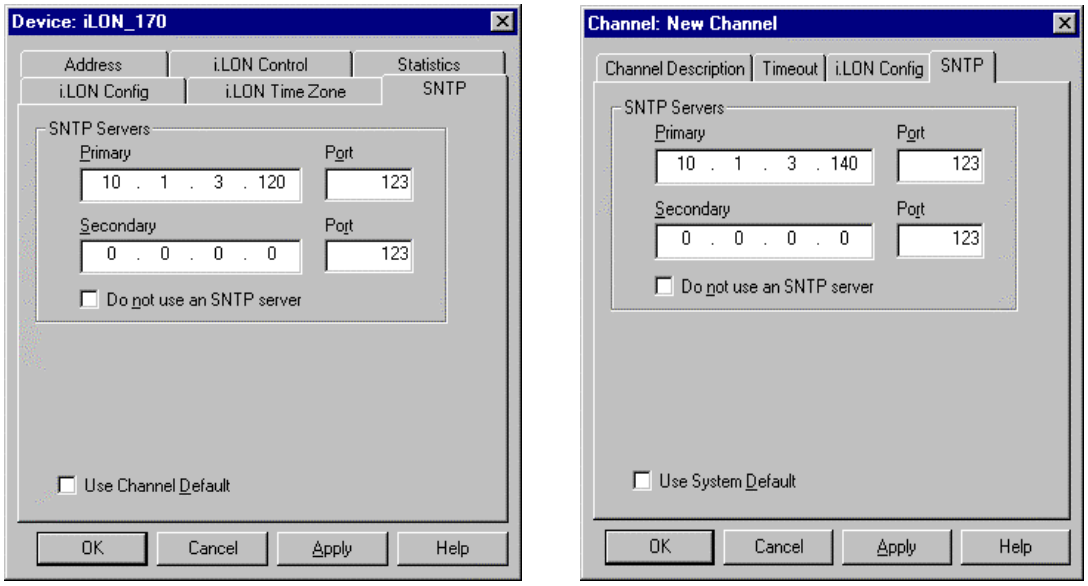


Figure 8-2 – SNTP Server Configuration for a Channel and Device

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

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

When the PC that runs the Configuration Server is already setup to run a third-party SNTP client, the Configuration Server's system and channel SNTP settings must be set accordingly. The third-party SNTP client will synchronize the PC's clock; therefore, system SNTP servers should *not* be specified in the Configuration Server. Doing so would cause the PC's clock to be synchronized to two SNTP servers—an undesired effect. When SNTP servers are not specified at the system level, as in this case, you must configure SNTP servers at the channel level so that each channel can synchronize to a SNTP 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. Select the **"Do not use an SNTP server"** checkbox. When checked, 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.
3. Click **OK** to save and return to the main dialog.
4. Specify SNTP Servers for all channels in the network. Clear the **Use System Default** checkbox under Channel Properties when using a third-party SNTP client.

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:

Site Name	Site Address
Ntp.css.gov	148.162.8.3
bonehed.lcs.mit.edu	18.26.4.105
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 a SNTP server on any PC in your LAN. You may use the same PC on which the Configuration Server is installed. An option is Tardis2000, shareware available from www.kaska.demon.co.uk. You can configure it 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

Creating an *i*.LON 1000 Web Page

This chapter contains a step-by-step tutorial that describes how create a simple *i*.LON 1000 web pages in conjunction with the LonMaker tool. These web pages allow you to monitor and control network variables over the Internet (or any other IP network).

Overview of Creating *i*.LON 1000 Web Pages

The *i*.LON 1000's embedded Web server application and the *i*.LON 1000's embedded data server application work together to serve web pages that reference network variables to a standard web browser.

The *i*.LON 1000's data server provides an anchor point to which both input and output network variables can be bound. Additionally, it knows how to pass the current value of network variables to the Web server, and how to accept data from the web server to propagate to its output network variables.

Prior to returning a web page to a browser, the web server parses the page searching for a special HTML tag indicating a network variable reference. The web server substitutes the current value of a network variable for this tag when returning information to the browser. Thus, any network variable defined on the *i*.LON 1000 can be referenced in a web page just by incorporating the correct HTML tags.

Web pages may be constructed with any off-the-shelf HTML editor.

Required Hardware

You will need the following hardware for this tutorial:

- 1 *i*.LON 1000 Internet Server (with FTT-10 channel)
- 1 LonPoint DI-10 Digital Interface Module
- 1 LonPoint DO-10 Digital Output Interface Module

Required Software

You will need the following software for this tutorial:

- LonMaker Integration Tool version 2.0 (or higher) with the LonMaker Basic Shapes Stencil.
- A standard FTP client application such as CuteFTP or AbsoluteFTP
- Netscape Navigator (version 4.0 or higher) or Microsoft Internet Explorer (version 4.0 or higher)

Setting Up The Hardware

Physically attach the DI-10, DO-10, *i*.LON 1000 and LonMaker PC to the FTT channel as shown in Figure 9-1. Attach the *i*.LON 1000 to the 10BaseT network. Check with your system administrator for a valid IP address, subnet mask, and gateway for the *i*.LON 1000. Be sure there is another PC on the IP network equipped with a browser and an FTP client.

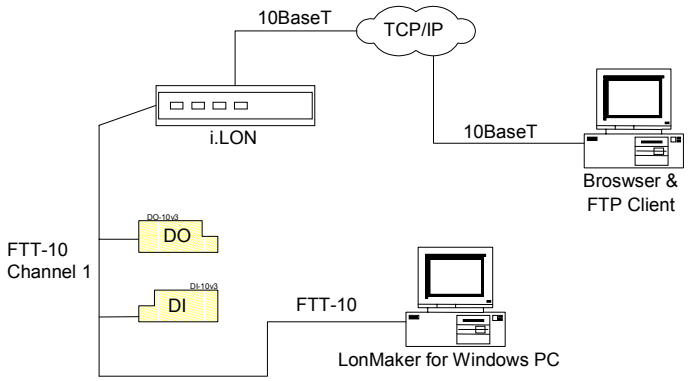


Figure 9-1 Tutorial Hardware Setup

Creating The LonMaker Network

This section describes how to create a simple LonMaker network using LonPoint devices and how to create a web page through which that network can be monitored and controlled using an *i*.LON 1000. Please refer to the LonMaker and LonPoint documentation for more information on performing the various LonMaker tasks described in this tutorial.

1. Set the *i*.LON 1000's IP address, subnet mask, gateway, FTP user name, and FTP password using the *i*.LON 1000 Console Application as described in Chapter 4.
2. Be sure that you can ping the *i*.LON 1000 device and log in as a FTP user before continuing
3. Verify that the web server component is running on your *i*.LON 1000 by typing **`listapp`** at the console prompt. The output should look like this:

```
iLON> listapp
Index  Name               Channel  State                Domain(hex)  Subnet/Node
-----  ----------------   -------  ------------------   -----------  -----------
1      Router             LonTalk  Unconfigured
                          IP       Unconfigured
3      DataServer         LonTalk  Unconfigured
4      WebServer                   Activated
```

   Three applications should be running in the *i*.LON 1000: the Router, DataServer, and WebServer. The DataServer and WebServer work together to serve web pages and are required for this tutorial.

   If these three applications do not appear on the *i*.LON 1000 console, type **`factory`** at the *i*.LON 1000's console prompt to reload the *i*.LON 1000 factory defaults. Note that after typing **`factory`** you will have to reset the IP configuration.

4. Create and open a new network using the LonMaker tool (version 2.0 or higher). This tutorial requires that you are attached to the network and the LONWORKS/IP channel is *Enabled* in the Configuration Server.
5. Drop a DI-10 device shape and a DO-10 device shape from the LonPoint Shapes stencil onto the LonMaker drawing and commission them. Set their state to "online".
6. Drop a device shape from the LonMaker Basic Shape stencil and name it "Web Server".

   As part of the device definition process, you are prompted to select or define the device template for the *iLON Web Server* device. Select **Upload From Device**. This option

instructs LonMaker to create a device template based on what the device reports as its external interface.

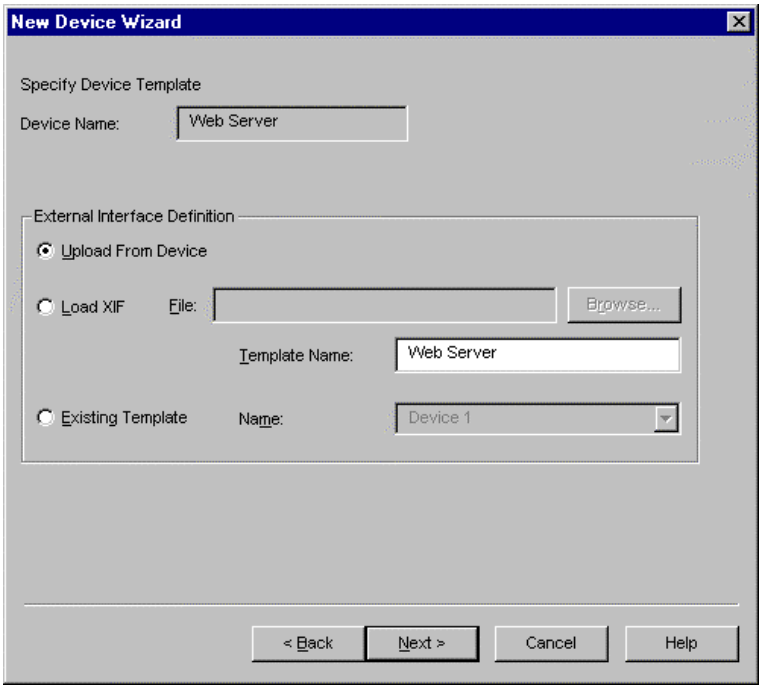
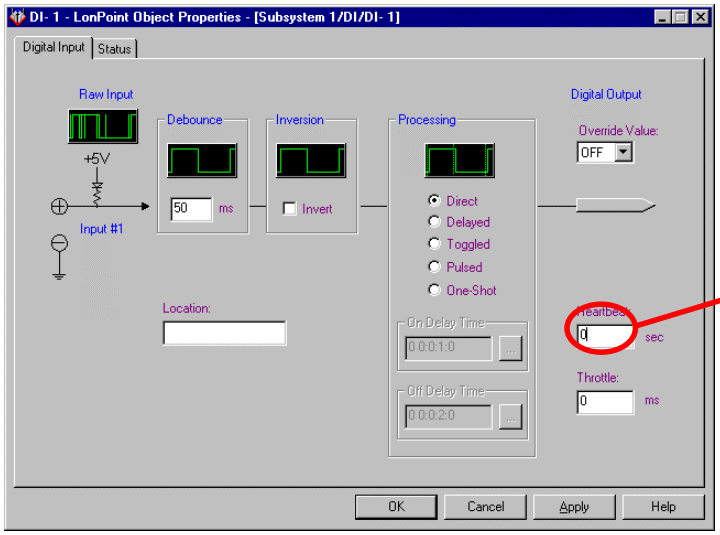


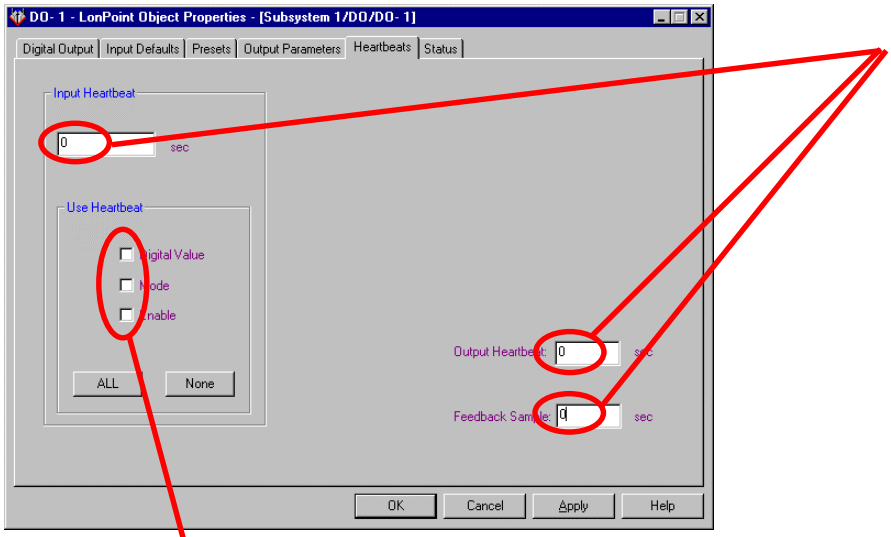
Figure 9-2 – Creating the Web Server Device

7. Ensure that you are attached to the network, specify the service pin installation method, and press the Service Control Switch on the *i*.LON 1000 when prompted.
8. From the LonPoint stencil, drop 4 "Digital Input" functional blocks. Associate one with each input on the DI-10 device.
9. From the LonPoint stencil, drop 4 "Digital Output" functional blocks. Associate one with each output on the DO-10 device.
10. Select each LonPoint function block, right-click, and select Configure. Disable heartbeats in both the input and output functional blocks as shown in Figures 9-3 and 9-4. If you leave heartbeats on, it will be much more difficult to determine if the web pages that you create later in this tutorial work as intended.



Set this value to zero for all digital input functional blocks.

Figure 9-3 – Disable Digital Input Functional Block Heartbeat



Set these values to zero for each Digital output functional block.

Figure 9.4 – Disable Digital Output Functional Block Heartbeat

Heartbeats are not required.

11. Drop a Functional Block shape from the LonMaker Basic Shapes stencil. Associate the functional block with the Web Server device's Virtual Functional Block. The drawing should look similar to Figure 9-5.

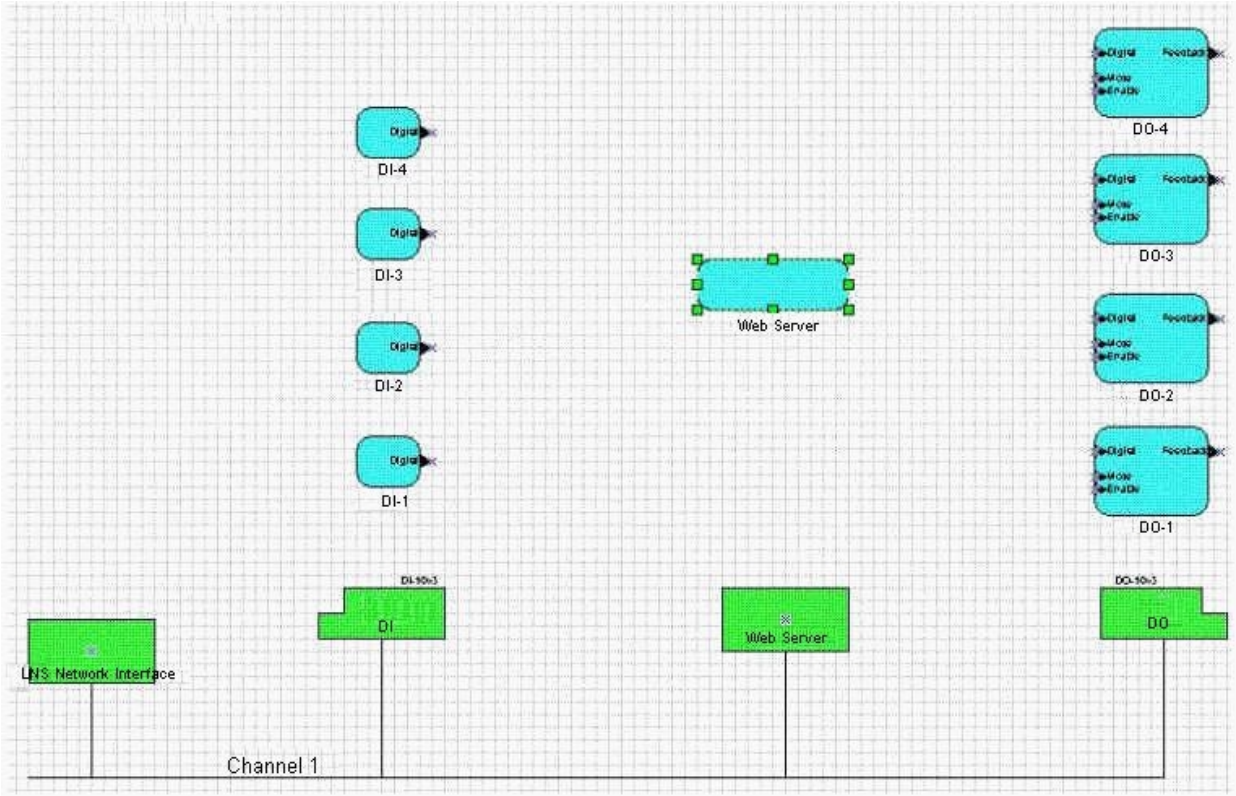


Figure 9-5 LonMaker Drawing Defining the *i*.LON 1000 Web Server

12. Drop an Input Network Variable shape from the LonMaker Basic Shapes Stencil onto the Web Server functional block to open the dialog shown in figure 9-6.

