ECHELON®

i.LON® 10 Ethernet Adapter User's Guide

078-0195-01D

Printed in the United States of America.

Echelon Corporation
www.echelon.com

Preface

This document describes how to connect and configure the *i*.LON 10 LONWORKS® adapter.

Welcome

The *i*.LON 10 Ethernet Adapter is a low-cost, high performance interface that connects LONWORKS based everyday devices to the Internet, a LAN, or a WAN. Through the *i*.LON 10 Ethernet Adapter, appliances, meters, load controls, lights, security systems, pumps, and valves can be connected to the Internet via a DSL or cable modem, residential gateway, settop box, switch, hub, or modem. A local or remote service center running Echelon's LNS® server can then configure, monitor and control the devices—from across the room or across the world.

Purpose

The *i*.LON *10 User's Guide* describes the hardware of the *i*.LON 10 Ethernet Adapter and also describes the configuration web pages hosted by the *i*.LON 10.

Audience

The *i*.LON *10 User's Guide* is intended for use by network installers who need to connect the *i*.LON 10 adapter to their LONWORKS network.

Related Reading

The i.LON 10 Ethernet Adapter Quick Start Guide – Describes how to connect the *i*.LON 10 hardware and configure the Setup and Security web pages to begin using the *i*.LON 10 Ethernet Adapter.

LNS Programmer's Guide – Describes how to write LNS applications that can take advantage of the communication provided by the *i*.LON 10 adapter.

LNS For Windows Programmer's Guide, xDriver Extension– Describes how the xDriver software can be used by an LNS application to manage communications with multiple LONWORKS networks that communicate over a TCP/IP network.

Requirements

In order to use the *i*.LON 10, you must have the following:

- A PC with LNS 3 (Service Pack 8, Update 1), Internet Explorer 6.0 or better, and an Ethernet card.
- A free-topology or power line LONWORKS network.

Contents

The *i*.LON 10 product comes with the following:

- *i.LON 10 Ethernet Adapter hardware.*
- *i.LON 10 CD*. This CD contains the latest LNS Updates and Adobe Acrobat versions of the documentation. For the most recent LNS updates, go to www.echelon.com/products/development/lns/.

- *Power supply*. For the free-topology model, this is an Echelon model 780x0 series power supply; for the power-line model, this is a Tamura 425x12400P power supply.
- *i.LON 10 Ethernet Adapter Quick Start Guide*.

For More Information and Technical Support

If you have technical questions that are not answered by the documentation you can get technical support from Echelon. To receive technical support from Echelon you must purchase one of Echelon's incident-based support services. Detailed information about these services may be found on the Echelon Services home page at www.echelon.com/services. You can obtain technical support via phone, fax, or email from your closest Echelon support center. The contact information is listed in the following table.

The support programs and the information in the following table are subject to change. See the Echelon Services home page at www.echelon.com/services for a description of the current offerings and support contracts. Your *i*.LON distributor may provide you with alternate contacts for support.

	London	San Jose	Tokyo
Language	English/French/ German/Italian	English	Japanese
Hours (Mon-Fri)	0900-1700 London Time	8:30am-4:30pm PDT	0900-1700 Tokyo Time
Telephone	+44 (0) 1923 430200	+1-408-938-5200 +1-800-258-4566 (US and Canada only)	+81 3 3440 7781
Fax	+44 (0) 1923 430300	+1-408-328-3832	+81 3 3440 7782
Email	lonsupport@echelon.co.uk	lonsupport@echelon.com	lonsupport@echelon.co.jp

Table of Contents

1
Introduction

This chapter provides an overview of the *i*.LON 10 Ethernet Adapter and how it fits into the *i*.LON family of products.

The *i*.LON 10 Ethernet Adapter

The *i*.LON 10 Ethernet Adapter connects LONWORKS networks to remote LNS Servers via a TCP/IP Ethernet connection. Multiple remote networks can be connected to a single LNS Server. On the PC containing the LNS Server, a piece of software called the xDriver manages communications between multiple LONWORKS networks using *i*.LON 10 Ethernet Adapters and LNS Servers, allowing for asynchronous and simultaneous updates (see the *LNS Programmer's Guide, xDriver Extension* for more information).

For example, imagine LONWORKS networks installed at 1000 separate hospital buildings in different locations. Each network contains a LONWORKS device that monitors the hospital's emergency power generator for various alarm conditions. Alarms initiate xDriver connections to an LNS service center where the alarm is processed and dispatched.

The *i*.LON 10 Ethernet Adapter is available in two models, free topology and power-line. The free topology model contains a TP/XF-FT-10 transceiver and can be connected to a TP/XF-FT-10 LONWORKS channel. The power-line model contains a PL-22 transceiver and can be connected to a PL-20 power-line LONWORKS channel.

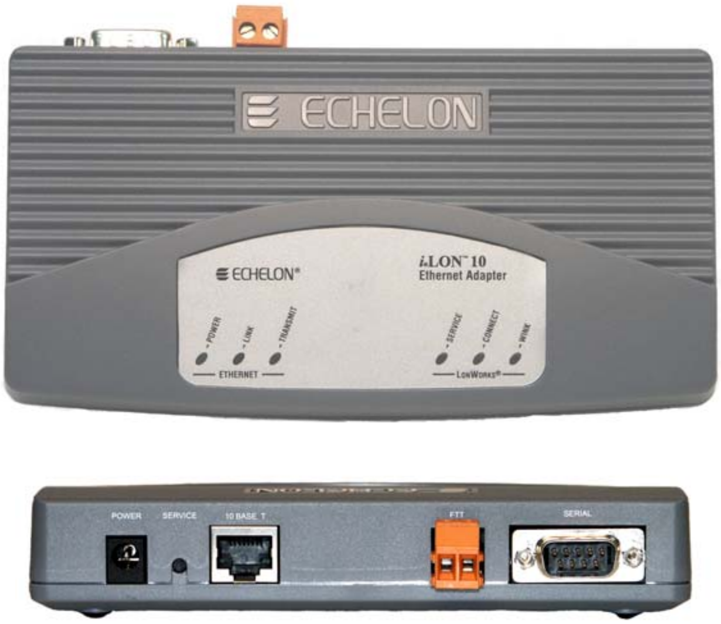
2

i.LON 10 Ethernet Adapter Hardware

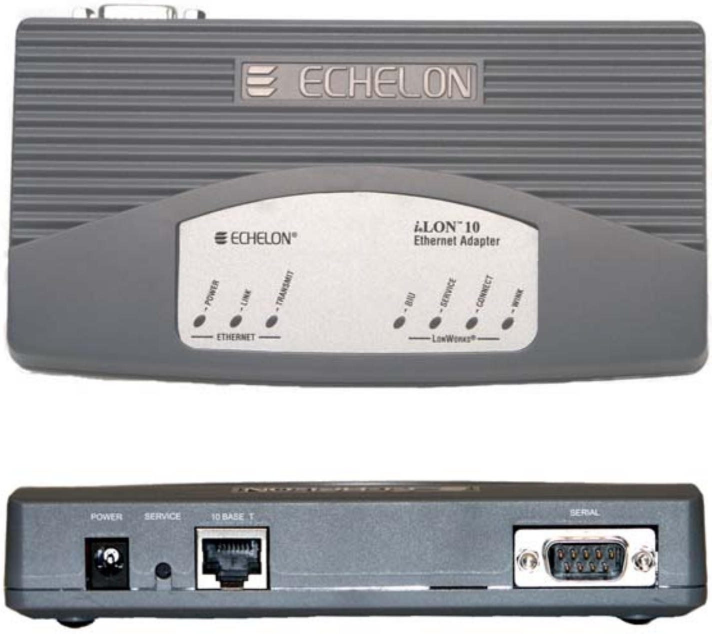
This section describes the hardware inputs and outputs for both the free-topology and power-line models of the *i*.LON 10 Ethernet Adapter. It also provides a template that can be used to mount the *i*.LON 10. See the *i*.LON 10 Ethernet Adapter Quick Start Guide for step by step instructions on how to connect the *i*.LON 10 Ethernet Adapter hardware.

i.LON 10 Ethernet Adapter I/O

The two models of the *i*.LON 10 Ethernet Adapter (power line and free-topology), have an identical form factor and have identical I/O with the exception of the differing LONWORKS network connectors and the **Band In Use LED** on the power-line model. The following diagram displays the *i*.LON 10 Ethernet Adapter (FT version) from the top and from the back, showing all hardware inputs and outputs.



***i*.LON 10 Ethernet Adapter, FT model**



***i*.LON 10 Ethernet Adapter, PL model**

These hardware inputs and outputs have the following function:

Power LED
Green LED that illuminates steadily while the *i*.LON 10 Ethernet Adapter has power.