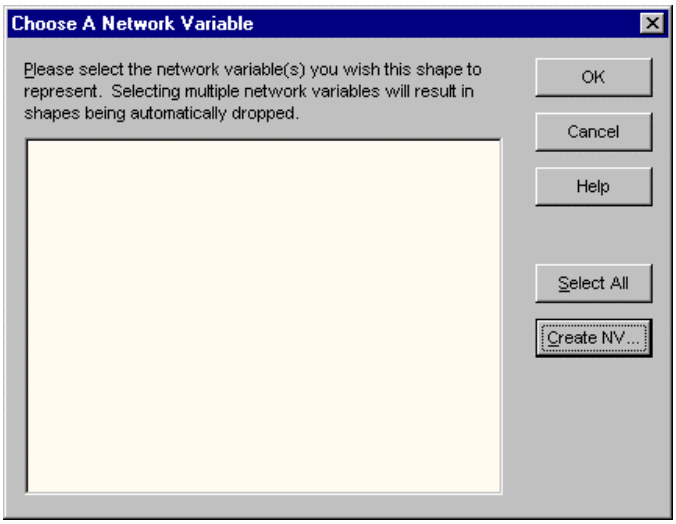


Figure 9-6 – Dropping a Network Variable Shape

13. Click **Create NV** to open a dialog which allows you to dynamically create complementary network variables on the host. From this dialog, click **Browse** and browse to one of the Digital output network variables on the DI-10 functional blocks, as shown in Figure 9-7.

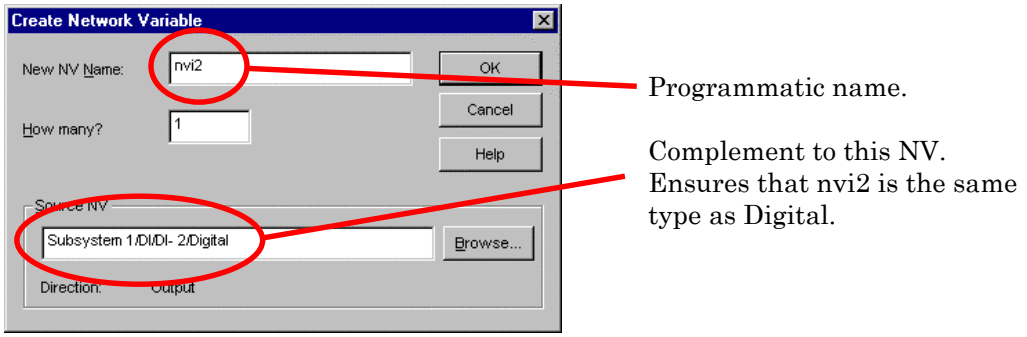


Figure 9-7 – Network Variable Creation

14. Assign a name to the new network variable in the **New NV Name** field and click **OK** to create the network variable on the *i*.LON 1000 and repeat this procedure 3 more times (once for each Digital output network variable on the DI-10 functional blocks) to create 4 input network variables on the host.

    WARNING! When creating these variables, the very first name you create becomes the "programmatic name" by which the variable will be referenced. Changing the name on the LonMaker drawing will not affect the programmatic name. To change a programmatic name you have to remove the network variable and then re-create it.

15. Add all the created input network variables as shapes to the Web Server functional block by clicking **Select All** and **OK** from the Choose a Network Variable dialog shown in Figure 8-6.

16. Repeat the procedure from steps 12 through 15 to create 4 output network variables (and corresponding shapes) on the Web Server functional block which are complementary to the 4 Digital input network variables on the 4 DO-10 functional blocks.

17. Once you've created all your network variables, verify that your virtual functional block resembles Figure 9-8.

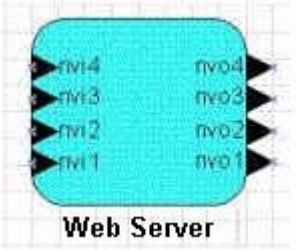


Figure 9-8 - Web Server's Virtual Functional Block

18. Connect the digital input functional blocks to the Web Server inputs, and the digital output functional blocks to the Web Server outputs. Figure 9-9 shows a sample of a LonMaker drawing created using these instructions.

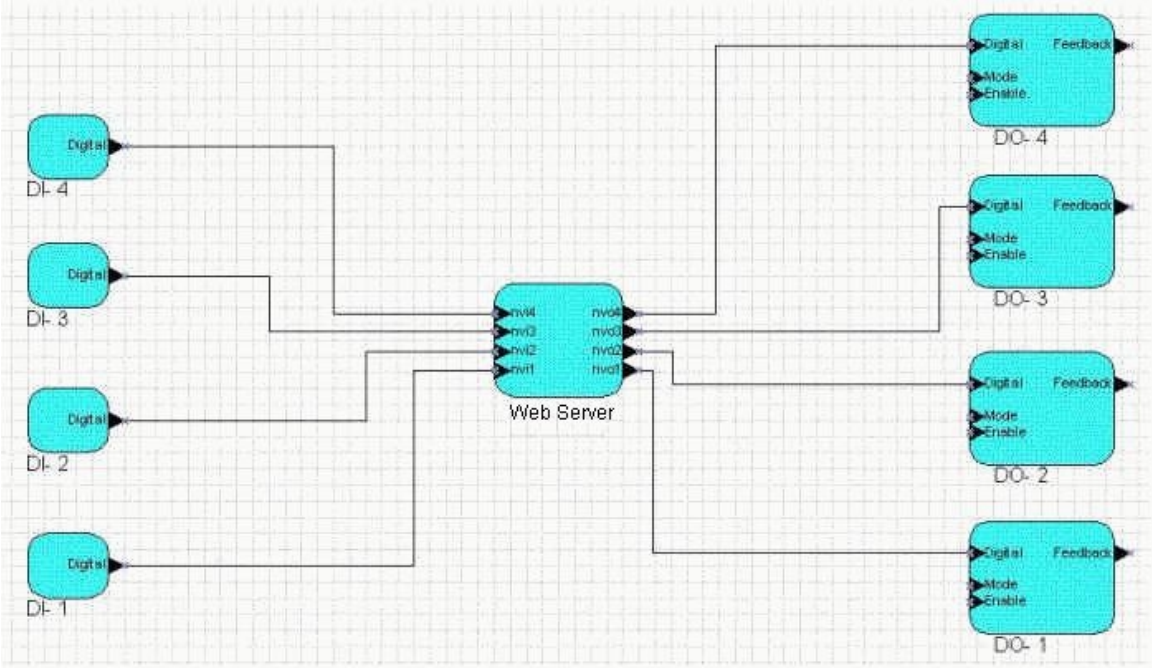


Figure 9-9 – Web Server Connected to DI and DO Devices

19. The Web Server functional block that you created can monitor and control the network variables on the DI-10 and DO-10 devices through a web browser. Next, you will write some HTML code and make references to the network variables on the *i*.LON 1000s virtual functional block.

Creating Web Pages

HTML files for the *i*.LON 1000 Web server may be created with any standard text or HTML editor. The *i*.LON 1000 Web server supports standard HTML for defining the structure and format of your web page, as well as the `<ILONWEB>` HTML tag for retrieving dynamic data elements and processing HTML forms. The `<ILONWEB>` tag is an extended HTML tag designed to provide access to *i*.LON 1000 system and network variable data through a web browser such as Netscape Navigator version 4.0 or higher, or Microsoft Internet Explorer version 4.01 or higher.

HTML files reside in a special directory on the i.LON 1000's flash disk. Other related files such as graphics and Java applets may also be stored on the flash disk. Approximately 1 MB of space is available for user files on the i.LON 1000's flash disk. Files are read and written to the i.LON 1000's flash disk using standard FTP over the IP connection.

To create a simple web page which will monitor and control the values of the network variables connected to the Web Server functional block (see *Creating the LonMaker Network*, earlier in this chapter), follow these steps:

1. Use a text or HTML editor to input the following HTML code:

```
<html>
<head>
<title>Display Digital Sensors (inputs)</title>
</head>
nvi1 = <iLonWeb FUNC=ShowValue SYMBOL=NVL_nvi1></iLonWeb><p>
nvi2 = <iLonWeb FUNC=ShowValue SYMBOL=NVL_nvi2></iLonWeb><p>
```

```
nvi3 = <iLonWeb FUNC=ShowValue SYMBOL=NVL_nvi3></iLonWeb><p>
nvi4 = <iLonWeb FUNC=ShowValue SYMBOL=NVL_nvi4></iLonWeb><p>
</html>
```

The *i*.LON 1000's built-in Web server understands the meaning of the special `<iLonWeb>` HTML tag. When the server returns a page to a requesting browser, the ***server*** parses the page and substitutes the current value of the network variable for the `<iLonWeb>` tag. (Those of you familiar with ASP or other server side substitution technologies will recognize this technique.)

This web page displays the current value of nvi1, nvi2, nvi3, and nvi4 (which are connected to the Digital output network variables of the 4 DI-10 functional blocks. It can be enhanced to contain other HTML objects such as pictures, MP3 files, and movies.

2. Save the HTML text above as `inputs.htm`.
3. Upload `inputs.htm` to the *i*.LON 1000's flash disk using a standard FTP program such as CuteFTP (`http://www.cuteftp.com`), AbsoluteFTP (`http://www.vandyke.com`), or the command line FTP client that ships with Microsoft Windows.

   The *i*.LON 1000 directory structure is as follows:

All web pages must be in the directory named `Web` or in a subfolder of `Web`. Any page that references network variables must be placed in the `/root/Web/forms` directory or a subdirectory below `/forms`. You may create other directories under `Web` to store graphics and other content. The *i*.LON 1000 has about 1MB of disk space available for your content

The log below shows a FTP session using the command-line FTP client included with Windows NT 4.0.

Transfer `inputs.htm` to the `/root/Web/forms` directory on the *i*.LON 1000.

```
C:\>ftp 24.1.7.251
Connected to 24.1.7.251.
220 VxWorks FTP server (VxWorks 5.3.1) ready.
User (10.1.0.169:(none)): ilon
331 Password required
Password:
230 User logged in
ftp> dir
200 Port set okay
150 Opening BINARY mode data connection
-rwx---A--  1 user    group         6890 Dec 28 08:48 eventlog.txt
-rwx---A--  1 user    group      2168580 Dec  9 15:36 iLonSystem
drwx------  1 user    group          512 Dec 12 14:58 ltConfig
-rwx---A--  1 user    group        51349 Dec 20 23:13 sntp.log
-rwx---A--  1 user    group          180 Dec  9 15:36 WebParams.dat
drwx------  1 user    group          512 Dec  9 15:36 demo
drwx------  1 user    group          512 Dec  9 15:36 lonworks
drwx------  1 user    group          512 Dec  9 15:36 Web
```

```
drwx------  1 user    group          512 Dec  9 15:36 snmp
-rwx---A--  1 user    group            0 Dec 20 09:47 ilonnear.txt
226 Transfer complete
632 bytes received in 0.48 seconds (1.32 Kbytes/sec)
ftp> cd Web/forms
250 Changed directory to "/root/Web/forms"
ftp> put inputs.htm
200 Port set okay
150 Opening BINARY mode data connection
226 Transfer complete
179 bytes sent in 0.00 seconds (179000.00 Kbytes/sec)
ftp>
```

4. To retrieve the web page enter `http://24.1.7.251/forms/inputs.htm` (where 24.1.7.151 is the *i*.LON 1000's IP address) in the browser's URL window. Be sure to use the proper case; file and directory names are case sensitive. You do not need to include the `Web` directory in the URL. `Web` is the implied root for all http requests.
5. Assume that switches 1 and 2 are OFF, and switches 3 and 4 are ON. The HTML code entered in Step 1 will generate the web page shown in Figure 9-10.

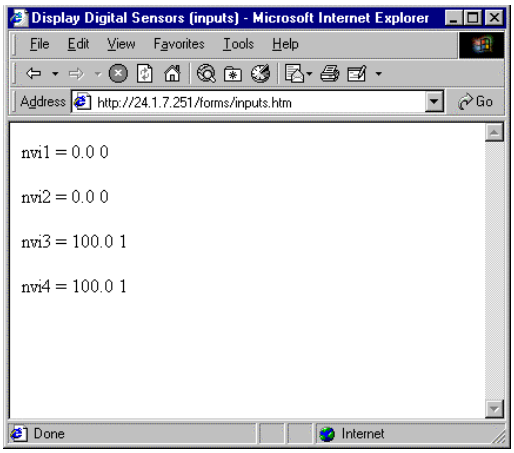


Figure 9-10 – Web Page Displaying Input Network Variable Values

Notice that the *i*.LON 1000's Web server converts the network variable values to strings. The browser "sees" only text.

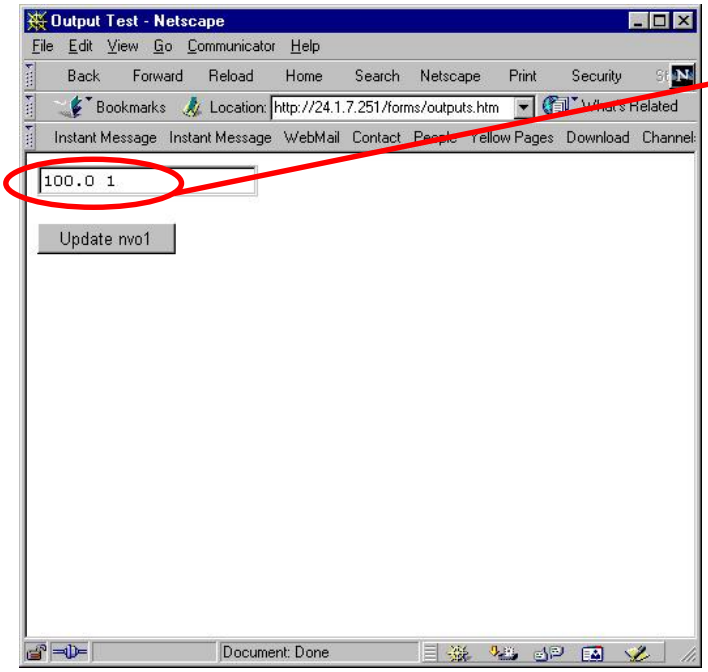
6. Open a new file using a standard text or HTML editor and enter the following HTML code:

```
<html>
<head>
<title>Output Test</title>
</head>
<form action="outputs.htm" method="get">
<iLonWeb_url>
<iLonWeb func=TextField type=text symbol=NVL_nvo1
size="20"></iLonWeb>
<p>
<input type="submit" value="Update nvo1">
</form>
</html>
```

This HTML will allows the output network variables defined on the *i*.LON 1000's Web Server functional block to be controlled from a web page. Since these network variables are connected to the Digital input network variables of the DO-10 device, this will allow you to change the output of the DO device from the web page.

7. Save this code as a file named `outputs.htm`. (The file name is important since the code references the file name in the *action* attribute of each form.) Using an FTP program, transfer the file to the *i*.LON 1000's `Web/forms` directory, as you did for `inputs.htm`.

8. Enter `http://24.1.7.251/forms/outputs.htm` (where `24.1.7.251` is the *i*.LON's IP address) in the browser URL window to display the web page shown in Figure 9-11.



Manually enter "100.0 1" (the SNVT_switch value for ON) in the text box and click the button marked "Update nvo1". This causes the *i*.LON to propagate its network variables.

Figure 9-11 – Web Page Displaying Output Network Variable

How the HTML Code Works

Let's examine how this process works. Most Web servers have the ability to call utility programs through a CGI gateway. These utility programs usually do something simple like create a GIF image of a stock chart based on stock symbol provided by the user. Usually, the stock symbol is typed into a text box. When the user clicks the "create a chart" button, the stock symbol is passed to the chart-making program as a parameter. The chart-making program makes the chart, saves it as a .GIF file, and tells the server that it has completed its task. The server then serves a page back to the browser, referencing the newly created GIF file.

Updating an output network variable uses a similar mechanism. When you click on the "Update nvo1" button, you are submitting the content of the text box (really the entire form) to the i.LON 1000's Web server. The server passes the form on to the form-processing engine through an internal i.LON 1000 interface that is similar to CGI. The engine looks for a network variable name associated with the text box, and then passes the value in the text box along with the network variable name to the *i*.LON 1000's data server. The data server

then propagates the network variable to the network. The sample below examines each component.

```
<form action="outputs.htm" method="get">
<iLonWeb_url>
<iLonWeb func=TextField type=text symbol=NVL_nvo1 size="20"></iLonWeb>
<p>
<input type="submit" value="Update nvo1">
</form>
```

Indicates the beginning and end of an HTML form. Forms may contain several elements. For example, this form contains a textbox, and a submit button.

```
<form action="outputs.htm" method="get">
<iLonWeb_url>
<iLonWeb func=TextField type=text symbol=NVL_nvo1 size="20"></iLonWeb>
<p>
<input type="submit" value="Update nvo1">
</form>
```

Creates an element in a form that is associated with a network variable. In this case the element is a textbox and the network variable is nvo1.

```
<form action="outputs.htm" method="get">
<iLonWeb_url>
<iLonWeb func=TextField type=text symbol=NVL_nvo1 size="20"></iLonWeb>
<p>
<input type="submit" value="Update nvo1">
</form>
```

Specifies that the element is a textbox (as opposed to a dropdown combo box, a list, a large text field, etc.)

The "NVL_" that prefaces the network variable name indicates that nvo1 is a local network variable. **Important!** You must include the NVL_ prefix. It is part of the required HTML syntax.

```
<form action="outputs.htm" method="get">
<iLonWeb_url>
<iLonWeb func=TextField type=text symbol=NVL_nvo1 size="20"></iLonWeb>
<p>
<input type="submit" value="Update nvo1">
</form>
```

Standard HTML submit button. Every form must have some mechanism that indicates the user has finished filling out the information in the textbox(s) and it is time to send the information to the web server. The most common method for doing this is to use a submit button. The Web browser recognizes that when a submit button click event occurs, it is time to send the form to the web server (the i.LON 1000 in our case) to process the form.

```
<form action="outputs.htm" method="get">
<iLonWeb_url>
<iLonWeb func=TextField type=text symbol=NVL_nvo1 size="20"></iLonWeb>
<p>
<input type="submit" value="Update nvo1">
</form>
```

The `<iLonWeb_url>` tag allows the *i*.LON 1000 to implement the necessary security to prevent access to network variables on web pages that are outside of a user's access range. See Chapter 11 for more information on setting up i.LON 1000 web page security)

When the *i*.LON 1000's Web server serves `outputs.htm` the above HTML code is translated to look like:

```
<form action="outputs.htm" method="get">
<INPUT TYPE=HIDDEN NAME=iLonWeb_URL VALUE=/forms/outputs.htm>
<INPUT TYPE=text NAME=NVL_nvo1 VALUE="0.0 0" MAXLENGTH=31 SIZE="20" >
<p>
<input type="submit" value="Update nvo1">
</form>
```

You can see the effect of the translation by viewing the source code in the browser. Notice that `<iLonWeb_url>` has been translated to `<INPUT TYPE=HIDDEN NAME=iLonWeb_URL VALUE=/forms/outputs.htm>`. The form-processing engine decides which network variables to update based on the hidden field. The form-processing engine will update all the network variables on the page listed in the *value* attribute of this hidden field. Because all NVs are sent to the engine when the form is processed, it generally makes sense to have only one form per web page.

```
<form action="outputs.htm" method="get">
<iLonWeb_url>
<iLonWeb func=TextField type=text symbol=NVL_nvo1 size="20"></iLonWeb>
<p>
<input type="submit" value="Update nvo1">
</form>
```

All forms have an *action* attribute. This attribute indicates which page will be served next (after submittal). The *method* attribute indicates that the form-processing engine should get all the values in the current form as a QueryString when the submit button is pressed. The "post" method is not supported.

10

Advanced Usage of the <iLonWeb> HTML Tag

This chapter contains information on creating more advanced web pages using the <iLonWeb> HTML tag. The <iLonWeb> tag is an extended HTML tag that provides access to *i*.LON 1000 system data and dynamic network variable data for monitoring and control through a web browser. This chapter assumes you have a basic understanding of HTML.

<iLonWeb> Web Tag Format

The <iLonWeb> tag identifies variables, include files, and form elements used by the *i*.LON 1000 Web server. The general syntax of the <iLonWeb> tag is:

<iLonWeb FUNC=*function* SYMBOL={NVL_|NVE_|ILON_|} *symbolname* [!FIELD:*field name*][!FORMAT:*format type*][!PROPAGATE:{*TRUE*/*FALSE*}][!WAIT:TRUE] > </iLonWeb>

The content of the web tag is defined by the *function* specified within the <iLonWeb> tag statement. Depending on the function, the web tag can simply display a network variable value, or it can accept user input from a web page displayed in a browser and change the value of a network variable. The appropriate network variable or internal *i*.LON 1000 system variable is specified within the <iLonWeb> tag using the SYMBOL attribute. The remaining attributes further qualify what the behavior of the function, such as formatting the output or displaying a specific field within a network variable. These are described in further detail in this chapter.

While the *i*.LON 1000 Web server parses and replaces the web tags in its HTML files according to their function, it ignores all text between the <iLonWeb...> and </iLonWeb> tags. In contrast, a standard browser reading the same HTML file will ignore the web tags and process the text between the tags. This feature can be useful when prototyping *i*.LON 1000 web pages in standard HTML editors. See *Working with Forms* later in this chapter for an example.

FUNC Attribute

Func=ShowValue

The ShowValue function displays the value of the variable identified with the SYMBOL attribute. The syntax of the ShowValue function is:

<iLonWeb FUNC=ShowValue SYMBOL=*symbolname*> </iLonWeb>

The following example shows the HTML required to display the current value of an input network variable named **localDigitalIn1** using the default text formatting. The network variable name is prefixed with "NVL_" indicating it is a local network variable. The *i*.LON 1000's Web server uses the first few characters of the symbol name parameter to determine how the symbol is to be acquired. See the *Web Tag Symbol Names* section for more detail on symbol prefixes.

```
<html>
<body>
LocalDigitalIn1=<iLonWeb FUNC=ShowValue
SYMBOL=NVL_localDigitalIn1></iLonWeb>
</body>
</html>
```

FUNC=Include

The Include function allows you to include the contents of files. This function reads the contents of the file identified with the FILE attribute. The FILE attribute must specify the

include path beginning with /forms/. The include file can also contain <iLonWeb> tags. The syntax of the Include function is:

<iLonWeb FUNC=Include FILE=*incpath*> </iLonWeb>

The following example shows the Include function used in HTML to include the file called **localConfig.htm**.

```
<html>
<body bgcolor="#CCCCFF">
<iLonWeb func=Include FILE=/forms/localConfig.htm></iLonWeb>
</body>
</html>
```

FUNC=CreateSymbol

The CreateSymbol function creates a global variable on the Web server. You can use global variables for a number of tasks including passing the variable to another form, modifying its value, or using it to set up a counter. CreateSymbol is often used to pass variables between forms to use with Java scripts. The syntax of the CreateSymbol function is:

<iLonWeb FUNC=CreateSymbol SYMBOL=*User Symbol* VALUE=*user defined*> </iLonWeb>

User Symbol may be any name not starting with symbol prefixes used in the *Web Tag Symbol Names* section.

The following HTML example creates and tests a user-defined symbol called **sValue**. The CreateSymbol function is used to create the symbol, and the ShowValue function is used to display the value assigned to the symbol when it was created.

```
<html>
<body bgcolor="#CCCCFF">
<iLonWeb func=CreateSymbol symbol=sValue value="This is a
Test"></iLonWeb>
<p>ShowValue of sValue is <iLonWeb func=ShowValue
symbol=sValue></iLonWeb>
</body>
</html>
```

Form element functions include CheckBox, RadioButton, TextField, and TextArea. See *Working with Forms*, in this chapter for more information.

SYMBOL Attribute

The *i*.LON 1000 Web server uses web tag symbol names to identify and retrieve different types of *i*.LON 1000 system data and network variable data that can be displayed in web pages. Web tag symbol names have prefixes that determine their type as described in Table 10-1.

Table 10-1 – Web Tag SYMBOL Name Prefixes

Web Tag Symbol Name Prefix	Description
NVE_, NVL_	Refer to network variable symbols. NVE_ refers to network variable symbols on remote devices that are polled by the *i*.LON 1000. NVL_ refers to network variable symbols local to the *i*.LON 1000 Web server.
ILON_	Refer to system variables generated inside the *i*.LON 1000 system software. These values cannot be changed through HTML forms; the values may be changed through the Console Application or the Configuration Server, depending on the symbol.
User Defined	Other prefixes that can be used as local web tag symbols in forms once created with the CreateSymbol tag.

Network Variable Symbols (NVL_ and NVE_ Prefixes)

The *i*.LON 1000 Web server fully supports dynamic network variables as defined by the LONMARK Guidelines. In addition, a network variable may be defined explicitly if you want to retrieve the value of a remote network variable, or poll a device each time a web browser makes a request from the *i*.LON 1000 Web server.

Two types of network variable references may be used in *i*.LON 1000 Web server web pages: local network variable references and explicit network variable references. Local network variable references cause the *i*.LON to return the value cached in a dynamically created local network variable (assuming that something is bound to the local network variable) and allow event-driven updates to be reported on web pages. Reading and writing of local network variables is accomplished through the use of the NVL_ symbol, described below.

Explicit network variable references are not located on the *i*.LON 1000 Web server, but exist elsewhere in the LONWORKS network and require explicit definition (you must set every associated communication and data formatting parameter). You have read-only access to explicit output network variables and read-write access to explicit input network variables. Reading and writing of explicit network variables is accomplished through the use of the NVE_ symbol, described below.

Local Network Variable Symbols (NVL_ Prefix)

In general, it is best to use local network variables as much as possible. Using local network variables has the following advantages over using explicit network variables:

- **Reduced Network Traffic.** If an output network variable is bound to the *i*.LON 1000, the *i*.LON 1000 will get value updates for the remote output whenever its value changes. The Web server can query the value of the local input network variable without producing any LONWORKS network traffic. If the same network variable is monitored through an explicit network variable tag reference (NVE_), a value query message will be sent on the LONWORKS network every time the *i*.LON 1000 serves the page. More web page hits equate to more traffic on the LONWORKS network.
- **Greater Manageability.** Network variable addresses and selectors may change when connections to the variable are added or deleted. This information is a required component of the NVE_ web tag. Reconfiguration may cause explicit network variable web tag references to become obsolete.
- **Ease of Use**. Local network variable references are easier to define and manage.

Local network variable symbol names are prefixed with NVL_ when specified in the <iLonWeb> tag. For example:

```
<iLonWeb Func=ShowValue SYMBOL=NVL_nvitemp> </iLonWeb>
```

Since the network variable is defined locally, the web server is aware of its type, size, and format, and can simply reference it by name. The syntax for a local network variable reference is:

NVL_<local network variable name>

The <local network variable name> is the programmatic name of the network variable dynamically created on the web server by a network management tool such as the LonMaker tool. The *i*.LON 1000 Web server can have up to 4096 network variables.

For example, the action of the following ShowValue function will display the contents of the local network variable, **DigitalOut**.

```
<iLonWeb FUNC=ShowValue SYMBOL=NVL_DigitalOut> </iLonWeb>
```

Explicit Network Variable Symbols (NVE_ Prefix)

While it is normally advantageous to use local network variables, there are several cases where this method does not work:

- Your network management tool does not know how to create dynamic network variables
- Your system is pre-installed, or self-installed and thus has no network management tool
- Your system is installed on the zero length domain
- You can create dynamic network variables, but you need so many that you run out of address table entries

In these cases, you need to poll the network variables on the network without binding them to the *i*.LON 1000's virtual functional block. Because the network variable is not local to the *i*.LON 1000, the network variable must be explicitly identified by a combination of its network address, NV type information, and transport attributes.

Explicit network variable symbol names are prefixed with NVE_ when specified in the <iLonWeb> tag.