Ethernet Link LED
Green LED that illuminates when the *i*.LON 10 Ethernet Adapter has established an Ethernet link via the 10Base-T port.

Ethernet Transmit LED
Green LED that flashes when traffic is detected on the 10Base-T network.

LONWORKS Service LED
Yellow LED that implements the Standard Neuron® Service LED behavior (see the *Neuron Chip Databook* for more information).

LONWORKS Connect LED
Yellow LED that illuminates steadily if the *i*.LON 10 Ethernet Adapter is connected with an LNS server. It is dark when no LNS server connection exists.

LONWORKS Wink LED
Yellow LED that flashes 5 times when the *i*.LON 10 Ethernet Adapter receives a LONWORKS wink command from the LONWORKS channel.

BIU LED
Yellow LED that illuminates when a carrier frequency is detected at 131.5 kHz to 133.5 kHz. This LED is only on the power-line version.

Power Input
Barrel connector power supply input for use with the included power supply (Echelon model 780x0 series for the free-topology model). The included Tamura 425x12400P

supply should be used with the power-line model.

10Base-T Ethernet Port Standard 10BaseT connection, type RJ-45.

LONWORKS TP/FT-10 Port For the free-topology model, an orange Weidmuller connector (Weidmuller model #134686) connected to an Echelon TP/FT-10 transceiver. This port exists only on the free-topology model.

Serial Port A DB-9 serial port. Can be used to connect the *i*.LON 10 Ethernet adapter to a modem. See *i.LON 10 Serial Port Pinout*, below, for more information about this port.

Service Pin Service pin is a recessed pushbutton used to send a LONWORKS service pin message on the LONWORKS channel. This button is also used to perform a security access reset as described in *Security Access Reset*.

i.LON 10 Serial Port Pinout

When connecting a DCE modem with a DB-9 serial port to the *i*.LON 10, the signals are communicated as shown in Table 2-1.

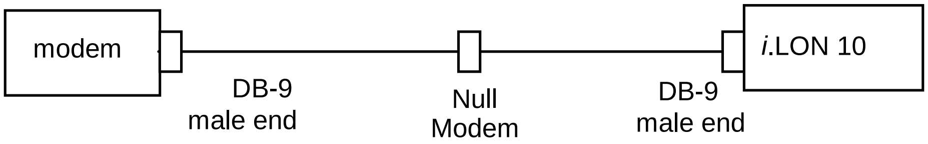
Table 2-1
DCE Modem to DTE i.LON 10 Adapter Connection (DB-9 to DB-9)

Modem Signal Name	*Cable DB-9 Male*	*Cable DB9 Female*	*i.LON 10 (DTE) DB-9 Male*
DCD	Pin 1	Pin 1	DCD—Pin 1
RxD	Pin 3	Pin 3	RxD—Pin 2
TxD	Pin 2	Pin 2	TxD—Pin 3
DTR	Pin 4	Pin 4	DTR—Pin4
GND	Pin 5	Pin 5	GND—Pin 5
DSR	Pin 6	Pin 6	DSR—Pin 6
RTS	Pin 7	Pin 7	RTS—Pin 7
CTS	Pin 8	Pin 8	CTS—Pin 8

When connecting a DTE modem with requiring a null modem cable with a DB-9 serial port to an *i*.LON 10, the signals are communicated as shown in Table 2-2.

Table 2-2
DTE Modem requiring a null modem cable to DTE i.LON 10 Adapter Connection (DB-9 to DB-9)

Modem Signal Name	***Cable DB-9 Male***	***Null Modem***	***Cable DB9 Femal e***	***i.LON 10 (DTE) DB-9 Male***
DCD	Pin 1	Pin 1-1	Pin 1	DCD—Pin 1
RxD	Pin 3	Pin 2-3	Pin 2	RxD—Pin 2
TxD	Pin 2	Pin 3-2	Pin 3	TxD—Pin 3
DTR	Pin 4	Pin 4-6	Pin 4	DTR—Pin4
GND	Pin 5	Pin 5-5	Pin 5	GND—Pin 5
DSR	Pin 6	Pin 6-4	Pin 6	DSR—Pin 6
RTS	Pin 7	Pin 7-8	Pin 7	RTS—Pin 7
CTS	Pin 8	Pin 8-7	Pin 8	CTS—Pin 8



When connecting a DCE modem with a DB-25 serial port to the *i*.LON 10, the signals are communicated as shown in Table 2-3.

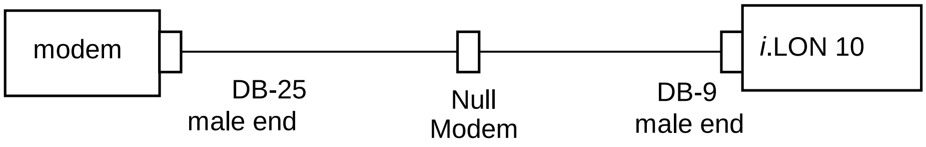
Table 2-3
DCE Modem to DTE i.LON 10 Adapter Connection (DB-25 to DB-9)

Modem Signal Name	***Cable DB-25 Male***	***Cable DB9 Female***	***i.LON 10 (DTE) DB-9 Male***
DCD	Pin 8	Pin 1	DCD—Pin 1
TxD	Pin 3	Pin 3	RxD—Pin 2
RxD	Pin 2	Pin 2	TxD—Pin 3
DTR	Pin 20	Pin 4	DTR—Pin4
GND	Pin 5	Pin 5	GND—Pin 5
DSR	Pin 6	Pin 6	DSR—Pin 6
RTS	Pin 7	Pin 7	RTS—Pin 7
CTS	Pin 8	Pin 8	CTS—Pin 8

When connecting a DTE modem with requiring a null modem cable with a DB-25 serial port to an *i*.LON 10, the signals are communicated as shown in Table 2-4.

Table 2-4
DTE Modem requiring a null modem cable to i.LON 10 Adapter Connection (DB-25 to DB-9)

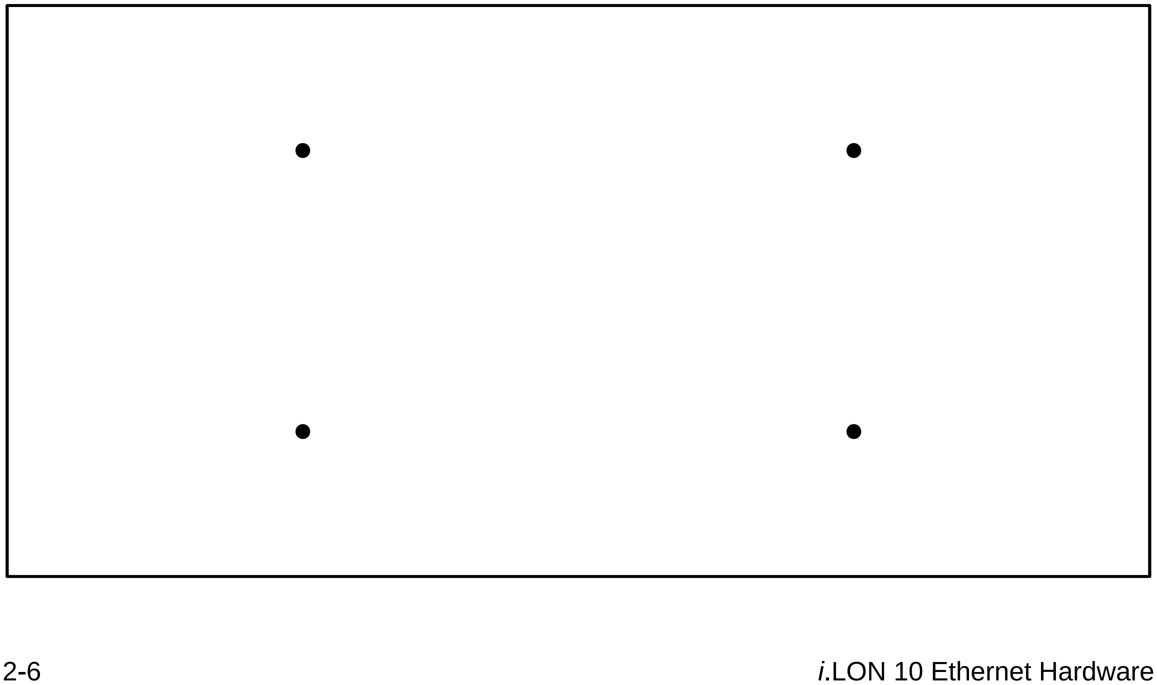
Modem Signal Name	***Cable DB-25 Male***	***Cable DB9 Female***	***i.LON 10 (DTE) DB-9 Male***
DCD	Pin 8	Pin 1	DCD—Pin 1
TxD	Pin 3	Pin 2	RxD—Pin 2
RxD	Pin 2	Pin 3	TxD—Pin 3
DTR	Pin 20	Pin 4	DTR—Pin4
GND	Pin 7	Pin 5	GND—Pin 5
DSR	Pin 6	Pin 6	DSR—Pin 6
RTS	Pin 4	Pin 7	RTS—Pin 7
CTS	Pin 5	Pin 8	CTS—Pin 8



Mounting the *i*.LON 10 Ethernet Adapter Hardware

To mount the *i*.LON 10 Ethernet Adapter, follow these steps:

1. Determine if you want to mount the *i*.LON 10 Ethernet Adapter horizontally or vertically.
2. Insert two #6 flat-head screws into the surface upon which the *i*.LON 10 is to be mounted. For horizontal mounting, these screws should be placed 73.5 mm apart. For vertical mounting, these screws should be placed 37.5 mm apart. The following template can be printed out and used to set screw locations:



Be sure the heads of screws are protruding slightly from the mounting surface.