The general syntax for the explicit network symbol is:

NVE_{AS:SN.DM:x.SU:x.NO:x | AS:GR.DM:x.GR:x.ME:x | AS:BR.DM:x.SU:x}.ST:e.PR:b.AU:b.SY:b.NI:x.NS:x.RY:x.TX:x.TY:x.SZ:x

The information that can be entered in this field is shown in Table 10-2

Table 10-2 – The NVE_ Symbol

Attribute	Description
AS:e	The network variable addressing mode. All addressing modes require the domain index (DM field) to be specified, which will always be 0 in the first release. The addressing mode field may have the following values, each of which require the following additional fields to be specified: AS:SN specifies subnet-node addressing. If specified, the SU field must specify the subnet ID, and the NO field must specify the node ID. Valid subnet ID values are 1 through 255. For example, if you want to read a network variable value on subnet 4, node 2: `<iLonWeb FUNC=ShowValue SYMBOL=NVE_`**`AS:SN.DM:0.SU:4.NO:2`**`.ST:UR.PR:0.AU:0.SY:0.NI:6.NS`

Attribute	Description
	:298.RY:3.TX:768.TY:95.SZ:2> </iLonWeb> Alternatively, AS:GR specifies group addressing. If specified, the GR field must specify the group ID, and the ME field must specify the number of members in the group, for example, if you want to send an update to group 3, which contains 4 members: <iLonWeb FUNC=ShowValue SYMBOL=NVE_**AS:GR.DM:0.GR:3.ME:4**.ST:UR.PR:0.AU:0.SY:0.NI:6.NS:298.RY:3.TX:768.TY:95.SZ:2> </iLonWeb> AS:BR specifies broadcast addressing. If specified, the SU field must specify the subnet ID for subnet broadcast, or must be 0 to define domain broadcast. For example, to broadcast to all devices on subnet 2: <iLonWeb FUNC=ShowValue SYMBOL=NVE_**AS:BR.DM:0.SU:2**.ST:UR.PR:0.AU:0.SY:0.NI:6.NS:298.RY:3.TX:768.TY:95.SZ:2> </iLonWeb>
ST:e	Service Type describes the message delivery service to be used when updating a remote input network variable. Values can be: UA for unacknowledged service, UR for unacknowledged-repeat, or AK for acknowledged. UR - The update message is sent several times, without any acknowledgment message from the far side. The number of repetitions is determined by the "Retry Count" attribute, and the repeated messages are separated by at least "TX Timer" milliseconds. UA - The update message is sent once, without any acknowledgement from the far side. AK - The update message is sent out and waits for an acknowledgement from the far side for "TX Timer" milliseconds. If no acknowledgement is received for the TX Timer period, the update message is sent again, and the wait for acknowledgement begins again. This is repeated "Retry Count" times.
PR:b	The priority attribute for messages to this network variable. This Boolean field is 0 for no priority and 1 for priority. If Priority is 1, network variable update and fetch messages will be sent as LONWORKS priority messages.
AU:b	The authentication attribute for messages to this network variable. This Boolean field is 0 for no authentication and 1 for authentication. If Authentication is 1, network variable update and fetch messages will be sent with the LONWORKS authentication protocol.
SY:b	The synchronous attribute for this network variable. This Boolean field is 1 for synchronous or 0 for non-synchronous.
NI:x	The index of the network variable in decimal within the application device.
NS:x	The network variable Selector, given in hex, is assigned by the LONWORKS binder to logically connect network variables on the network, causing network variable value updates to be directed to the assigned targets. A selector value of FFFF in this field signifies that the *i*.LON 1000 is polling some device's output network variable.
RY:x	Specifies the number of retries to use. See the above "Service Type" attribute for a description of how this attribute affects updates of remote input network

Attribute	Description
	variables. When fetching the value of a remote input or output network variable, this value determines how many retry messages are attempted with the "Request-Response" service type used. The retry protocol in this case is the same as described above for the "Acknowledged" service type. This is a decimal number between 0 and 15.
TX:x	The Transaction Timer (Tx Timer) should be set based on the network media and channel "distance" between the *i*.LON 1000 and the remote device. Short channel paths over fast media can use smaller values for this timer, while long channel paths or slow media will require larger values. This value is a decimal number.
TY:x	Network variable type. If the remote network variable is a Standard Network Variable Type (SNVT), enter the type index here as a decimal number. If the network variable is not a standard type, enter 0.
SZ:x	The size of the NV in bytes. This is a decimal value from 1 to 31.

Example of Using the NVE_ Symbol

Assume that an input network variable (nviRunSwitch) on the *i*.LON 1000 is bound to an output network variable (nvoMasterPower) on an elevator car controller node. The design of the car controller device is such that nvoMasterPower is the fourth network variable defined in the Neuron C program for the car controller, thus the network variable index of nvoMasterPower is 3 since network variable indexes are zero based. The car controller device has a subnet/node address of 1/5 and is installed on the 1 byte domain with a domain value of 88.

The following HTML code would display the value of the RunSwitch network variable using the NVE_ symbol:

```
<HTML>
<HEAD>
<TITLE>Server Side Substitute Example</TITLE>
<BODY BGCOLOR="#CCCCFF">
RunSwitch = <iLonWeb func=ShowValue
symbol=NVE_AS:SN.DM:0.SU:1.NO:5.ST:AK.PR:0.AU:0.SY:0.NI:3.NS:FFFF.RY:3.
TX:192.TY:8.SZ:2></iLonWeb>
</BODY>
</HTML>
```

Like any other LONWORKS node, the *i*.LON 1000 may simultaneously belong to two domains. The DM element of the NVE_ tag tells the *i*.LON 1000 web server which of it's domain table entries to use for the network variable poll. (In this case we are specifying the first entry – domain indices are zero based – and we expect that the *i*.LON 1000 has been installed on the one byte domain value=88 by some network management tool or the INSTALL console command).

The SU:1 and NO:5 tags specify the subnet/node address of the device we want the *i*.LON 1000 to poll.

The NI:3 tag specifies the network variable index of the network variable we want to poll. NS:FFFF indicates that the network variable selector is FFFF, and SZ:2 indicates that the network variable we are polling is 2 bytes in length.

If you are polling (i.e. monitoring) an output network variable, the selector value should always be set to FFFF. If you are setting (i.e. controlling) the value of a bound input network

variable, the selector needs to be set to whatever value has been assigned to that network connection by the network management tool. If you are setting an unbound input network variable, the selector should be set to 3FFF minus the network variable index.

Complex Example of Using the NVE_ Symbol

This example shows how the NVE_ symbol can be used to control a number of network variable inputs and outputs which are not bound to the *i*.LON 1000 device.

Given a device containing the following Neuron C application:

```
#pragma enable_io_pullups

IO_0 output bit ioLED = 1;     // IO0 LED on LTM-10 Eval Board
IO_4 input bit ioSwitch;       // IO4 Switch on LTM-10 Eval Board

network input SNVT_count nvi0;   //0
network input SNVT_count nvi1;   //1
network input SNVT_count nvi2;   //2
network input SNVT_count nvi3;   //3
network output SNVT_count nvo0;  //4
network output SNVT_count nvo1;  //5
network output SNVT_count nvo2;  //6
network output SNVT_count nvo3;  //7

when (reset)
{
   io_out(ioLED, 1);
   nvo0 = 0;
   nvo1 = 0;
   nvo2 = 0;
   nvo3 = 0;
}

when (nv_update_occurs(nvi0))
{
   nvo0 = nvi0;
}

when (nv_update_occurs(nvi1))
{
   nvo1 = nvi1;
   io_out(ioLED, 0);
   delay(1000);
   io_out(ioLED, 1);
}

when (nv_update_occurs(nvi2))
{
   int i;
   nvo2 = nvi2;
   for (i=0; i<2; i++)
   {
      io_out(ioLED, 0);
      delay(1000);
      io_out(ioLED, 1);
      delay(1000);
```

```
   }
}

when (nv_update_occurs(nvi3))
{
   int i;

   nvo3 = nvi3;
   for (i=0; i<3; i++)
   {
      io_out(ioLED, 0);
      delay(1000);
      io_out(ioLED, 1);
      delay(1000);
   }
}

when (io_changes(ioSwitch))
{
   io_out(ioLED, (int)input_value);
}
```

The following HTML

```
<form action="testfile.htm" method="get">
<ilonweb_url>

nvi0: <iLonWeb func=TextField type=text
symbol=NVE_AS:SN.DM:0.SU:1.NO:3.ST:AK.PR:0.AU:0.SY:0.NI:0.NS:3FFF.RY:3.
TX:192.TY:8.SZ:2 size=20></iLonWeb><p>

nvi1: <iLonWeb func=TextField type=text
symbol=NVE_AS:SN.DM:0.SU:1.NO:3.ST:AK.PR:0.AU:0.SY:0.NI:1.NS:3FFE.RY:3.
TX:192.TY:8.SZ:2 size=20></iLonWeb><p>

nvi2: <iLonWeb func=TextField type=text
symbol=NVE_AS:SN.DM:0.SU:1.NO:3.ST:AK.PR:0.AU:0.SY:0.NI:2.NS:3FFD.RY:3.
TX:192.TY:8.SZ:2 size=20></iLonWeb><p>

nvi3: <iLonWeb func=TextField type=text
symbol=NVE_AS:SN.DM:0.SU:1.NO:3.ST:AK.PR:0.AU:0.SY:0.NI:3.NS:3FFC.RY:3.
TX:192.TY:8.SZ:2 size=20></iLonWeb><p>

<input type="submit" value="Submit">
<br>
<br>

nvo0: <iLonWeb func=ShowValue
symbol=NVE_AS:SN.DM:0.SU:1.NO:3.ST:AK.PR:0.AU:0.SY:0.NI:4.NS:FFFF.RY:3.
TX:192.TY:8.SZ:2></iLonWeb><p>

nvo1: <iLonWeb func=ShowValue
symbol=NVE_AS:SN.DM:0.SU:1.NO:3.ST:AK.PR:0.AU:0.SY:0.NI:5.NS:FFFF.RY:3.
TX:192.TY:8.SZ:2></iLonWeb><p>
```

```
nvo2: <iLonWeb func=ShowValue
symbol=NVE_AS:SN.DM:0.SU:1.NO:3.ST:AK.PR:0.AU:0.SY:0.NI:6.NS:FFFF.RY:3.
TX:192.TY:8.SZ:2></iLonWeb><p>

nvo3: <iLonWeb func=ShowValue
symbol=NVE_AS:SN.DM:0.SU:1.NO:3.ST:AK.PR:0.AU:0.SY:0.NI:7.NS:FFFF.RY:3.
TX:192.TY:8.SZ:2></iLonWeb><p>
```

Produces the web page shown in Figure 10-1:

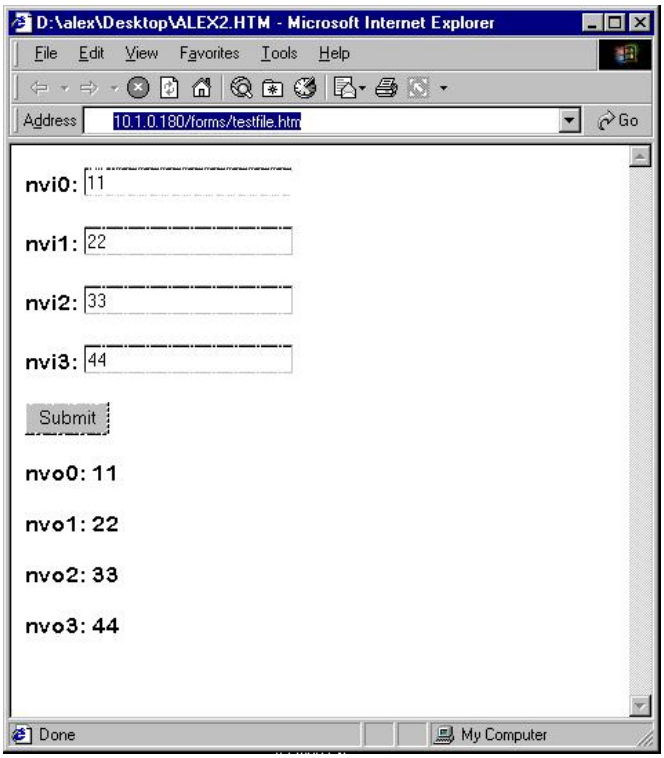


Figure 10-1 – Example *i*.LON 1000 Web Page

You can test this example by loading the Neuron C code above into an LTM-10 (NodeBuilder) device, and placing the testfile.htm file on your *i*.LON. Changing the nvi values updates the nvo values when the submit button is pressed. Note that you may need to press the submit button more than once because there is no guarantee that the network variable updates will return from the devices before the resulting page is served back to the browser. In a production system, you may wish to use the browser's scripting capabilities to insert sufficient delay so as to guarantee a response from each device.

The Web Tag Wizard and Webgen Utility

To make the job of creating `<iLonWeb>` network variable tags easier and more accurate, the *i*.LON 1000 software ships with an *i*.LON 1000 web tag wizard (installed under PROGRAMS | Echelon i.LON). This wizard automatically generates an `<iLonWeb>` HTML tag based on the information you enter. If you have an LNS database available, the WebGen utility (available for free download from the i.LON website at http://www.echelon.com/ilon) can be used to rapidly create web pages allowing you to monitor and control network variables in that database.

System Symbols (ILON_ Prefix)

System symbol names are specified in the `<iLonWeb>` tag with the SYMBOL= attribute to display read-only *i*.LON 1000 device information. System symbol names are prefixed with "ILON_".

The system symbols in Table 10-3 are used with the ShowValue tag to display information from the *i*.LON 1000 device. The symbols are also demonstrated in the default web page example, which is installed on the PC in `iLON\Images\Web\forms\localConfig.htm`.

Table 10-3 – System Symbol Names (ILON_ Prefix) Used With ShowValue

Web Tag Symbol	Description
iLon_Sys_IpAddress	The IP address of the *i*.LON 1000 device, e.g. 10.1.253.101.
iLon_Sys_IpMask	The IP network mask of the *i*.LON 1000 device, e.g. 255.255.255.0.
iLon_Sys_IpName	The IP name of the *i*.LON 1000 device, e.g. iLonDataSvr01
iLon_Sys_Gateway	The IP address of the gateway device, e.g. 10.1.253.1
iLon_Sys_DhcpEnabled	1 if DHCP is enabled, 0 [zero] if not enabled.
iLon_Sys_MacAddress	The Ethernet MAC address of the *i*.LON 1000 device, e.g. 00-23-34-45-56-AB
iLon_Sys_LtUids	The unique IDs, or Neuron IDs, available in the *i*.LON 1000 device for LONWORKS applications.
iLon_Sys_LtXcvrId	The LONWORKS transceiver ID of the attached transceiver.
iLon_Sys_LocalPort	The IP port used by the LONWORKS IP communications software. Normally 1628.
iLon_Sys_ConfigServer	The IP address and port of the Configuration Server, if any. The port follows the address after a colon, e.g. 10.1.253.34:1629
iLon_Sys_TimeServers	The IP address and port of the two time servers, e.g. 10.1.0.1:123,10.1.253.99:123
iLon_Sys_TimeSynched	1 for synchronized with a server, 0 [zero] for not synchronized.
iLon_Sys_Time	The time in Unix format of the local time on the *i*.LON 1000 device.
iLon_Sys_TimeZone	The Timezone settings for the *i*.LON 1000 device. This includes both the offset from universal coordinated time [UTC] and the settings for daylight savings time.

Two types of memory for processing web requests are pre-allocated when the web server starts: global memory, which is used by all the web tasks, and per-request memory, which is used by a particular web task for the duration for one request. The symbols in Table 10-4 allow a page to obtain memory information. For example, in the CreateSymbol function, some of the parameters and security information use the global partition while the request partition is used by the current request only. The global symbols can be placed in any pages after the pages that perform CreateSymbol are used. The request symbols should be placed at the end of pages that process the most complex requests. All of the following symbol values are expressed in bytes.

Table 10-4 – System Symbol Names (ILON_ Prefix) Used to Obtain Memory Information

Web Tag Symbol	Description
iLon_Mem_RequestPartTotal	Total memory allocated to process requests.
iLon_Mem_RequestPartFree	Free memory in a request partition.
iLon_Mem_RequestPartLargest	Largest free block in a request partition.
iLon_Mem_RequestPartUsed	Used memory in a request partition.
iLon_Mem_GlobalPartTotal	Total global memory allocated.
iLon_Mem_GlobalPartFree	Free memory in a global partition.
iLon_Mem_GlobalPartLargest	Largest free block in the global partition.
iLon_Mem_GlobalPartUsed	Used memory in a global request partition.

Web Tag Attributes

When a network variable is specified with the NVL_ or NVE_ symbol in the SYMBOL= attribute of the <iLonWeb> tag, four optional attributes may be used to further define how a network variable is displayed or changed.

- FIELD:
- FORMAT:
- PROPAGATE:
- WAIT:

The attributes may be used in any combination within a single <iLonWeb> tag with the exception of WAIT:. WAIT: must be used in conjunction with PROPAGATE:. The colon (:) is required as part of the syntax. If web tag attributes are used, use the exclamation point (!) to delimit the attributes. For example:

```
<iLonWeb FUNC=TextField
SYMBOL=NVL_DigitalOut!FIELD:value!PROPAGATE:TRUE> </iLonWeb>
```

The web tag in the example above will display the contents of the field called **value** contained in the local network variable, **Digital_Out**. The value will be displayed as a read-write value in a text field. If the form containing this text field is submitted, the new value will be propagated onto the network immediately.