3. Slide the *i*.LON 10 Ethernet adapter onto the screws. You may need to adjust the screws into or out of the wall slightly to assure a secure mounting.

i.LON 10 Hardware Specifications

Operating Input Voltage	**Power line**: 12.5 VDC provided by LONWORKS enabled power supply such as Tamura model #425x12400P **Free topology**: 9VDC
Operating Input Current	270 mA Model 72010 400 mA Model 72011
Operating Temperature Range	0° C to +50° C
Operating Humidity Range	25 to 90% RH @ 50° C
Non-operating Humidity Range	95% RH max @ 50° C
EMC	FCC Part 15 Class B, ICES-003 Class B, EN55024, EN 55022 Class B, VCCI Class B, C-Tick
Agency Listings	UL 60950, CSA C22.2 No. 60950, EN60950, CE

FCC Compliance Statement – Class B

This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if no installed and used in accordance with the manufacturer’s instruction manual, may cause interference with radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, you are encouraged to try to correct the interference by one or more of the following measures:

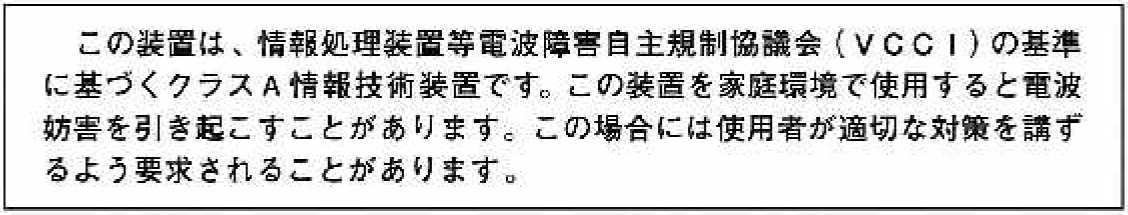
- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that which the receiver is connected.
- Consult the dealer or an experienced radio/television technician for help.

Changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

IC Compliance Statement – Class B

This Class B digital apparatus meets the requirements of the Canadian Interference-Causing Equipment Regulations of ICES-003.

VCCI Compliance Statement – Class B ITE



この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

This is a Class B product based on the standard of the Voluntary Control Council for Interference (VCCI) for information technology equipment. If this equipment is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

3

Using the *i*.LON 10 Ethernet Adapter with a 10BaseT Connection

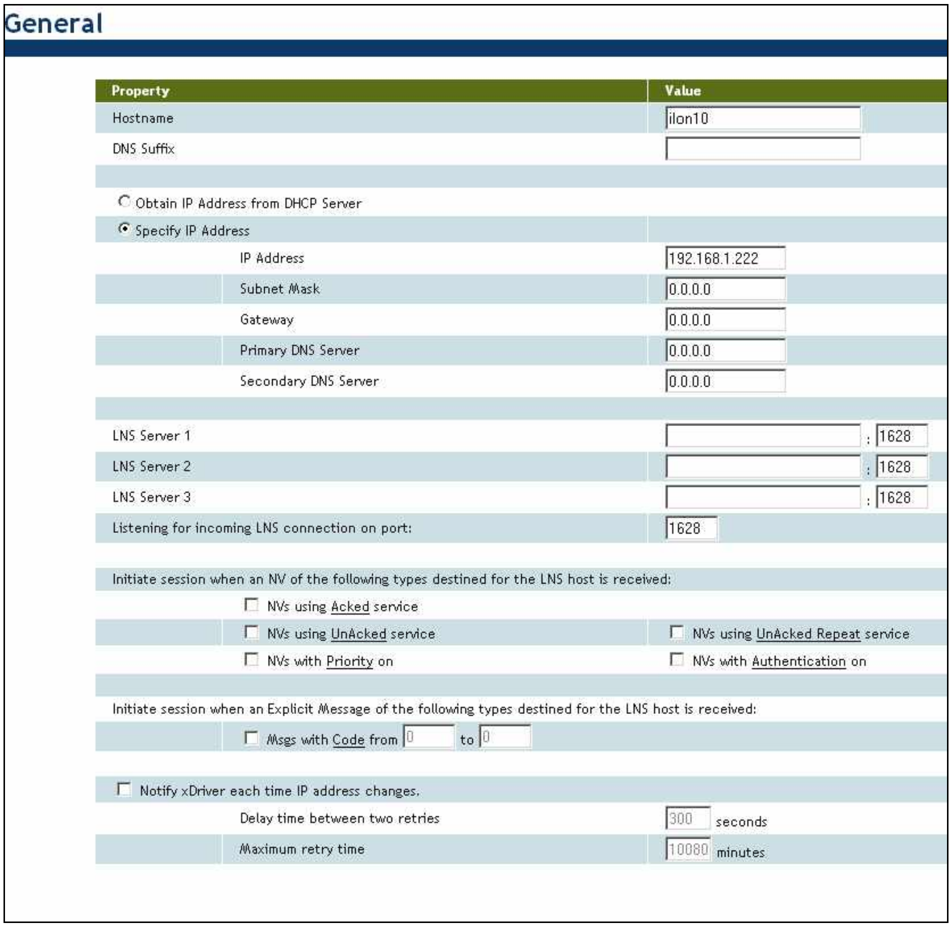
This chapter discusses how to configure the *i*.LON 10 Ethernet Adapter's General Setup web page to facilitate communications between the LONWORKS network and the LNS Server using TCP/IP.

The *i*.LON 10 Ethernet Adapter General Configuration Page

You can access the *i*.LON 10 Ethernet Adapter's General setup page by pointing your browser to 192.168.1.222 and clicking the Setup link. If you are unable to access the i.LON 10 Ethernet Adapter's web pages, ensure that:

- The PC is on the same subnet as the *i*.LON 10 Ethernet Adapter. By default, the IP address of the *i*.LON 10 Ethernet Adapter is 192.168.1.222. The IP address is reset to this value whenever a security access reset (see *Performing a Security Access Reset* in Chapter 5) is performed. See the *i.LON 10 Ethernet Adapter Quick Start Guide* for a step-by step description of how to configure the *i*.LON 10.
- If Internet Explorer is configured to use a proxy server, set the **Bypass Proxy Server for Local Addresses** option. You can access proxy server options in Internet Explorer 6.0 by opening the **Tools** menu, then clicking **Options**, then selecting the **Connections** tab of the **Options** dialog, and then clicking **LAN Settings** on the **Connections** tab.

This General setup page appears as shown in the following figure:



General

Property	Value
Hostname	ilon10
DNS Suffix	
○ Obtain IP Address from DHCP Server	
● Specify IP Address	
IP Address	192.168.1.222
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
LNS Server 1	: 1628
LNS Server 2	: 1628
LNS Server 3	: 1628
Listening for incoming LNS connection on port:	1628
Initiate session when an NV of the following types destined for the LNS host is received:	
☐ NVs using Acked service	
☐ NVs using UnAcked service	☐ NVs using UnAcked Repeat service
☐ NVs with Priority on	☐ NVs with Authentication on
Initiate session when an Explicit Message of the following types destined for the LNS host is received:	
☐ Msgs with Code from 0 to 0	
☐ Notify xDriver each time IP address changes.	
Delay time between two retries	300 seconds
Maximum retry time	10080 minutes

If you are unable to access this page, verify that if your PC is on the same subnet as the *i*.LON 10. To access this page in non-secure mode, the **HTTP Access** option on the security page must be selected. See *i*.LON 10 Ethernet Adapter Security Web Page in Chapter 5 for more information).