FIELD:

Network variables may contain fields that vary according to the network variable type. The contents of these fields can be displayed and changed by specifying the field name with the FIELD: attribute.

For example, the Standard Network Variable Type (SNVT) SNVT_switch contains two fields: **value** and **state**. To display the contents of the **value** field in the local network variable **DigitalOut**, use the following tag.

```
<iLonWeb FUNC=ShowValue SYMBOL=NVL_DigitalOut!FIELD:value> </iLonWeb>
```

Important! The default value of the PROPAGATE: attribute is FALSE when operating on a network variable field. For further information, see *PROPAGATE:*.

FORMAT:

You may assign a format to a network variable to control how the data is displayed and changed in your web page. Specify the format of the network variable using the FORMAT attribute.

Network variable formats can come from three places:

LonMark Standard Network Variable Type (SNVT) Device Resource Files

This is a set of files that describes the data structures within SNVTs and also describes the formats to be used for display of SNVT data. On the *i*.LON 1000, these files may be found in the directory `/root/lonworks/types`, and are named `STANDARD.ENU`, `STANDARD.TYP`, `STANDARD.FMT` and `STANDARD.FPT`.

The default format for a SNVT is its native format, as described in the `STANDARD.FMT` text file within the resource file set. To assign a different SNVT format, or to assign a SNVT format to a user network variable type, explicitly assign the format type. For example:

```
FORMAT:SNVT_switch
```

User Network Variable Type (UNVT) Device Resource Files

This is a set of files created by device manufacturers to describe non-standard network variables. Using the same mechanisms as the standard resource files, they describe how to format data from a particular manufacturer's device. On the *i*.LON 1000, all device resource files will be found in the directory `/root/lonworks/types`.

UNVT formats must be specified using a fully qualified format name of the form:

```
#<progID>[<selector>].<format name>
```

In this syntax, the "#", "`[`", "`]`" and "`.`" characters are literal characters. The program ID is represented as a hex byte string (in the "`RAW_HEX_PACKED`" format described below). The selector is a one-digit string from 0 to 6, and the format name syntax is similar to that used for SNVT types, except that the type name starts with "UNVT" instead of "SNVT". For example:

```
FORMAT:#8011223344556677[1].UNVT_switch
```

Built-in Formats

Built-in formats are provided by the underlying formatting engine, and they include "`RAW`", "`RAW_HEX`", and "`RAW_HEX_PACKED`". All of these formats display the network variable data byte-by-byte, in the same order that the bytes arrive on the network (the Neuron has Big Endian byte ordering, the opposite of the PC's Little Endian ordering, and network variable data must be in Big Endian order on the LONWORKS network). The "`RAW`" format displays the data as decimal byte values, with each byte separated by a space. The "`RAW_HEX`" format

displays the data as hexadecimal byte values, with each byte separated by a space. The "RAW_HEX_PACKED" format displays each byte as a two-digit hex value, with no spaces in between the byte values.

The "RAW_HEX_PACKED" format is the default format for non-SNVT network variables that do not specify a format.

PROPAGATE:

The PROPAGATE: attribute allows you to specify whether a value should be transmitted across the network immediately, or buffered. For example:

```
<iLonWeb FUNC=TextField
SYMBOL=NVL_DigitalOut!FIELD:value!PROPAGATE:TRUE></iLonWeb>
```

The PROPAGATE: attribute defaults to TRUE when a tag references a complete network variable, and FALSE when a tag references a network variable field. Network variable fields may not be manipulated individually over the LONWORKS network—the entire network variable value can be changed, but not one field at a time. These default settings are designed to assure that updates are consistently delivered for the specified network variable. In addition, it is typically more efficient to update several fields and propagate the network variable once, instead of causing propagation for each field update.

If your HTML form sets a network variable value field-by-field, the propagate attribute should be set to FALSE for all of the network variable field tags in the form except the last one. The last propagate attribute of TRUE will cause the network variable value to be propagated over the network. Note that if you set propagate to TRUE for each field, some fields may contain indeterminate values in the network variable update, which should not be propagated.

WAIT:

The WAIT: attribute allows you to specify whether to wait for the acknowledgement of a write command. Using the wait feature, you may test whether a local output network variable's update is acknowledged by the remote inputs. The test will only be valid if the local output network variable is connected to one or more remote network variables by the acknowledged address services. If the connection is made by an unacknowledged message service, the test will always return a positive response, even if the network variable update did not reach its target.

To perform the test:

1. Set the WAIT: attribute to TRUE by adding !WAIT=TRUE to the web tag responsible for writing the network variable. This causes the data server to wait for an acknowledgement (ACK) or failure from the network variable before returning from processing that field.
2. Modify the web page so it reads back the results of the acknowledgement. Following the update tag, place a ShowValue tag for the same network variable and specify a field name of "$ErrStatus" (!FIELD:$ErrStatus). This field returns the value of the network variable's error status.

If all of the expected acknowledgments were received, the returned error string will be empty. If any acknowledgements failed, the string "No acknowledgement from remote network variable" will be returned. Since an empty error string will be returned on success,

you can always display the error string, perhaps in a color indicating that an error condition exists.

Working with Forms

Forms are used in web pages to get information from end users. HTML form elements allow you to present and collect that information by using input objects such as text boxes and check boxes. **Only one form is recommended for each page.** See *Form Element Functions* later in this manual for further information.

A function within the *i*.LON 1000 web tag, called a form element function, invokes a routine that performs a specific task. The form element function acts upon the network variable that you specify in the SYMBOL= attribute. Other attributes may further qualify what the function does, such as formatting the output or displaying a specific field within a network variable.

The following web tag uses the check box function and assigns a value of 1 to the state field of the DigitalOut network variable when the user selects this checkbox in a web page.

Opening a Form

To include a form in a web page, start with a HTML document then insert the appropriate `<iLonWeb>` tags to build your form. The first step in building a form is to use a form element function to open a form.

<FORM ACTION=filename.htm METHOD=GET><iLonWeb_URL></FORM>

Web Tag Element	Description
<FORM >	This tag is standard HTML and signals the start of a form.
ACTION=	This attribute is standard HTML and identifies what happens to the data when the form is submitted for processing. ***Netscape Users: See the browser constraint information in the next section.***
METHOD=	This attribute defines the method used to send data to the server. GET is the supported method and sends data to the server by appending the data to the URL itself after a question mark (?) separator. POST is *not* supported.

<iLonWeb_URL>	This tag is required between the <FORM> and </FORM> tags. This tag implements a security feature by creating a hidden field that is the URL of the page containing the form. The form processor checks the URL to ensure the users are accessing only the variables that they are authorized to access.
</FORM>	This tag signifies the end of the form.

Important! While it is recommended that you use only one form per page, *i*.LON 1000 Web server will support multiple forms on the same page on the condition that each read-write network variable defined on the page is defined on one form only. This prevents unintentional updating of network variables.

Netscape Browser Constraint

When using a Netscape web browser, you must set the ACTION= attribute to the name of the file that you are creating. For example, if you are creating a web page called "testpg.htm", set the ACTION= attribute as follows:

```
<form method="get" action="testpg.htm">
   <iLonWeb_url>
   <iLonWeb func=TestField symbol=NVL_DigitalOut!propagate:TRUE>
   </iLonWeb></p>
   <p><input type="submit" name="Submit" value="Submit"></p>
</form>
```

If the Action of the form is not set, the "File not found" error will be shown on a return page from the Web server.

Submit or Reset a Form

Once information has been entered into a form, the form must be submitted to the server. This is accomplished using the Submit function. Alternatively, a form that has not already been submitted can be restored to its original values using the Reset function. These two functions, Submit and Reset, are standard HTML form elements that control forms in web pages. For information on their use and syntax, consult a standard HTML reference.

When used in conjunction with the *i*.LON 1000 web tags, the Submit function creates a button that, when clicked, informs the *i*.LON 1000 Web server to update those read/write network variables whose values are displayed on forms in the page. The reset function creates a button that resets any form element to its original value, or, if a submit button was clicked, to its most recently submitted value. For example:

```
<INPUT type="submit" value="Write NV">
<INPUT type="reset" value="Reset modifications">
```

Important! Clicking the submit button causes all forms on a page to submit their data to the server, even if no change has been made to a form. While the *i*.LON 1000 Web server

will support multiple forms per page, provided each form references a unique network variable, it is recommended that only one form be used per page, to avoid the unintentional updating of unchanged network variables.

Refresh a Form

After submitting a value to update a network variable, the URL is appended with the submitted value in the browser's address window. If you subsequently use the web browser's Reload button (Netscape) or Refresh button (IE) to try to obtain the current value of the network variable, the value appended to the URL is written to the network variable instead. Instead of using the web browser's Reload or Refresh button, create your own Refresh button to obtain the current value of a network variable that is defined in your web page. This function will get the latest value of the network variable and display it when the web page is reloaded. For example:

```
<INPUT type="button" value="Refresh"
onClick="window.location.assign(window.location.pathname)">
```

When you click on a Refresh button in a form to reload a web page, the browser might load the web page from cache memory. That cached web page could contain old network variable values. To force the browser to load a new page, add the following Meta web tag in the <head> tag of the web page.

```
<head>
<META HTTP-EQUIV="Expires" CONTENT="Tue, 25 Apr 1995 09:30:00 -0700">
</head>
```

As an alternative to using the Refresh button, create a link to the current web page:

```
<a href="iLonTest1.htm"><b>Refresh</b></a>
```

Form Element Functions

This section describes the form element functions supported by the *i*.LON 1000 Web server. The following table lists the *i*.LON 1000 Web server form element functions and their actions. Unlike most HTML elements, the *i*.LON 1000 web tag functions are case sensitive.

Function	Action on the Specified Network Variable
CheckBox	A value of 1 is selected for the specified network variable when the user checks the check box, a value of 0 is written if the box is unchecked.
Hidden	Hides the text field that contains the value of the specified network variable.
RadioButton	The value assigned to a radio button is selected for the specified network variable when the user clicks it.
TextArea	Displays the value of the specified network variable with access to modify it.
TextField	Displays the value of the specified network variable with access to modify it.

CheckBox

A Check Box is an object that presents the user with a choice to select or deselect an option. The CheckBox tag creates a check box in your web page form and sends a value of 1 to the form processor when the user selects the check box and submits the form for processing. The form processor will set a value of 0 for a deselected check box.

The web tag example below creates a CheckBox object in a web page form. The table that follows describes each web tag element.

```
<iLonWeb FUNC=CheckBox SYMBOL=NVL_nvoCbx1></iLonWeb>
```

Web Tag Element	Description
`<iLonWeb>`	The *i*.LON 1000 tag.
FUNC=CheckBox	Specifies the CheckBox function and causes a checkbox to be created in the form.
SYMBOL=NVL_nvoCbx1	Specifies that the local network variable called `nvoCbx1` is the symbol that a value is written to when the user selects the checkbox in the form.
</iLonWeb>	The ending *i*.LON 1000 tag.

Hidden

The Hidden function allows you to include text in your web page without displaying it on the screen. This function is useful when you want to make network variable values available to a program, like JavaScript, but not for users to see or edit. For example, the following web tag hides the value of the NVL_nvoDigital network variable on the web page.

```
<iLonWeb FUNC=Hidden SYMBOL=NVL_nvoDigital></iLonWeb>
```

Web Tag Element	Description

<iLonWeb>	The *i*.LON 1000 tag.
FUNC=Hidden	Hides the text field that contains the value of the specified network variable.
SYMBOL= NVL_nvoDigital	Specifies the local network variable called nvoDigital on the web page.
</iLonWeb>	The ending *i*.LON 1000 tag.

RadioButton

Radio buttons are objects that present the user with a series of items and allow the user to choose one item from the series. A value is assigned to each radio button defined in the tag, and when the user selects a radio button, the corresponding value is sent to the form processor.

The following web tag example creates a series of radio button objects in a web page form. The table that follows describes each web tag element.

```
<iLonWeb FUNC=RadioButton SYMBOL=NVL_nvoRb1 VALUE="1"
Checked></iLonWeb>
<iLonWeb FUNC=RadioButton SYMBOL=NVL_nvoRb1 VALUE="2"> </iLonWeb>
<iLonWeb FUNC=RadioButton SYMBOL=NVL_nvoRb1 VALUE="3"></iLonWeb>
```

Web Tag Element	Description
<iLonWeb>	The *i*.LON 1000 tag.
FUNC=RadioButton	Specifies the radio button function and causes a radio button object to be displayed in the form.
SYMBOL=NVL_nvoRb1	Specifies that the local network variable called nvoRb1 be written to when the form is processed.
VALUE="1"	Specifies the network variable update value assigned to the radio button.
Checked	Indicates that this radio button is selected by default.
</iLonWeb>	The ending *i*.LON 1000 tag.

TextArea

A text area is an input field that allows the user to input an amount of information into a form defined by the dimensions of the text area. Input to the text area field is written to the network variable specified in the tag.

This is an example of the TextArea function that creates an input area with 4 rows and 6 columns. The table below describes each web tag element.

```
<iLonWeb FUNC=TextArea TYPE=text SYMBOL=NVL_nvoBuffer ROWS=4
COLUMNS=6></iLonWeb>
```

Web Tag Element	Description
<iLonWeb>	The *i*.LON 1000 web tag.
FUNC=TextArea	Specifies the text area function. Causes a text area in the web page form to be created.
TYPE={text|password}	"Text" specifies the input will appear as text. "Password" specifies that input will appear as asterisks in the text box.
SYMBOL=NVL_nvoBuffer	Specifies that the local network variable called is the symbol that a value is written to when the form is processed.
ROWS=4	Indicates that the text area will be 4 rows high.
COLUMNS=6	Indicates that the text area will be 6 columns wide.
</iLonWeb>	The ending tag

TextField

A text box allows the user to insert a relatively small amount of text information into a form. Use this tag when you want to modify a network variable value.

The text box example and description below creates a text box that is 20 characters wide and allows the user to update a local output network variable named **nvoDigital1**.

```
<iLonWeb FUNC=TextField TYPE=text SYMBOL=NVL_nvoDigital1 SIZE=20
MAXLENGTH=58></iLonWeb>
```

Web Tag Element	Description
<iLonWeb>	The *i*.LON 1000 tag.
FUNC=TextField	Specifies the text field function. Causes a text box to be displayed in the web form.
TYPE={text|password}	"Text" specifies the input will appear as text. "Password" specifies that input will appear as asterisks in the text box.
SYMBOL=NVL_nvoDigital1	Specifies that the local network variable called `nvoDigital1` be written to when the form is processed.
SIZE=20	Indicates that the width of the text box is 20 characters.
MAXLENGTH=58	Indicates that the field is 58 characters long. If `SIZE` is less than `MAXLENGTH`, the input text will scroll within the text box displayed in the browser.
</iLonWeb>	The ending tag

11

i.LON 1000 Web Page Security

This chapter contains information on restricting viewing and modification of *i*.LON 1000 web pages.

Overview of *i*.LON 1000 Web Page Security

The ***i***.LON 1000 Internet Server supports a web page security mechanism 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 Parameters utility. This utility is included in the standard *i*.LON 1000 software distribution and is accessible from the i.LON program group. **(START | PROGRAMS | Echelon i.LON | i.LON Web Server Parameters)** The i.LON Web Server Parameters utility creates a file, WebParams.dat, that must be transferred to the *i*.LON 1000's root directory. (/root/WebParams.dat)

WebParams.dat is parsed by the *i*.LON 1000 on startup to establish web page restrictions. Note that firmware versions 1.00 & 1.01 store WebParams.dat as plain text with no encryption or password protection. This means that *i*.LON 1000 security is protected from inspection by ftp security (user name and password) only. Be sure to set proper user names and passwords for FTP access to prevent WebParams.dat from being viewed. Also, be sure to secure the PC on which you generated the WebParams.dat file.