The setup page has the following fields:

Hostname

The TCP/IP host name of the *i*.LON 10 Ethernet Adapter. This name will be converted to all lower case by the firmware. When the *i*.LON 10 Ethernet Adapter establishes a connection with an LNS server it provides its fully qualified host/domain name so the LNS server knows which LONWORKS database to open. By default, the *i*.LON 10 Ethernet Adapter's host name is `ilon10`. The *i*.LON 10 Ethernet Adapter must be reset for change in this value to take effect. The URL of the i.LON 10 is `Hostname.DNS Suffix` (i.e. if **Hostname** is set to `ilon10` and **DNS Suffix** is set to `echelon.com`, the URL will be `ilon10.echelon.com`. Valid characters are numbers, letters, and the hyphen (‘-‘) character. This field has a maximum of 63 characters. By default the **Hostname** is iLON10.

DNS Suffix

The IP domain name in which the *i*.LON 10 Ethernet Adapter is installed. This value is optional. This field has a maximum of 63 characters.

Obtain IP Address from DHCP Server

Set this option to have the *i*.LON 10 Ethernet Adapter obtain its IP address, subnet mask, default gateway, and DNS servers from the local network's DHCP server. If this option is set, you must set the **Hostname** and **DNS Suffix** and register these values with your DNS administrator. This option is enabled by default.

To see the IP address that has been assigned to the *i*.LON 10, open the System Log web page in secure mode (see *Viewing the i.LON 10 System Log Web Page* in Chapter 6).

Specify IP Address

Set this option when specifying a static IP address for the *i*.LON 10 Ethernet Adapter in **IP Address**.

IP Address

Static IP address used by the *i*.LON 10 Ethernet Adapter if **Obtain IP address from DHCP Server** is not set. By default, this value is set to `192.168.1.222`.

Subnet Mask

Subnet mask used by the *i*.LON 10 Ethernet Adapter if **Obtain IP address from DHCP Server** is not set. By default, this value is `0.0.0.0`.

Gateway

Gateway used by the *i*.LON 10 Ethernet Adapter if **Obtain IP address from DHCP**

Server is not set. By default, this value is `0.0.0.0`.

Primary/Secondary DNS Server

The primary and secondary DNS Servers used to resolve LNS Server names if **Obtain IP address from DHCP Server** is not set. If DNS servers are specified both here and by the DHCP server, the DNS server specified by DHCP will be used.

LNS Server 1/2/3

Up to three LNS Server names or IP addresses in the form `<LNS Server IP Address>:<port>` or `<LNS Server Name>:<port>` (for example, you can specify `123.2.34.1:1628` or `mylns.echelon.com:1628`). The *i*.LON 10 Ethernet Adapter will attempt to send packets to the first server on the list. If that server does not respond, it will try the second server, then the third. LNS Servers can be specified by DNS name. If DNS names are used, a DNS server must be listed in **Primary/Secondary DNS Server** or be available through the local network's DHCP server. Each Server name can be up to 63 characters long.

Listen for Incoming LNS Server Connection on Port

The TCP port on which the *i*.LON 10 Ethernet Adapter receives packets (LONWORKS messages). Defaults to 1628. It is not recommended that the port number be set below 1025, as ports 0 through 1024 are normally reserved.

Note that to receive incoming LNS connections, the **Listen for Incoming LNS Connections** option on the Security Web page must be checked (this option is cleared by default).

Initiate Session when an NV/Explicit Message of the Following Types Destined for the LNS Host is Received

Specify under what conditions the i.LON 10 Ethernet Adapter will initiate an uplink connection to the LNS host. By default, all of these checkboxes are cleared (i.e. an update will never initiate a connection to the host). Use these options to limit the sorts of network variable updates or explicit messages that will initiate a session.

Notify xDriver Each Time IP Address Changes

This option is not supported for LNS 3, Service Pack 8, Update 1, and earlier.

Set this option to notify the xDriver when the IP address of the i.LON 10 Ethernet Adapter changes. This may resolve connectivity problems if a non-static IP address is used.

Delay Time Between Two Retries

This option is not supported for LNS 3, Service Pack 8, Update 1, and earlier.

This option is only available if **Notify xDriver Each Time IP Address Changes** is checked. If the *i*.LON 10 attempts to inform the xDriver of an IP address change and is not successful, this is the amount of time before another attempt is made.

Maximum Retry Time

This option is not supported for LNS 3, Service Pack 8, Update 1, and earlier.

This option is only available if **Notify xDriver Each Time IP Address Changes** is checked. The amount of time, in minutes, for which the *i*.LON 10 Ethernet Adapter will attempt to inform the server of an IP address change.

Submit

Click to close this page, write the configuration changes to FLASH memory, and reset the *i*.LON 10 Ethernet Adapter. Configuration changes will take effect upon reboot.

4

Using the *i*.LON 10 Ethernet Adapter With a Modem

This chapter describes how to connect a modem to the *i*.LON 10 Ethernet adapter and how to configure the PPP web page to allow the *i*.LON 10 to dial-out, accept incoming calls, and respond to shoulder-tap.

Connecting The *i*.LON 10 Ethernet Adapter to a Modem

You can connect the *i*.LON 10 Ethernet Adapter to an analog, GSM, or ISDN modem using a standard DB-9 – DB-25 straight though modem cable.

You must use a straight through modem cable to connect the *i*.LON 10 to the Modem. A crossover cable will not work.

In order to for a modem to communicate with the i.LON 10, it must support all of the following signals: Tx, Rx, GND, RTS, CTS, DSR, DTR and CD. Check with the modem manufacturer to confirm that the modem you want to use supports these signals.

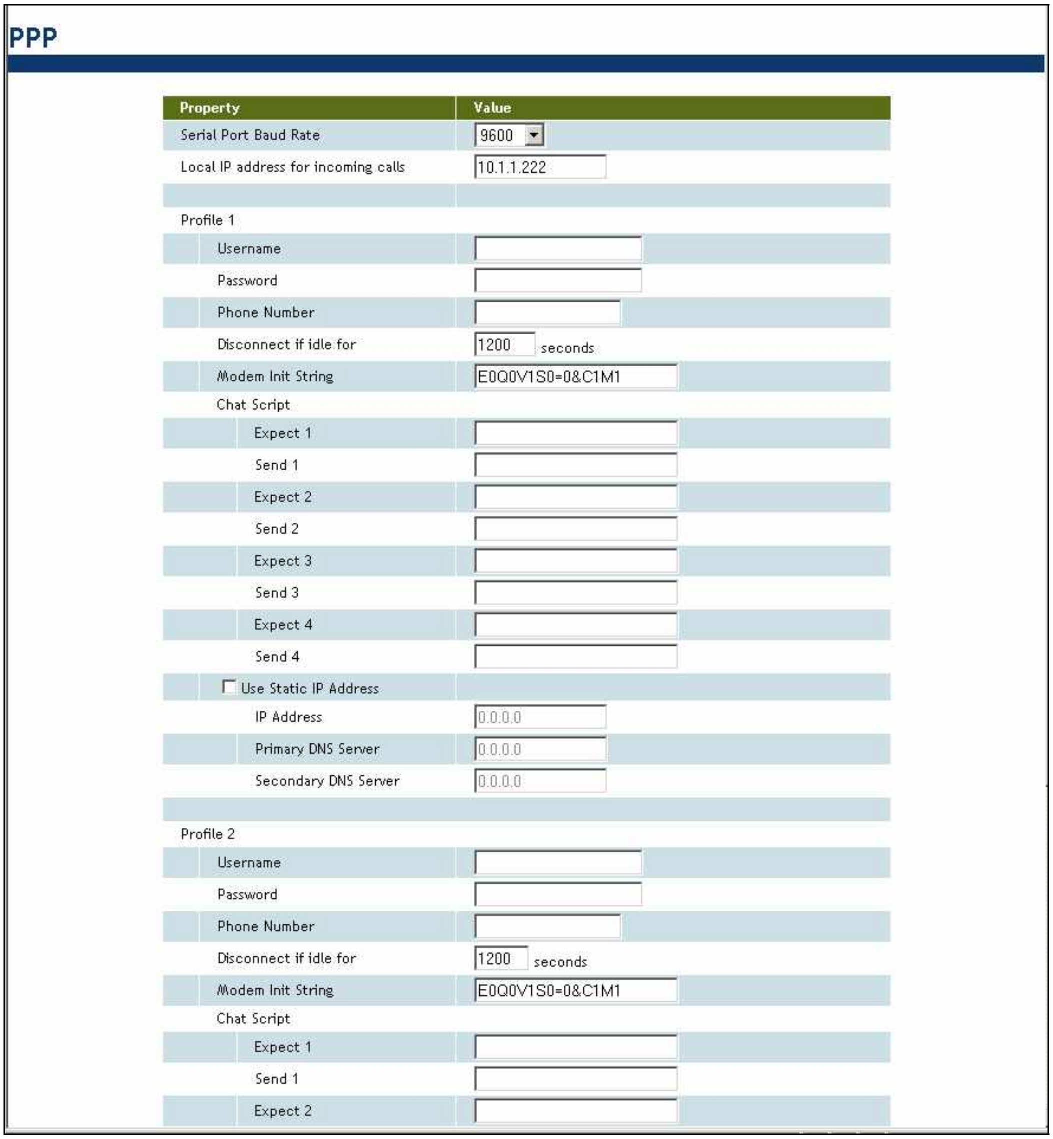
Configuring the *i*.LON 10 Ethernet Adapter for PPP