The *i*.LON 1000's factory default WebParams.dat file allows access to all files found under /root/Web from any location by any user. To modify existing *i*.LON 1000 web security you have to create a new (or edit the existing) WebParams.dat file. The updated file must be transferred (uploaded) to the *i*.LON 1000, and the *i*.LON 1000 must be rebooted for the new security settings to take effect.

To change the security settings on an *i*.LON 1000, follow these steps:

1. Download the existing `WebParams.dat` file from the *i*.LON 1000 using an FTP application.
2. Start the *i.LON Web Server Parameters* application, and open `WebParams.dat` (File > Open menu option).
3. Make the required security changes (see below) and save `WebParams.dat` using the file > Save menu option.
4. Upload `WebParams.dat` to the *i*.LON 1000's `/root` directory using an FTP application.
5. Reboot the *i*.LON 1000 to activate the security changes.

Setting Access Restrictions

Security *Realms* are used to define *i*.LON 1000 access restrictions. A *realm* is defined to be the combination of URL (folder in *i*.LON 1000), group (users group name), and location (IP address range from where the URL may be accessed). In other words, a realm defines which files (URL) may be accessed by which group of users (group) and from which IP addresses (location).

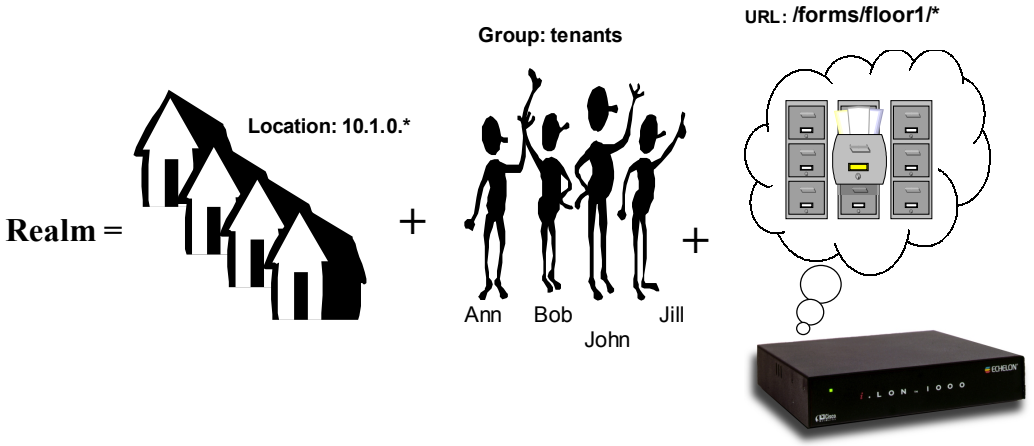


Figure 11-1 – An *i*.LON 1000 Security Realm

URLs are defined with the assumption that you are starting from the root of the web site and not the *i*.LON 1000 device. For example, to restrict access to http://building10/forms/floor3/ the URL must be defined as "/forms/floor3/*". The wildcard is required in order to place this setting across the entire directory. To restrict access to the whole site you need to URL "/*". See Figure 11-2 for examples of URLs. **Note that the leading "/" is required syntax**.

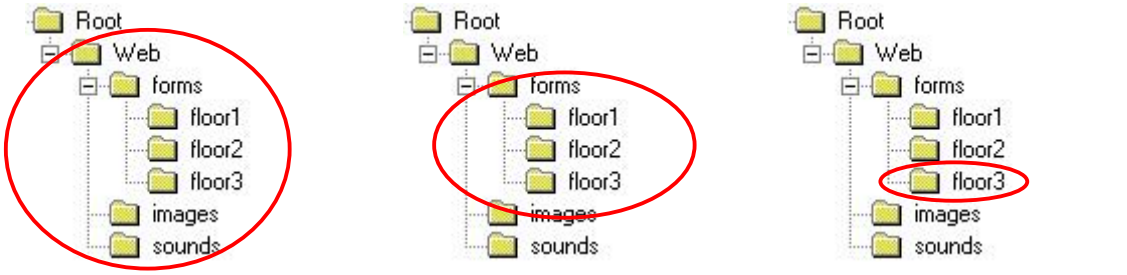


Figure 11-2 – URL Examples

Users and Groups

Each person who will be given access (i.e. a user name and password) to the *i*.LON 1000 is called a user. Users are organized into groups. Each user can be in exactly one group, and all users in a given group will have identical access. If each user must have different access rights, you must define a group for each user.

In order to define a group you must first define a list of users and passwords, for example,

```
Ann : boxcar
Bob : trumpet
John : foxtrot
Jill : mustang
superuser : sfs43fs6f
```

Users are then grouped together based on the *i*.LON 1000 web folders that they are going to access. For instance, if Ann, Bob, Jill and John live in the same building, you could group them by floor. Ann, Bob, and Jill have apartments on the second floor, Bob also happens to have a workshop on the first floor. Finally, John has an apartment on the third floor. The property management company maintains the web site. Their web master has the access name superuser. Table 11-1 shows which users are to have access to which folders.

Table 11-1 – Example ***i*.LON 1000** Web Page Security Chart

	floor 1	floor2	floor3
Ann		x	
Bob	x	x	
Jill		x	
John			x
superuser	x	x	x

The *i*.LON security mechanism allows each user to be a member of one group only. Thus, the 4 groups will need to be created. One each for access to floors 1 & 2 (Bob), floor 2 (Ann, Jill), floor 3 (John), and all floors (superuser):

To set up the users and groups described above, follow these steps:

1. Setup usernames and passwords from the **users** tab of the *i.LON Web Server Parameters* application as shown in Figure 11-3.

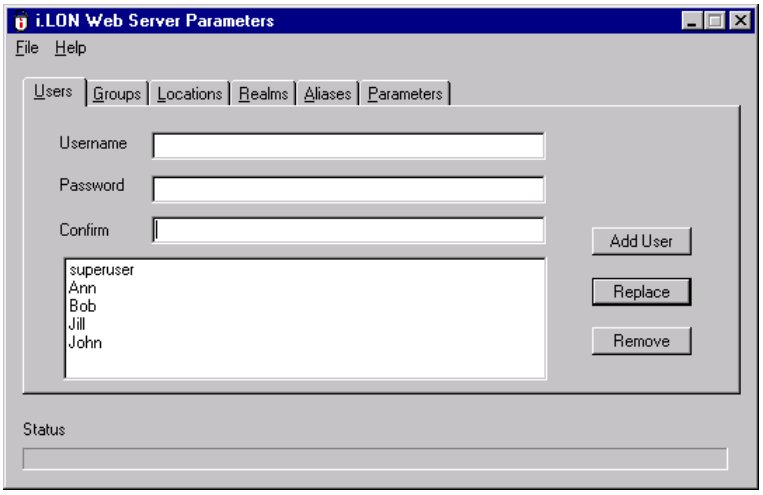


Figure 11-3 – Creating *i*.LON 1000 Users

2. Once all the user names and passwords have been entered, create the necessary groups using the Groups tab of the *i.LON Web Server Parameters* application as shown in Figure 11-4.

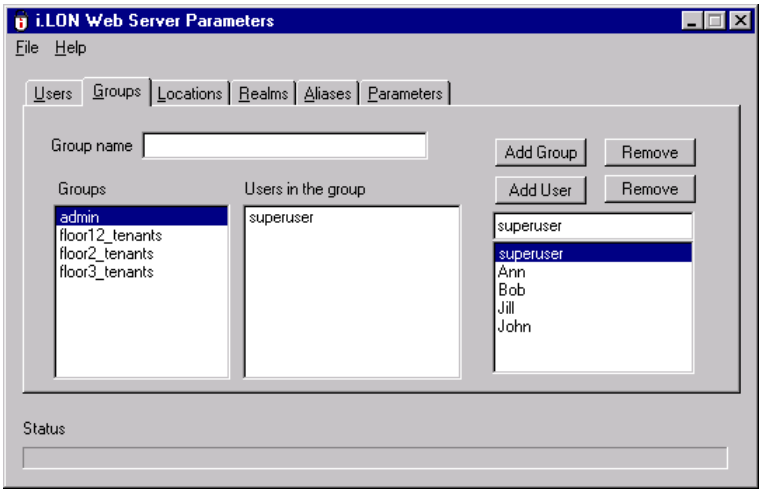


Figure 11-4 – Creating ***i*.LON 1000** Groups

3. Finally, add users to specific groups by selecting the group and then clicking the **Add User** button for each user you want to add to the group.

Locations

Locations are defined as ranges of IP addresses from which a particular group of users can access a particular folder. "*" is used as a wildcard. Examples:

Location name	IP address range	Comments
All	*.*.*.*	Any IP address
Tenants	10.1.0.*	Any host with IP in the range 10.1.0.1 – 10.1.0.254 Note that 10.1.0.0 is a network address and 10.1.0.255 is a broadcast address, hence they are not included
Topgun	10.1.0.10	IP address of the host used by superuser (property manager) to update web pages

Use the *i.LON Web Server Parameters* application's **Locations** tab to define these locations as shown in Figure 11-5.

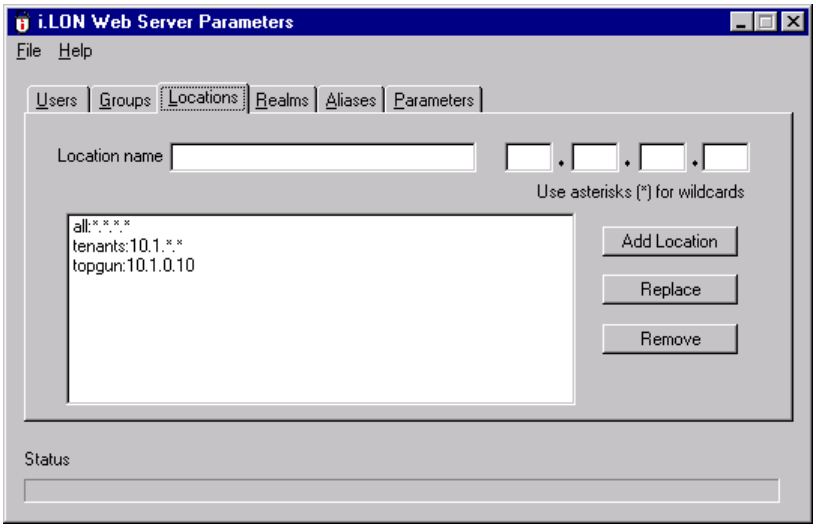


Figure 11-5 – Setting ***i*.LON 1000** Locations

Note that if you declare a location "A" that happens to be a subset of another location "B", it is assumed that "A" is not included in the access rights of users in location "B". For example:

```
topgun: 10.1.0.10
tenants: 10.1.*.*
all: *.*.*.*
```

This declaration actually means that `tenants` is the whole range 10.1.*.* with the exception of 10.1.0.10. Similarly, `all` excludes 10.1.*.*.

Realms

Realms define the folders the various groups and locations are allowed to access. Each realm is in the format `URL:GROUP:LOCATION`, where users from `GROUP` and `LOCATION` are given access to the `URL`. These values can be selected in the Realms tab of the i.LON Web Server Parameters utility.

For example, design a security setup for an *i*.LON 1000 website that allows users to monitor occupancy information, temperature, and lux level on the floor on which they live. This is a three-story building so we have floors 1, 2 and 3, with corresponding web pages stored in subfolders under /forms: /forms/floor1, /forms/floor2, and /forms/floor3. There are five users that can access this site: superuser, Ann, Bob, Jill, and John. They belong to groups tenants_floor12, tenants_floor2, tenants_floor3, and admin as described above.

Tenants are allowed to access web pages of their floor only, but can login from any local host;

Local hosts may have any IP address in the network 10.1.0.0 / 24 (i.e. 10.1.0.1 – 10.1.0.254). There is one "superuser" that designs web pages, and has unlimited access to the website; for security reasons he will access the site from one host only, with IP address 10.1.0.10; the web site should be restricted to any other users.

Based on this description, the **Realms** tab should appear as shown in Figure 11-6.

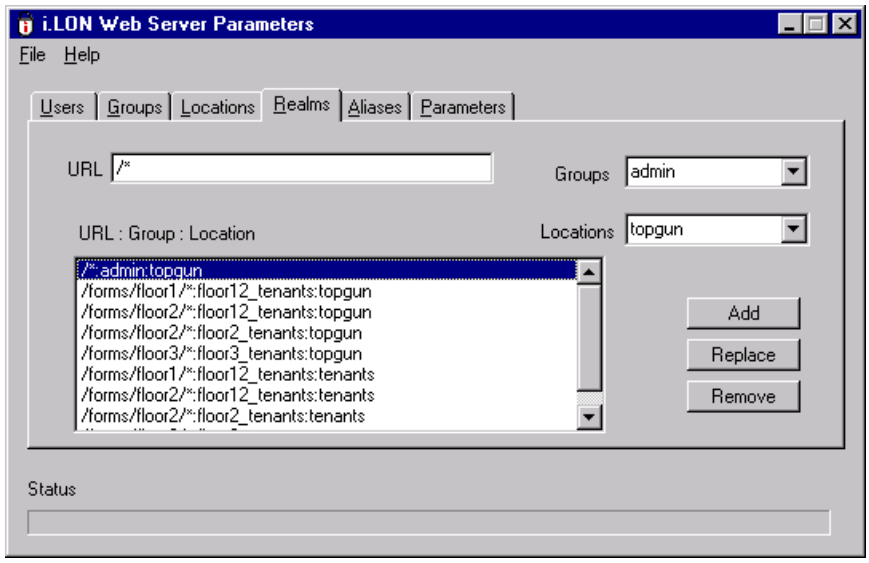


Figure 11-6 – Defining ***i*.LON 1000** Realms

Sample WebParams.dat file

The following WebParams.dat was generated according to the scenario discussed above.

```
iLonSecurity 1.2
GlobalMemoryBytes:16384
RequestMemoryBytes:16384
TaskStackBytes:10240
NumTasks:1
TaskPriority:95
MaxSymbols:100
(Users)
admin:superuser:sfs43fs6t
floor12_tenants:Bob:trumpet
floor2_tenants:Ann:boxcar
floor2_tenants:Jill:mustang
floor3_tenants:John:foxtrot
(Locations)
all:*.*.*.*
tenants:10.1.*.*
topgun:10.1.0.10
```

```
(Realms)
/*:admin:topgun
/forms/floor1/*:floor12_tenants:topgun
/forms/floor2/*:floor12_tenants:topgun
/forms/floor2/*:floor2_tenants:topgun
/forms/floor3/*:floor3_tenants:topgun
/forms/floor1/*:floor12_tenants:tenants
/forms/floor2/*:floor12_tenants:tenants
/forms/floor2/*:floor2_tenants:tenants
/forms/floor3/*:floor3_tenants:tenants
```

12

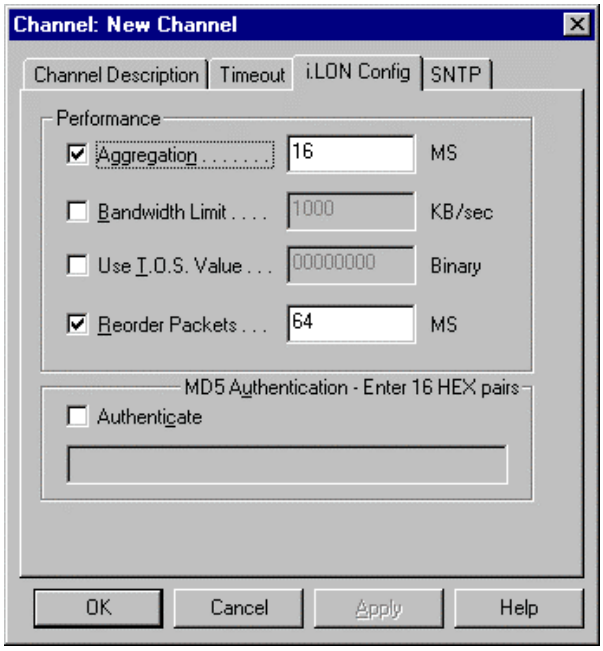
Advanced Topics

This chapter provides detailed information on *i*.LON 1000 advanced topics.