The *i*.LON 10 Ethernet Adapter supports three methods of establishing communication using a modem attached to its serial port:

- *Dial-out* – The *i*.LON 10 Ethernet Adapter can be configured to use an attached modem to dial-out to an ISP. Once connected to an ISP, a connection to an LNS Server on an attached TCP/IP network can be established.
- *Dial-in* – The *i*.LON 10 Ethernet Adapter can be configured to use an attached modem to accept incoming calls.
- *Shoulder tap* – The *i*.LON 10 Ethernet Adapter can be configured to listen for an incoming call, then dial-back in response. This allows you to call the *i*.LON 10 from a remote location and have the *i*.LON 10 respond by calling an ISP that is local to it, thus avoiding toll charges and providing security. The *i*.LON 10 Ethernet Adapter cannot simultaneously support the dial-in and shoulder-tap methods.

The i.*LON 10 Ethernet Adapter PPP Configuration Page*

The *i*.LON 10 Ethernet Adapter PPP Configuration Web page appears as shown in the following figure:



PPP

Property	Value
Serial Port Baud Rate	9600 ▾
Local IP address for incoming calls	10.1.1.222
Profile 1	
Username	
Password	
Phone Number	
Disconnect if idle for	1200 seconds
Modem Init String	E0Q0V1S0=0&C1M1
Chat Script	
Expect 1	
Send 1	
Expect 2	
Send 2	
Expect 3	
Send 3	
Expect 4	
Send 4	
□ Use Static IP Address	
IP Address	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Profile 2	
Username	
Password	
Phone Number	
Disconnect if idle for	1200 seconds
Modem Init String	E0Q0V1S0=0&C1M1
Chat Script	
Expect 1	
Send 1	
Expect 2	

This Web page contains the following options:

Serial Port Baud Rate

The speed of communications on the DB-9 serial port. The *i*.LON 10 Ethernet Adapter supports rates of 9600 bps, 19200 bps, 38400 bps, and 56700 bps. The serial bit rate should equal the bit rate of the attached modem.

Local IP Address for Incoming Calls

Set the IP address that will be assigned to incoming calls by the *i*.LON 100 server. By default, this is the IP address of the *i*.LON 10 incremented by one (e.g. if the IP address of the *i*.LON 10 is 10.1.4.14, the address assigned to an incoming call will be 10.1.4.15).

Profile 1/Profile 2

The *i*.LON 10 Ethernet adapter supports two dial-out profile. If a connection cannot be made to the first profile, the second will be tried. The *i*.LON 10 will alternate between profiles until a connection is established or until the number of retries specified by **Number of Retries to Use when Attempting Outbound PPP Connection Attempts** on the *Security* Configuration Web page has been reached. Each profile contains the following options:

Username

The username to be used by the *i*.LON 10 Ethernet Adapter when connecting to an ISP. This name can be up to 63 characters.

If you are using a GSM/GPRS modem, you should leave this field blank.

Password

The password to be used by the *i*.LON 10 Ethernet Adapter when connecting to an ISP. This password can be up to 63 characters.

If you are using a GSM/GPRS modem, you should leave this field blank.

Phone Number

The phone number to be dialed by the *i*.LON 10 Ethernet Adapter for this profile. This field accepts all alphanumeric characters and the following additional characters:

`- , ; ! @ * # =`

This field may contain up to 63 characters (no spaces).

If you are dialing a regular phone number (i.e. not a packet switching connection like a cell phone), it is recommended that you append a '@' to the end of your phone number (e.g. 1-800-555-1212@). This will cause the *i*.LON 10 to log "NO ANSWER" rather than "NO CARRIER" if the phone is not answered. This is important because the *i*.LON 10 will stop dialing a number if it gets two "NO CARRIER" responses, since it is assumed to be a voice pickup and FCC regulations prohibit more than two calls from a modem to a voice-answered phone number.

If you are using a GSM/GPRS modem, you should set this field to **99***1#**.

Disconnect if Idle For

The idle timeout in seconds. If the connection is idle for this length of time, the call will be ended. By default, this value is set to 1200 seconds. This value must be an integer 0 or greater.

Setting this value to 0 disables the idle timeout (i.e. the connection will stay open indefinitely).

Modem Init String

The initialization string sent to the modem before each connection attempt. Use this field to insure that the modem’s baud rate matches the value set in **Serial Port Baud** Rate. The **Modem Init String** for **Profile 1** is sent on the serial port each time the i.LON 10 is reset.

You do not need to enter “AT” before each member of the init string (i.e. rather than “AT&C1;AT&F” you should enter “&C1&F”.

The default Modem Init String is “ATE0Q0V1S0=0&C1&M1. If you are using a US Robotics modem, it is advised that you change this to “ATE0Q0V1S0=0&C1&B1M1.” The B1 command causes the modem to automatically use the bit rate used by the i.LON 10 (this commend is not available in non-US Robotics modems). See *GSM/GPRS Service Providers Tested with the i.LON 10 Ethernet Adapter*, later in this chapter for more information about Modem Init Strings to use with GSM/GPRS modems.

You can use the modem initialization string to implement flow control (i.e. to limit the speed of the connection). For most modems, &U<n> sets the lowest acceptable connection speed and &N<n> sets the highest acceptable connection speed, where <n> can be set to:

6	9600 bps
10	19200 bps
16	33600 bps

Do not use the &C0 command in either of the Profile initialization strings. Using this command will prevent the i.LON 10 from initiating a dial out session.

See your modem documentation for more information on supported init strings.

Chat Script

Only used if the ISP requires more handshaking than a user name and password. Each field can accept up to 63 characters.

Use Static IP Address

Set this checkbox to manually set the **IP Address**, **Primary DNS Server**, and **Secondary DNS Server** of the *i*.LON 10 Ethernet Adapter when connected to an ISP.

	If this checkbox is cleared, this information will be set by the ISP.
Submit	Click to close this page, write the configuration changes to FLASH memory, and reset the *i*.LON 10 Ethernet Adapter. Configuration changes will take effect upon reboot.

Configuring the i.LON 10 Ethernet Adapter for Dial-out

The *i*.LON 10 Ethernet Adapter can be configured to dial-out when it needs to form an uplink communication with the LNS Server. To configure the *i*.LON 10 Ethernet adapter to dial-out to an ISP, follow these steps:

1. If **Allow Access to Secure Pages Without a Security Access Reset** is not enabled on the Security Web page, perform a security access reset as described in *Performing a Security Access Reset* in Chapter 5.
2. Click **Security** to open the *i*.LON 10 *Security* Configuration Web page.
3. If it is not already checked, check the **Allow Access to Secure Pages Without a Security Access Reset** option, click **Submit**, and then wait for the *i*.LON 10 to reboot.
4. Ensure that the **Enable Outbound PPP Calls** checkbox is set.
5. Set **Number of Retries to Use When Attempting Outbound PPP Connection Attempts**.
6. If **Enable Ethernet** is checked, check **Use PPP as Dial Backup when Ethernet Link Fails**. If this is not set, the *i*.LON 10 will never attempt to dial out.
7. Click **Submit**.
8. Click **General** to open the General Setup Web page.
9. Enter the IP address or hostname (if DNS is enabled) for an LNS Server in **LNS Server 1**. Optionally set **LNS Server 2** and **LNS Server 3** to configure backup LNS Servers.
10. Set at least one of the **Initiate Session when an NV/Explicit Message of the Following Types Destined for the LNS Host is Received** options so a uplink connection will be attempted when the specified type of network variable or explicit message is sent to the host.
11. Click **Submit**.
12. Click **PPP** to open the *i*.LON 10 PPP Configuration Web page.
13. Set the ISP phone number, user name, password, and initialization string under **Profile 1** and **Profile 2** as described under *The i.LON 10 Ethernet Adapter PPP Configuration Page,* earlier in this chapter.
14. Click **Submit**.