Aggregation

The *i*.LON 1000 router implements aggregation for transporting LONWORKS packets over the IP channel. LONWORKS packets are relatively small in size and often arrive at the *i*.LON 1000 router in bursts or at a high rate. Aggregating packets under these conditions decreases the overhead necessary to send packets over IP, decreases IP network traffic, and greatly increases the performance of the *i*.LON 1000 router.

The *i*.LON 1000 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; set the timer to 16 MS, 32 MS, or accordingly.



If the network is idle and a single LONWORKS packet arrives at the *i*.LON 1000 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.

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 1000 prepares to send an IP packet, the *i*.LON 1000 uses the authentication key and the public MD5 algorithm to compute a digest over each LONWORKS packet (or APDU) in the UDP payload. The APDU is identical to the packets described in the draft LONMARK RFC 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 1000 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 1000 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 1000 through the Console Application. 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.

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. Select the **i.LON Config** tab.

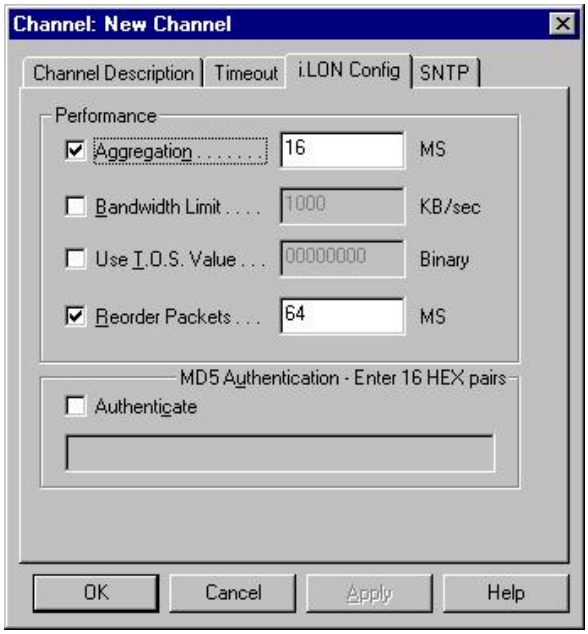


Figure 12-1 – i.LON Config Tab

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

   All authentication keys within a single network must match. Be sure that you have previously entered the same authentication key on the *i*.LON 1000 devices defined on this channel using the Console Application.

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

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

Device Resource Files

To install or upgrade device resource files on the *i*.LON 1000:

1. Stop the Web server before installing the files. Using the Configuration Server, select the ***i*.LON Control** tab in the device properties option and click on **WebServer Stop** or use the **deactivate** console command.
2. Use a FTP program to upload device resource files from the source to the *i*.LON 1000. Transfer the files to the `/lonmark/types` directory. If you are upgrading the standard device resource files on the *i*.LON 1000, you may download the source files from the LONMARK web site at www.lonmark.org.
3. Start the Web server after installing the files. Using the Configuration Server, select the ***i*.LON Control** tab in the device properties option and click on **WebServer Start**.

Using DHCP with *i*.LON 1000 Devices

While the *i*.LON 1000 supports DHCP to retrieve its IP address, subnet mask, and gateway address, manual configuration of these values provides several advantages over using DHCP. Consider the following:

- **DHCP Server Failure.** If the DHCP server fails, the *i*.LON 1000 will not be able to retrieve its addresses, and as a result will not function after a reboot. Manual configuration of the *i*.LON 1000 addresses eliminates this potential failure mode.
- **Maintenance**. Each *i*.LON 1000 router may require an individual address reservation in the DHCP server. Creating these address reservations typically includes collecting the MAC Ids from each *i*.LON 1000. Replacing an *i*.LON 1000 requires changing the DHCP reservation as well. The use of redundant DHCP servers requires replicating DHCP reservations.
- **Additional Configuration.** Using DHCP on the *i*.LON 1000 does not eliminate a configuration step or allow for entirely remote configuration, as it might for some IP hosts. Using DHCP adds an extra step, since you must use the *i*.LON 1000 console to configure several parameters, in addition to making the DHCP server reservations.

If you decide to use DHCP, you must decide whether or not your *i*.LON 1000 should have a static IP address. A static address is one that does not change each time the *i*.LON 1000 boots. A manually configured address is static. DHCP servers typically do not provide static address, but they can generally be configured to do so. An *i*.LON 1000 must have a static IP address if any of the following are true:

- The *i*.LON 1000 will run the Router application.
- The *i*.LON 1000 will be controlled using the Configuration Server.

You do not need to use a static address if you are running the *i*.LON 1000 Web server only and do not want to manage it with the Configuration Server. If your *i*.LON 1000 needs a static address, your network administrator will need to create an individual address reservation for it in the DHCP server, most likely using the Ethernet MAC ID of the *i*.LON 1000.

To use DHCP on the *i*.LON 1000, you must enable it from the Console Application using the command `dhcp on`. The DHCP server must have been configured to provide the following information:

- IP Address
- Subnet Mask
- Gateway Address (optional)

The values listed above are the only information obtained from the DHCP server by the *i*.LON 1000.

DHCP Server Failure

If an *i*.LON 1000 with DHCP enabled boots up and fails to retrieve its IP address, subnet mask, and gateway address from the DHCP server, the *i*.LON 1000 will remain in a loop, continuously attempting to retrieve this information, until you manually intervene.

To restore the *i*.LON 1000 to regular operation, follow these steps:

1. Open the Console Application and reboot the *i*.LON 1000 by pressing Control-X. Interrupt the boot process by pressing the "!" when instructed, as described in *Interrupting the Boot Process* in Appendix A. The command prompt reappears.
2. Issue the command **`dhcp`** `off`, to disable DHCP.
3. Enter the IP address, subnet mask, and gateway address using the console commands to assign that information to the *i*.LON 1000.
4. Issue the `reboot` command to apply the new address changes to the *i*.LON 1000.

i.LON 1000 System Event Log

The *i*.LON 1000 maintains a history of significant system events to track and help technical support personnel 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 1000's root directory (`/root/eventlog.txt`). System events are logged to the file when the eventlog feature is enabled on the *i*.LON 1000 through the Console Application.

To view the event log file, first transfer the file as text 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:

Urgent Trace 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 time servers configured. 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 DataServer: persistent data lost due to <reason> Suggested action: recommission the router or	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: 1 **"an image corruption"** – The image file located in /root/ltConfig was corrupted.

Urgent Trace Message	Description
application instance.	2 **“a program ID change" -** This might occur when changing the application mix 3 **"a signature mismatch" -** The image file was corrupted. 4 **"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. Try deleting 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. Try deleting unused files or running chkdsk.
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 1000 box has changed. This is expected after the IP address has been changed and the box rebooted. The box 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 *i*.LON 1000 Configuration Server.
Startup - Server start failed	An unforeseen error has prevented a proper startup. Consider setting "factory defaults" through the Console Application.
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.

Using *i*.LON 1000 Devices with SNMP

The *i*.LON 1000 supports SNMP v1/v2 protocols and comes standard with MIB II support for managing networked devices. The SNMP agent runs a task on the *i*.LON 1000 and responds to requests for device information from an IP network manager such as Netview or HP OpenView. Using an IP network management tool, you can retrieve a sequence of MIB variables to report a number of IP statistics such as the device’s IP address, MAC identifier, and packet counts. Refer to your IP network management tool for further information on reporting IP statistics.

The SNMP configuration file, **snmpd.cnf**, is installed on the *i*.LON 1000 in the `/root/snmp` directory and contains standard writable and non-writable SNMP values. Two communities, *private* and *public*, are defined and, by default, give users write access to the SNMP values. The configuration file can be modified to specify a trap community, add and change

communities for specifying access to SNMP values, and change the sysName, sysLocation, and sysContact variables.

A backup copy of the configuration file exists in `\lonworks\iLON\Images\iLON 1.00\snmp` on the PC for restoring the file if needed. The *i*.LON 1000 copy of the file gets overwritten upon reboot and, as a result, any comments, such as which values can be changed, are lost.

Appendix A

i.LON Console Application Reference

This appendix provides an overview of the Console Application and describes the console commands, the *i*.LON 1000 boot process, and the line editor.

Console Application

The *i*.LON 1000 contains a console application that is accessed by connecting to the *i*.LON 1000's *console* port using a terminal emulator, as described in Chapter 4, *Using the i.LON Console Application*. The console application allows you to control the *i*.LON 1000's operation, and set basic parameters such as the *i*.LON 1000's IP address, subnet mask, and FTP username and password. Console commands are entered through a simple command-line interface.

Interrupting the Boot Process

The *i*.LON 1000 undergoes an extensive boot process upon power-up and when reset by the reset button or a reboot command issued in the Configuration Server or console application. During the boot process, the *i*.LON 1000's disk structure is automatically checked to ensure that any structural errors on the disk are repaired (similar to running a check-disk 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 1000 system image. Successful completion is indicated when the *i*.LON 1000 displays its normal command-line prompt.

If the *i*.LON 1000 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 1000. 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 1000 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 1000 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 1000 software to restore proper operation.

While in the bootrom state, only a subset of the normal console commands are available. The *i*.LON 1000 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.

Console Command List

The console application provides a command line interface through which you issue a set of console commands to control the operation of the *i*.LON 1000. This section provides a complete list of console commands. This list can be displayed by typing help all at the command prompt.

The syntax for the console commands listed in Table A-1 is: **command** *argument*

Table A-1 – Console Commands

Command	Description
activateapp *index | name*	Activates an application instance, specified by index or name. Only the following are supported: Router (1) DataServer (2) WebServer (3)
authkey *key*	Modifies/sets the authentication key. Specify key in hexadecimal (spaces permitted).
cd [*directory*]	Change directory, or show directory if no argument.
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 upon creation. See **activateapp** for supported names.
date *dd/mm/yyyy*	Modifies/sets the date. Not allowed if the device is synched to a time 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. Primarily used for troubleshooting.
delete *file*	Deletes a file or directory.
dhcp [*on|off*]	Indicates whether DHCP will be used to retrieve the *i*.LON 1000's IP address, subnet mask, and gateway address. Set DHCP to *off* to manually configure the IP address, subnet mask, and gateway address. See *Using DHCP with i.LON 1000 Devices* in *Reference* for more information on using DHCP.
dir [*directory*]	Lists file directory contents.
factorydefault	Restores the *i*.LON 1000 settings to the factory default settings. Any files, such as web pages, added by the user are not affected.
format	Formats the flash disk. **Caution!** This command deletes all files, including the *i*.LON 1000 System image file. After using this command, you must upload a new software image to the *i*.LON 1000.
ftppassword *password*	Sets the FTP password to *password*. A required parameter; anonymous FTP not allowed.
ftpuser *name*	Sets the FTP user name to *name*. A required parameter; anonymous FTP not allowed.
gateway *address*	Modifies/sets the gateway address e.g. gateway 10.1.10.1
help [all | *command*]	Displays a listing of the common console application commands, the full command set, or a help description for the specified command.
hostname *name*	Modifies/sets the host name of the *i*.LON 1000 as used by DHCP
install *idx [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 1000 Web server to a pre-installed network. **Echelon does not recommend or support using this command**. Both the Web server and *i*.LON 1000 router should be installed using a standard network installation tool such as LonMaker.
ipaddress *address*	Modifies/sets the *i*.LON 1000's IP address e.g.: ipaddress 10.1.253.100
listapp	Lists the current application instances.
mkdir *directory name*	Creates a directory.

Command	Description
ping *host address*	Tests the communications to another IP host.
reboot	Reboots the *i.*LON 1000.
removeapp *index* | *name*	Deletes an existing application instance, specified by index or name. See **activateapp** for supported names.
rename *file1 file2*	Renames *file1* to *file2*.
servicepin *index*	Sends a service pin message for the application specified by *index*.
sntpaddress *address [address2]*	Sets the SNTP address for diagnostic purposes only. Set SNTP addresses for normal use through the Configuration Server application. The addresses set with this command will override those SNTP addresses set with the Configuration Server application. This setting is not persistent over a reboot; the SNTP server information set in the Configuration Server will take effect after a reboot.
sntplog [*on*|*off*]	Enables or disables SNTP logging. Note that 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/sets the subnet mask, e.g. subnetmask 255.255.255.0
time *hh*:*mm*:*ss*	Sets the time. Not allowed if the device is synched to a time server.
timezone *zone*	Use this command for diagnostic purposes only. Set the timezone of the *i.*LON 1000 through the Configuration Server. This command sets the time zone with the following format: <name_of_zone>:<time_in_minutes_from_UTC>:<dst_used>:<daylight_start>:<daylight_end> where <dst_used> 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 2am. 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.
trace level *number*	Sets the tracing level; 0 = None; 1 = Urgent tracing only (default); 2 = Verbose tracing (for debugging only, not recommended)
type *filename*	Displays the file contents. **Warning!** Do not use this command with binary files.

Special Control Commands

Ctrl X

When the Console Application is active, the keystroke, Ctrl X, reboots the *i.*LON 1000. Use the Ctrl X keystroke as a last resort to reboot in cases when the system is hung and will not respond to console commands. Be careful not to use this command unintentionally.

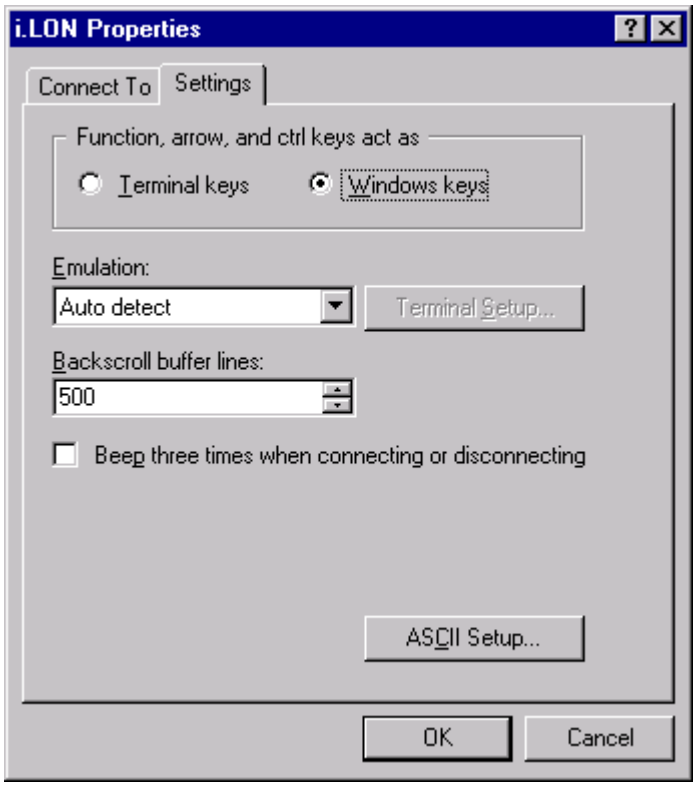
Ctrl C

The keystroke, Ctrl C, terminates the execution of any console command.

Command History and Line Editing

The console application includes command history and line-editing features. The command history recalls the last 20 typed commands and the line editor provides keystrokes to edit previously typed commands.

If you are using HyperTerminal as the terminal emulator to connect to the *i*.LON 1000 console application, set your function, arrow, and control keys to function like in Windows. Select **Properties** from the File menu, click on the **Settings** tab and select the **Windows keys** radio button.



Line Editor Commands

To edit a command, press the ESC key to enter edit mode, and use the commands listed below. Certain commands (e.g., 'i') will enter an input mode and allow you to type characters into the command line. The ESC key will return the command editor to edit mode. The RETURN key always gives the line to the command processor from either editing or input mode.

The following list is a summary of the commands available in edit mode.

Movement and search commands

*n*G	- Go to command number *n* .
/*s*	- Search for string *s* backward in history.
?*s*	- Search for string *s* forward in history.
n	- Repeat last search.
N	- Repeat last search in opposite direction.

*n*k - Get *n*th previous command in history.
n- - Same as k.
*n*j - Get *n*th next command in history.
n+ - Same as j.
*n*h - Move left *n* characters.
BACKSPACE - Same as h.
*n*l - (letter el) Move right *n* characters.
SPACE - Same as l.
*n*w - Move *n* words forward.
*n*W - Move *n* blank-separated words forward.
*n*e - Move to end of the *n*th next word.
*n*E - Move to end of the *n*th next blank-separated word.
*n*b - Move back *n* words.
*n*B - Move back *n* blank-separated words.
f*c* - Find character *c*, searching forward.
F*c* - Find character *c*, searching backward.
^ - Move cursor to first non-blank character in line.
$ - Go to end of line.
0 - Go to beginning of line.

Insert commands

Input is expected until ESC is pressed.

a - Append.
A - Append at end of line.
c SPACE - Change character.
cl - Change character.
cw - Change word.
cc - Change entire line.
c$ - Change everything from cursor to end of line.
C - Same as c$.
S - Same as cc.
i - Insert.
I - Insert at beginning of line.
R - Type over characters.

Editing commands

*n*r*c* - Replace the following *n** characters with *c*.
*n*x - Delete *n** characters starting at cursor.
*n*X - Delete *n** characters to the left of the cursor.
d SPACE - Delete character.
dl - Delete character.
dw - Delete word.
dd - Delete entire line.
d$ - Delete everything from cursor to end of line.
D - Same as d$.
p - Put last deletion after the cursor.
P - Put last deletion before the cursor.
u - Undo last command.

~ - Toggle case, lower to upper or vice versa.

*The default value for *n* is 1.

Special commands

^U - Delete line and leave edit mode.
^L - Redraw line.
RETURN - Leave edit mode and give line to command processor.

Appendix B

Web Page Examples

This appendix explains how to install and use the Web server application example, including a LonMaker network and web pages, that ships with the *i*.LON 1000.

i.LON 1000 Web Server Application Examples

The *i*.LON 1000 PC software includes examples of Web server applications that illustrate and explain how the *i*.LON 1000 can be used as a Web server. After setting up these Web server examples, you will be able to monitor and control your LonPoint devices through a web browser. To use the examples, you must provide the following:

- 1 - LonPoint digital input device
- 1 - LonPoint digital output device
- 1 - *i*.LON 1000 devices
- LonMaker Integration Tool version 2.0 (or higher)
- Web Browser: Internet Explorer 4.0 and higher, or Netscape Navigator 4.0 and higher

The example files include:

- **ILON_example.zip**. A LonMaker database and drawing located in the `\lonworks\iLON\Examples` PC directory.
- Several HTML web pages located in the `\lonworks\iLON\Examples\WebPages` PC directory.
  - `exampg1.htm`
  - `exampg2.htm`
  - `exampg3.htm` (contains `exampg31.htm`, `exampg32.htm`, and `exampg33.htm`)
  - `exampg4.htm` (contains `exampg41.htm`, `exampg42.htm`, and `exampg43.htm`)
  - `exampg5.htm`
  - `exampg6.htm`
- The default web page, `index.htm`, located in the `/root/Web` directory of the *i*.LON 1000.
- The following example user types and formats should be copied from the PC's `\lonworks\iLON\Examples\types` directory to the `/root/lonworks/types` directory on the *i*.LON 1000.
  - `ilonexa.enu`
  - `ilonexa.fmt`
  - `ilonexa.fpt`
  - `ilonexa.typ`

You must reboot the *i*.LON 1000 after these files are copied.

See the *Web Page Examples* section for a description of how each example web page functions.

To set up the Web server application example:

1. Install the *i*.LON 1000 devices and LonPoint devices.
2. Open LonMaker and restore the example database and drawing from the `\lonworks\iLON\Examples` PC directory.
3. Commission the *i*.LON 1000 devices, LonPoint devices, and Web server.

4. Use FTP to upload the HTML web page examples and type files to the *i*.LON 1000 acting as the Web server. Upload the web page files to the `/root/Web/forms` directory. Upload the type files to `/root/lonworks/types`.
5. Stop and start the Web server using the Configuration Server. Select the device acting as the Web server, click on the *i*.LON Control tab in Device Properties, and click **Stop Web Server**. To restart the Web Server, click **Start Web Server**.
6. Use a web browser to view the example web pages. Enter the IP address of the *i*.LON 1000 Web server into the address field in your web browser along with the directory of the web page that you wish to view.

Web Page Examples

This section describes the functionality of each web page provided with the Web server application example. In general, the web pages are designed to display text, form elements, and both local and remote network variables values using various functions to demonstrate the possibilities when you are building your own web pages.

Monitor Local Network Variable (exampg1.htm and exampg6.htm)

The web pages exampg1.htm and exampg6.htm allow you to monitor a local network variable defined on the *i*.LON 1000 Web server. The local input network variable is bound to an output network variable on a LonPoint digital input device. When the LonPoint output network variable value changes, that value is propagated over the network to update the local input network variable on the *i*.LON 1000. You can see the new value of the local network variable through the web page by clicking on the Refresh button to display the most recent network variable values.

In exampg1.htm, the network variable is displayed on the web page as both a standard type (SNVT_switch) and user-defined type (UNVT_switch). It is formatted on the web page to display the two fields within the SNVT_switch and UNVT_switch network variable types: value and state. In exampg6.htm, the network variable is displayed as a standard type (SNVT_switch) and is formatted to display as one value.

Monitor a Remote Network Variable (exampg2.htm)

The web page `exampg2.htm` allows you to monitor a remote output network variable defined on a LonPoint digital input device. As the output network variable changes on the device, the new value can be seen on the web page by clicking on the Refresh button to display the most recent network variable values.

The output network variable is displayed on the web page as both a standard type (SNVT_switch) and user-defined type (UNVT_switch). It is formatted to display the two network variable fields defined in a SNVT_switch and UNVT_switch: value and state.

Change a Local Output Network Variable (exampg3.htm)

`Exampg3.htm` displays and allows you to change the value of a local output network variable defined on the *i*.LON 1000 Web server. The local output network variable is bound to a remote input network variable on a LonPoint digital output device. When a new value is entered through the web page and the Write NV button is clicked, the local output network variable is modified and the new value is propagated to its connected input network variable. The new value appears in the web page when the web page is refreshed.

You can also modify the remote input network variable from this page by entering a new value and clicking on the Write NV button. The value is changed on the remote device, but is not reflected on the *i*.LON 1000 device since this is an update to a remote input network variable.

This web page uses frames to format the page and display the SNVT_switch network variable values for the value and state fields.

Change a Remote Input Network Variable (exampg4.htm)

`Exampg4.htm` displays and allows you to change the value of a remote input network variable defined on a LonPoint digital output device. When a new value is entered through the web page and the corresponding Write NV button is clicked, the new value is propagated to the remote input network variable. This web page uses frames to format the page and display both the SNVT_switch and UNVT_switch type network variable values for the value and state fields.

Evaluate and Calculate with JavaScript (exampg5.htm)

This web page, `exampg5.htm`, displays and evaluates four switch inputs defined locally on the *i*.LON 1000 Web server. JavaScript calculates a "Result" based on the input of the 4 input network variables. If all of the input network variables are equal to 1, the calculated value is 1. Otherwise, the calculated value is 0. This web page demonstrates using JavaScript to generate the result of a logical AND operation on all 4 inputs.

Display the Local *i*.LON 1000 Symbol Values (index.htm)

This web page, `index.htm`, is displayed as the default page for the *i*.LON 1000 device and confirms your connection to the *i*.LON 1000 Web server. It is linked to `localConfig.htm`, a page that displays the values of the local *i*.LON 1000 symbols.

Appendix C

Client Side Programming Examples

Today's advanced web browsers support a variety of scripting languages that allow code to be executed on the client (browser). The two most popular scripting languages are VBScript, developed by MicroSoft Corp. and JavaScript developed by Netscape Communications in cooperation with Sun Microsystems. Both of these scripting languages let you create highly interactive web pages, and both are compatible with the *i*.LON 1000's server side substitution technique of serving network variables to a browser.

A discussion of scripting languages is beyond the scope of this document. This chapter provides two examples of passing network variable information to a scripting language.

Loading a Network Variable Value into a JavaScript Variable

Loading a network variable value into a JavaScript variable is useful when you want to interpret the meaning on a network variable for your user. For example, you may want to print "ON" or "OFF" on your web page instead of the native 100.0 1 or 0 0 returned for a SNVT_switch. The trick is to remember that network variable values returned from the *i*.LON 1000 Internet Server are just strings. This means that you can assign a network variable value to a JavaScript variable in the same way that you assign a string to a JavaScript variable.

```
<HEAD>
<TITLE>EXAMPLE</TITLE>

<SCRIPT>
function printLightState()
{
   // Pick off the two individual components of SNVT_switch

   lightState = "<ilonweb func=ShowValue
symbol=NVL_nviLightState!FIELD:state></ilonweb>";

   lightValue = "<ilonweb func=ShowValue
symbol=NVL_nviLightState!FIELD:value></ilonweb>";


   // Test for the correct definition of "ON" as per LonMark

   if ((lightState) && (lightValue > 0))
   {
      holdstring = "ON"
   }
   else
   {
      holdstring = "OFF"
   }

   // Output a string based on the state/value of SNVT_switch

   document.write(holdstring);
}

</SCRIPT></HEAD>

<HTML>
<BODY>
Current light state is: <SCRIPT>printLightState()</SCRIPT>

</BODY>
</HTML>
```

Automatically Refreshing Web Pages Using JavaScript

Scripting languages allow access to a browser's Document Object Model or DOM. This is a very powerful feature. It allows the web page designer to control the browser's attributes. For example, it is possible to programmatically change a window's background color, or to remove a browser's menus and location box, or resize a browser's window, or launch new instances of the browser, etc.

In the following example, JavaScript is used to access the *window* object through the browser's DOM to cause the web page to reload automatically. The web page generated by this code is shown in figure C-1 (This can also be accomplished by using an HTML META tag, but since this is a chapter on client side programming, we chose to illustrate this technique.)

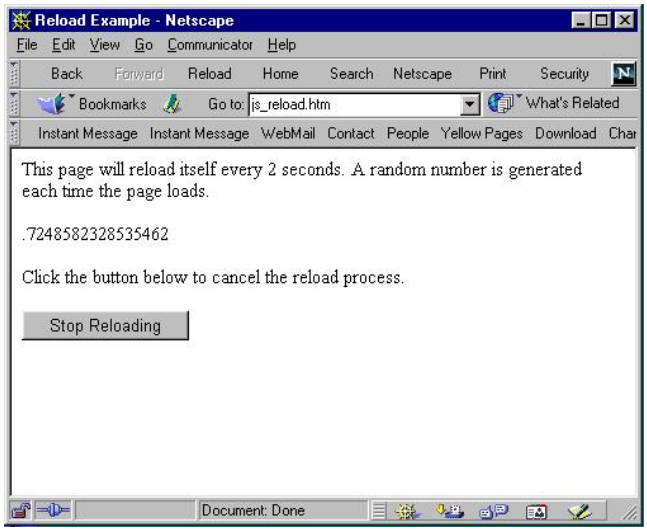


Figure C-1 – Example of an Automatically Refreshing Web Page

The following code generates the web page shown above:

```
<HEAD>
<TITLE>Reload Example</TITLE>

<SCRIPT>
//-----------------------------------------
// Returns a random number between 0 and 1
//-----------------------------------------
function getRandom()
{
   return Math.random()
}

//-----------------------------------------
// Forces a reload of the current URL
//-----------------------------------------
function reloadMe()
{
   window.location.reload()
}
</SCRIPT></HEAD>
```

```
<HTML>
<BODY>
This page will reload itself every 2 seconds.  A random number is
generated each time the page loads.<p>

<SCRIPT>
//-----------------------------------------------------
// Writes a random number to the page
//-----------------------------------------------------
var x = getRandom();
document.write(x)
</SCRIPT>

<SCRIPT>
//-----------------------------------------------------
// The setTimeout() function evaluates an expression or
// calls a function once after a specified number of
// milliseconds elapses
//
// Here it is used to call the reloadPage() function
// every 2 seconds.
//-----------------------------------------------------
timerID = window.setTimeout("reloadMe()", 2000)
</SCRIPT>

<p>
Click the button below to cancel the reload process.

<p>
<FORM>
<INPUT TYPE="button" VALUE="Stop Reloading"
   NAME="stop_reloading_button"
   onClick="clearTimeout(timerID)">
</FORM>

</BODY>
</HTML>
```

Scripting languages can be used to load multiple animated GIF files and display a particular GIF based on the value of a given network variable. This is the basis for creating fully animated web pages.

Finally, scripting languages can also be used to submit forms back to a web server. This is useful when you want to present a single button (no text boxes) to a user and send a particular network variable update depending on which button is pressed by using JavaScript to trap an image's onClick() event, and then submitting a hidden form in the onClick() event's code section.

Appendix D

i.LON 1000 Web Server Errors

This appendix describes the hypertext transfer protocol (HTTP) errors which can occur when developing a web page with the *i*.LON 1000 web server.

HTTP Errors

The following errors may occur when viewing a web site which is served by the *i*.LON 1000 web server:

Error	Cause
HTTP_BAD_REQUEST (400)	The web page contains invalid HTTP protocol. This error may occur if an HTTP request improperly "escapes" special characters.
HTTP_UNAUTHORIZED (401), HTTP_FORBIDDEN (403)	The user does not have permission to access this page.
HTTP_NOT_FOUND (404)	The requested page or file was not found.
HTTP_REQUEST_ENTITY_TOO_LARGE (413)	The requested URL is too long. This may occur when submitting a web page that has many forms or many elements within a single form. By default, the *i*.LON 1000's web server processes a maximum size query string of 1024 bytes. The maximum size of the query string may be modified by changing the value of `Maxurlsize` in the *i*.LON 1000's `params.dat` file. **Note:** The maximum size of a URL may be limited by specific browser implementations.
HTTP_INTERNAL_SERVER_ERROR (500)	Internal error.
HTTP_NOT_IMPLEMENTED (501)	The web server does not support the functionality required to fulfill the request. Using `post` instead of `get` to submit a form to the *i*.LON 1000's web server may cause this error.
HTTP_SERVICE_UNAVAILABLE (503)	The server is temporarily unable to handle the service due to temporary overloading or maintenance. This error may occur if an HTTP request is made while the server is in the process of shutting down or rebooting.
HTTP_GATEWAY_TIMEOUT (504)	This indicates an HTTP protocol error. This may indicate a socket error occurs.