When the *i*.LON 10 needs to communicate with the LNS Server (as determined by the **Initiate Session** options on the *General* Configuration Web page) it will attempt to dial the number configured in **Profile 1**; if no connection is established, it will attempt the number configured in **Profile 2**; both numbers will be retried up to the number of times specified by the **Number of Retries** option set in step 3.

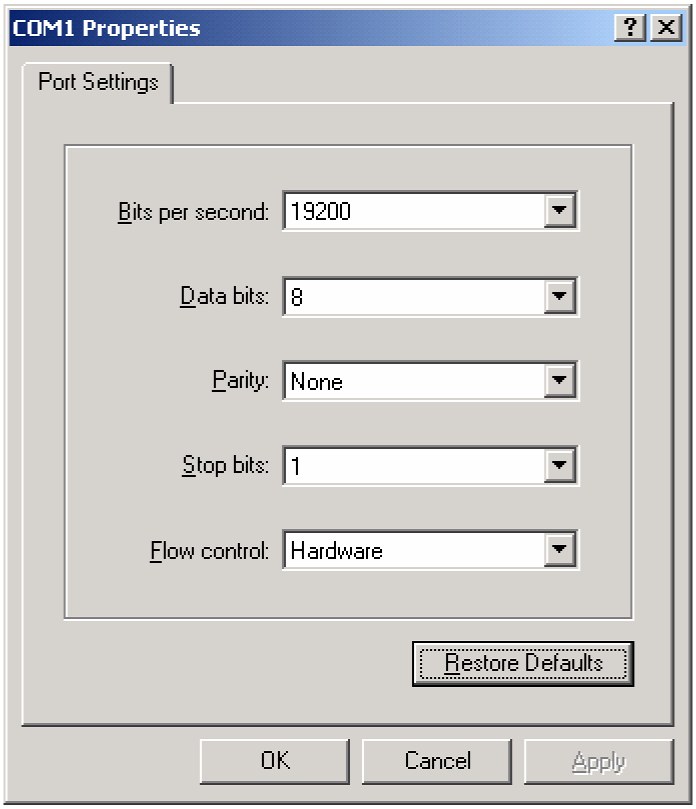
Troubleshooting Dial-out Problems

If you are having trouble getting the *i*.LON 10 Ethernet Adapter to connect to an ISP, perform the following tests:

Test the Modem

To test the modem, follow these steps:

1. Connect the modem to your computer's serial port using the straight-through modem cable used to connect the *i*.LON 10 to the modem.
2. Open HyperTerminal. Assure that the scroll lock is turned off on your computer (if it is on, press the <Scroll Lock> button to turn it off). In HyperTerminal, set the **Bits Per Second** to the same rate as used to communicate with the *i*.LON 10. Set **Data Bits** to 8, **Parity** to None, **Stop Bits** to 1, and **Flow Control** to Hardware, as shown in the following figure:



Bits per second: 19200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: Hardware

3. In HyperTerminal, turn on Echo. To do this, follow these steps:
   i. Click the **File** menu and select **Properties**. The HyperTerminal **Properties** dialog opens.
   ii. In the **Properties** dialog, select the **Settings** tab.
   iii. Click **ASCII Setup**. The **ASCII Setup** dialog opens.
   iv. In the **ASCII Setup** dialog, set the **Echo Typed Characters Locally** checkbox.
   v. Click **OK** in the **ASCII Setup** and **Properties** dialogs.
4. Request a response from the modem by performing the following steps:
   i. In HyperTerminal, press <Enter> several times. This should allow the modem to automatically detect the baud rate setting of HyperTerminal.

ii. Type “AT” in capital letters and press <Enter>. The modem should respond with “OK”. If the modem does not respond, repeat this step several times. If you cannot get a response, verify that the modem is turned on.

iii. If you still get no response, watch the LEDs on the modem when you enter ‘AT”. If they do not flicker, the modem is not responding the command. This could be due to any of the following:

- Wrong type of modem cable being used. Confirm that you are using a straight through cable.
- Faulty modem cable being used. Try a different straight through cable.
- You are connected to a different serial port than the one provided to HyperTerminal. Many computers have multiple serial ports (COM1, COM2, etc.), and often COM1 is used for the internal modem. Try switching HyperTerminal to COM2, COM3, etc.
- Serial port is malfunctioning. Try connecting to a different serial port. Be sure to change the HyperTerminal port settings to the new serial port.

5. If the previous steps have not diagnosed the problem (i.e. you are connected to the correct port, you have the right cable, etc), reset the modem to its factory defaults. In HyperTerminal, type “AT&F” and hit enter a few times. Even if you see no response, this command resets almost all modems to their factory default settings.

Test for a Dial Tone

This section assumes you have confirmed communication with the modem as described in the previous section and that your modem is still connected to your computer. To test for a dial tone, follow these steps:

1. In HyperTerminal, type “ATDT” and press <Enter>. You should hear a dial tone through the modem’s speaker.
2. If you do not hear a dial tone, assure that the modem’s speaker is enabled and that the volume is set correctly. To do this, follow these steps:

   i. In HyperTerminal, type “ATM1” and press <Enter>. This will enable the modem’s speaker.

   ii. In HyperTerminal, type “ATL2” and press <Enter>. This will set the modem’s speaker volume to medium.

   Once you have enabled the speaker and set the volume, repeat step 1.
3. Assure that your modem type (digital or analog) matches the phone line type.
4. If there is still no dial tone, assure that the phone line attached to the modem is functional. Attach a telephone to the phone line to verify that there is a dial tone.

Test the ISP Phone Number and Account

This section assumes you have confirmed communication with the modem and confirmed that there is a dial tone, as described in the previous sections. This section further assumes that you have a computer attached the modem and a separate computer running the LNS server attached to the Internet. To test the ISP phone number and account, follow these steps:

1. On the computer attached to the modem, dial the ISP. In HyperTerminal, type "ATDT 555-1234" (replace 555-1234 with the phone number supplied by your ISP for POP connections. Be sure to include an prefixes needed to get an outside line. A comma may be used to force a short pause (e.g. "ATDT 9,555-1234").

   You should hear a dial tone, then dialing, and a high-pitched whistling when the ISP's modem picks up. You may or may not see anything on your HyperTerminal display (this varies by ISP). If you do not hear the ISP's modem pick up, contact your ISP's customer support.

2. If step 1 is successful, connect to your ISP using Windows dial-up networking. Be sure to include your account ID and password in the Windows Dial-up Networking Dialer.

   Once a connection is established, you should be able to browse web pages using Internet Explorer. If you are unable to establish a connection, verify that you correctly entered your account ID and password. If these are correct, contact your ISP's customer support.

3. On the computer attached to the modem, open a command prompt, type "ping <LNS Server IP address>", and press <Enter>. If your computer is in communication with the LNS Server computer, you will see responses from the *i*.LON 10.

   If the ping fails the IP Address provided by the ISP may not be routable or the ISP may have disabled your ability to ping IP address on the Internet. Contact your ISP for more information.

4. If the ping is successful, start an LNS client and attempt to connect to the LNS Server as a Remote Lightweight client (see the *LonMaker® User's Guide* and the *LNS for Windows Programmer's Guide* for more information). If you cannot connect, your ISP may be blocking on ports used by the LNS Server. Contact your ISP to resolve this problem before using the i.LON 10 for dial-up.

Test the i.LON 10 with the Modem

This section assumes you have confirmed communication with the modem, confirmed there is a dial tone, and confirmed that you can log into your ISP account. To test the *i*.LON 10 with the modem, follow these steps:

1. Attach the modem to the *i*.LON 10 using the same straight-through cable that you used to connect the modem to the PC in the previous sections.

2. Access the *i*.LON 10 via HTTP and configure it for dial-out, as described in *Configuring the i.LON 10 Ethernet Adapter for Dial-out*, earlier in this chapter. Use the same serial port baud rate specified in *Test the Modem*, earlier in this chapter. Use the same username and password specified in *Test the ISP Phone Number and Account*, earlier in this chapter.

3. Attach the *i*.LON 10 to a LONWORKS network. The LONWORKS network must have a network variable that is bound to the host. See *Binding Network Variables to the Host* in the *LonMaker User's Guide* for more information.

4. On the General Setup web page, set the appropriate checkbox under **Initiate Session when an NV of the Following Types Destined for the LNS Host is Received** to cause a session to be started when the network variable that is bound to the host is updated.

5. Generate a network variable event on the network variable that is bound to

the host. This should force the *i*.LON 10 to dial-out. Watch the modem LEDs for activity and listen for dial tone, ringing, and connection:

- If the modem LEDs do not flash, the *i*.LON 10 is probably not communicating with the modem.
- If the LEDs flash, but the modem doesn't dial:
  - i. Set **Modem Init String** on the PPP Configuration Web page to "&F". This will reset the modem to its factory defaults.
  - ii. Check that the RS-232 line speed is the same as you used when testing the modem with the computer.
  - iii. If you have the LonTalk® Protocol Analyzer available, confirm that an attempt was made to send a packet from the LONWORKS network to the host. If no attempt was made, assure that the **Initiate Session when…** option set in step 4 is set appropriately for the network variable being updated.
- If the modem dials, but no connection takes place, confirm that the port numbers specified on the General Setup Web page are open on the ISP and the computer with the LNS Server.
- If everything appears to be configured correctly, check the Event Log page for errors.

Configuring the i.LON 10 Ethernet Adapter for Dial-in

To configure the *i*.LON 10 Ethernet Adapter to accept incoming calls, follow these steps:

1. Click **Security** to open the *i*.LON 10 *Security* Configuration Web page.
2. Ensure that the **Allow and Authenticate Incoming PPP Connections** checkbox is set. You must clear the **Allow PPP Dial-back (Shoulder Tap)** checkbox to do this.
3. Set the **Username** and **Password** options under **Allow and Authenticate Incoming PPP Connections**. This username and password must be provided by the caller in order to establish communications with the *i*.LON 10 Ethernet Adapter.
4. Set **Answer Phone After <x> Rings**. This is the number of rings after which the *i*.LON 10 will pick up he phone.
5. Click **Submit**.
6. Click **PPP** to open the *i*.LON 10 PPP Configuration Web Page.
7. Set **Local IP Address for Incoming Calls**. This is the IP address that will be assigned to incoming calls by the *i*.LON 10. The caller (typically a PC using Windows dial-up networking) will be assigned this address plus one (i.e. if this field is set to 10.6.8.100, the PC will be assigned 10.6.8.101.
8. Click **Submit**.

Troubleshooting Dial-in Problems

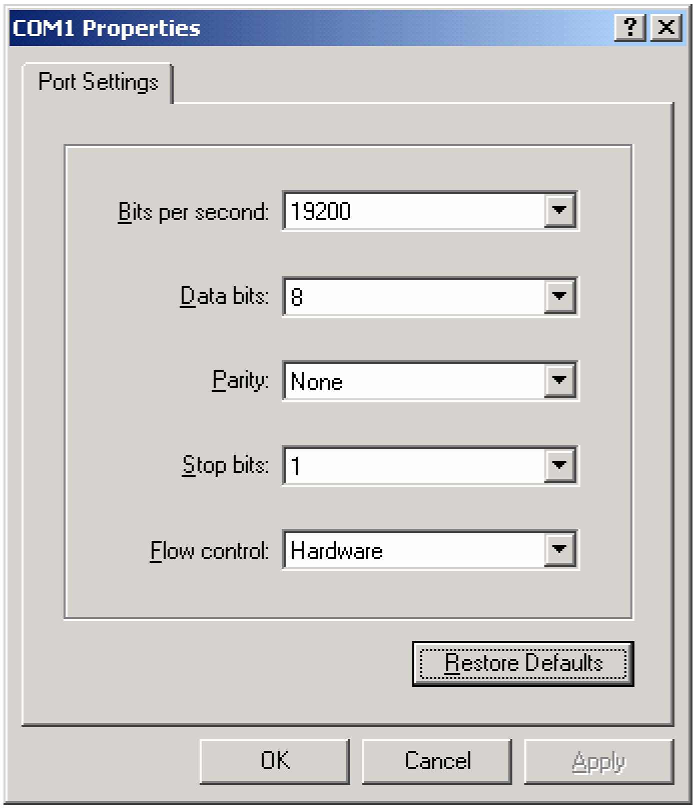
If you are having trouble dialing into the *i*.LON 10 Ethernet adapter, perform the following tests:

Test the Modem

1. Connect the modem to your computer's serial port using the straight-through

modem cable used to connect the *i*.LON 10 to the modem.

2. Open HyperTerminal. Assure that the scroll lock is turned off on your computer (if it is on, press the <Scroll Lock> button to turn it off). In HyperTerminal, set the **Bits Per Second** to the same rate as used to communicate with the *i*.LON 10. Set **Data Bits** to 8, **Parity** to None, **Stop Bits** to 1, and **Flow Control** to Hardware, as shown in the following figure:



Bits per second: 19200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: Hardware

3. In HyperTerminal, turn on Echo. To do this, follow these steps:

   i. Click the **File** menu and select **Properties**. The HyperTerminal **Properties** dialog opens.

   ii. In the **Properties** dialog, select the **Settings** tab.

   iii. Click **ASCII Setup**. The **ASCII Setup** dialog opens.

   iv. In the **ASCII Setup** dialog, set the **Echo Typed Characters Locally** checkbox.

   v. Click **OK** in the **ASCII Setup** and **Properties** dialogs.

4. Request a response from the modem by performing the following steps:

   i. In HyperTerminal, press <Enter> several times. This should allow the modem to automatically detect the baud rate setting of HyperTerminal.

   ii. Type “AT” in capital letters and press <Enter>. The modem should respond with “OK”. If the modem does not respond, repeat this step several times. If you cannot get a response, verify that the modem is turned on.

   iii. If you still get no response, watch the LEDs on the modem when you enter ‘AT”. If they do not flicker, the modem is not responding the command. This could be due to any of the following:

- Wrong type of modem cable being used. Confirm that you are using a straight through cable.
- Faulty modem cable being used. Try a different straight through cable.
- You are connected to a different serial port than the one provided to HyperTerminal. Many computers have multiple serial ports (COM1, COM2, etc.), and often COM1 is used for the internal modem. Try switching HyperTerminal to COM2, COM3, etc.
- Serial port is malfunctioning. Try connecting to a different serial port. Be sure to change the HyperTerminal port settings to the new serial port.

5. Using HyperTerminal, initialize the modem for an incoming call by typing "ATE0Q0V1S0=0&C1&M1" and pressing <Enter>. If you are using a US Robotics modem, use ATE0Q0V1S0=0&C1&B1M1 (the B1 string forces the modem to use the bit rate supplied by the *i*.LON 10).

   You should see a confirmation string from the modem (e.g. "OK") that the initialization string was received. If you do not see a confirmation, enter "AT&F" to reset the modem to its factory defaults, then reenter the initialization string described above.

6. Dial the phone number connected to the modem using a phone or another modem. Watch the HyperTerminal window; if "RING" does not appear, follow these steps:

   i. Connect a phone in parallel to the modem (i.e. use a phone cable splitter). Try dialing the modem again. If the phone does not ring, something may be wrong with your incoming phone line. If the phone, but HyperTerminal does not show the "RING" string, go to the next step.

   ii. Configure the modem to auto-answer after one ring by typing "ATS0=1". The AA LED on the modem should illuminate. Note that this will override the **Answer Phone After <x> Rings** field on the Security Web page. If HyperTerminal still does not pick up, something may be wrong with your modem.

Test the Modem with the *i*.LON 10

This section assumes you have confirmed that the modem is functioning properly, as described in the previous section. To test the *i*.LON 10 with the modem, follow these steps:

1. Attach the modem to the *i*.LON 10 using the same straight-through cable that you used to connect the modem to the PC in the previous sections.

2. Access the *i*.LON 10 via HTTP and configure it for dial-in, as described in Configuring the i.LON 10 Ethernet Adapter for Dial-in, earlier in this chapter. Use the same serial port baud rate specified in *Test the Modem*, earlier in this chapter. Use the same username and password specified in *Test the ISP Phone Number and Account*, earlier in this chapter.

3. Force the serial port to a fixed baud rate that will match the *i*.LON 10. Append &N6&U6 to the **Modem Initialization String** on the PPP Setup Web page (i.e. "ATE0Q0V1S0=0&C1&M1*&N6&U6*") to set the baud rate to 9600 bps.

   See your modem documentation for additional parameters and flags that regulate bit speed.

4. Verify that the user name and password set using **Dial Up and Networking Connections** on the computer matches the user name and password set on the PPP Setup Web page of the *i*.LON 10.
5. Assure that **LCP Extensions** is unchecked in the Windows **PPP Settings** dialog. You can open this dialog by following these steps:
   i. Open the Windows dial-up connection used to dial the *i*.LON 10.
   ii. Select the **Networking** tab.
   iii. Click the **Settings** button.
6. If you are using a computer running Windows 2000 or Windows XP to dial the *i*.LON 10, open a command prompt and enter "netsh ras set tracing ppp enable". This will enable tracing of outgoing calls. A file named "ppp.log" will be created in the <WINNT Director>\tracing folder. Review this file for any errors; see http://support.microsoft.com for more information on how to read this file.

   Once you have completed tracing, open a command prompt and type "ras set tracing ppp disable" to turn off tracing.

Test the *i*.LON 10 After Establishing a Dial-in Connection

This section assumes that you have confirmed that the modem is functioning properly and that a PPP connection is being established between the modem and the dialing computer, as described in the previous sections. To test the *i*.LON 10 after a dial-in connection is established, follow these steps:

1. On the dialing computer, open a command prompt, type "ipconfig", and press <Enter>. A list of all IP addresses allocated to the computer will appear. One of the entries should be "PPP adapter <name of adapter>" where <name of adapter> is the dial-up connection. This IP address should be one greater than that of the *i*.LON 10 device (i.e. if the *i*.LON 10 device's IP address is 192.168.1.222, the PPP adapter entry will show an IP address of 192.168.1.223).
2. On the dialing computer, open a command prompt, type "ping <i.LON 10 IP address>" and press <Enter>. If the *i*.LON 10 is in communication with the computer, you will see responses from the *i*.LON 10.

   If the ping fails there may be a device attached to the computer that is routing packets that should be sent over the dial-up connection over an alternate route. Disable all network cards and dial-up connections other than the *i*.LON 10 dial-up connection.

Configuring the i.LON 10 Ethernet Adapter for Shoulder Tap

To configure the *i*.LON 10 Ethernet adapter to respond to incoming calls by dialing out to an ISP, follow these steps:

1. If **Allow Access to Secure Pages Without a Security Access Reset** is not enabled on the Security Web page, perform a security access reset as described in *Performing a Security Access Reset* in Chapter 5.
2. Click **Security** to open the *i*.LON 10 *Security* Configuration Web page.
3. If it is not already checked, check the **Allow Access to Secure Pages Without a Security Access Reset** option, click **Submit**, and wait for the *i*.LON 10 to reboot.

4. Ensure that the **Allow PPP Dial-back (Shoulder Tap)** checkbox is set. You must clear the **Allow and Authenticate Incoming PPP Connections** checkbox to do this.
5. Set **Respond to Shoulder Tap after <x> Rings**. If the *i*.LON 10 receives a call of at least this many rings, once the caller has hung up, the *i*.LON 10 will initiate a dial-out session.
6. Ensure that the **Enable Outbound PPP Calls** checkbox is set.
7. Set **Number of Retries to Use When Attempting Outbound PPP Connection Attempts**.
8. Click **Submit**.
9. Click **PPP** to open the *i*.LON 10 PPP Configuration Web page.
10. Set the ISP phone number, user name, password, and initialization under **Profile 1** and **Profile 2** as described under *The i.LON 10 Ethernet Adapter PPP Configuration Page*, later in this chapter.
11. Click **Submit**.

When the *i*.LON 10 receives a call of the specified number of rings, it will attempt to dial the number configured in **Profile 1**; if no connection is established, it will attempt the number configured in **Profile 2**; both numbers will be retried up to the number of times specified by the **Number of Retries** option set in step 5.

Analog Modems Tested with the i.LON 10 Ethernet Adapter

The following table lists the analog modems that have been tested with the *i*.LON 10 Ethernet Adapter, as well as recommended modem initialization strings:

Name	**Model**	**Init String**
US Robotics	USR5686E	E0Q0V1S0=0&C1&B1M1
US Robotics	14400 Sportster	E0Q0V1S0=0&C1&B1M1
US Robotics	33600 Sportster	E0Q0V1S0=0&C1&B1M1
US Robotics	V.92 56K	E0Q0V1S0=0&C1&B1M1
ZyXEL	U-1496	E0Q0V1S0=0&C1&B1M1
Intel	144/144e	E0Q0V1S0=0&C1&B1M1
Hayes	Smartmodem Optima 14400	E0Q0V1S0=0&C1&B1M1
Hayes	Smartmodem V series 9600	E0Q0V1S0=0&C1&M1 (default)
Hayes	Ultrasmart modem 9600	E0Q0V1S0=0&C1&M1 (default)
Zoom	3049C	E0Q0V1S0=0&C1&M1 (default)
Zoltrix	Rainbow 56K FMVSP56e	E0Q0V1S0=0&C1&M1 (default)
Modern Blaster	DE5621	E0Q0V1S0=0&C1&M1 (default)

Using GSM/GPRS Modems with the i.LON 10 Ethernet Adapter

In order for a GSM or GPRS modem to communicate with the i.LON 10, it must support all of the following signals: Tx, Rx, GND, RTS, CTS, DSR, DTR and CD. Check with your service provider to confirm that the modem you want to use supports these signals.

GSM/GPRS Service Providers Tested with the *i*.LON 10 Ethernet Adapter

The following table lists the GSM/GPRS service providers that have been tested with the *i*.LON 10 Ethernet Adapter and recommended init strings for each provider:

Service Provider	**Uplink/ Downlink**	**Init String**
T-Mobile	Both	E0Q0V1S0=0&C1M1+CGDCONT=1, "IP","internet2.voicestream.com"
AT&T	Uplink only	E0Q0V1S0=0&C1M1+CGDCONT=1,"IP","proxy"

In order to establish a downlink connection over GSM, a service must support CSD (Circuit Switched Data). This service is supported by T-Mobile. If you want to establish downlink connections using services that do not support CSD (such as AT&T) you have the following options:

- Keep the GSM/GPRS connection open all the time and inform the LNS Server of the IP address.
- Use the shoulder-tap method (see *Configuring the i.LON 10 Ethernet Adapter for Shoulder Tap*, earlier in this Chapter) to have the *i*.LON 10 establish an uplink connection, then ensure that the LNS application sends the downlink messages when the connection is established.

5

i.LON 10 Ethernet Adapter Security

This chapter describes the security of the *i*.LON 10 Ethernet Adapter.

i.LON 10 Ethernet Adapter Security

The *i*.LON 10 Ethernet Adapter can institute a number of measures to make itself as secure as possible:

- *MD5 Authentication.* The *i*.LON 10 Ethernet Adapter provides the option of using MD5 Authentication with all communications between it and the LNS Server, requiring a 16 byte authentication key. See *i.LON 10 Ethernet Adapter Security Web Page* in Chapter 5 for more information.
- *Security Web Page*. The *i*.LON 10 Ethernet Adapter Security Web Page allows you to password protect or disable entirely the ability to access *i*.LON 10 Ethernet Adapter Web pages, load new firmware, dial-in to the *i*.LON 10, or establish uplink communication from an LNS Server.
- *Security Access Reset*. A security access reset can be required to open the security web page, or reset the *i*.LON 10 Ethernet Adapter's configuration. A security access reset requires physical access to the *i*.LON 10 hardware.

Performing a Security Access Reset

If the **Allow Access to this Page Without Security Access Reset (SAR)** option on the Security Web page is not checked, the following features of the *i*.LON 10 Ethernet Adapter are available only after performing a security access reset:

- Access to the MD5 Authentication Key on the Security web page (see *i.LON 10 Ethernet Adapter Security Web Page*, later in this chapter).
- Access to the **Display Factory Defaults** button on the setup web page.
- Access to the security web page (see *i.LON 10 Ethernet Adapter Security Web Page*, earlier in this chapter).
- Access to the Perform self-test page, as described in *Performing a Self-test* in Chapter 6.
- Access to the firmware upgrade web page (see *Uploading i.LON 10 Ethernet Adapter Firmware* in Chapter 6.

To perform a security access reset, follow these steps:

1. Remove the *i*.LON 10 Ethernet Adapter from the TCP/IP network and attach it to the PC using a crossover Ethernet cable or a local server hub.
2. Disconnect the power supply from the *i*.LON 10 Ethernet Adapter.
3. Press and hold the service switch on the *i*.LON 10 Ethernet Adapter using a paper clip or similar device.
4. Reconnect the power supply to the *i*.LON 10 Ethernet Adapter while still pressing in the service switch.
5. Continue holding the service switch. In approximately 10 seconds the wink and connect LEDs will illuminate. Release the service pin.

The *i*.LON 10 Ethernet Adapter will now be in security access mode. When the *i*.LON 10 Ethernet Adapter is in security access mode, its IP address is temporarily changed to `192.168.1.222` and the user name and password are set to `ilon/ilon`; they are changed back to the values set on the Setup and Security web pages once the *i*.LON 10 is reset. In order to access the *i*.LON 10, your computer must be able to communicate on the 192.168.1.x subnet. This can be accomplished in one of the following ways:

- Manually change your computer's IP address to 192.168.1.x (where x is any value from 2-255).
- Open a DOS command line window and enter the following command:

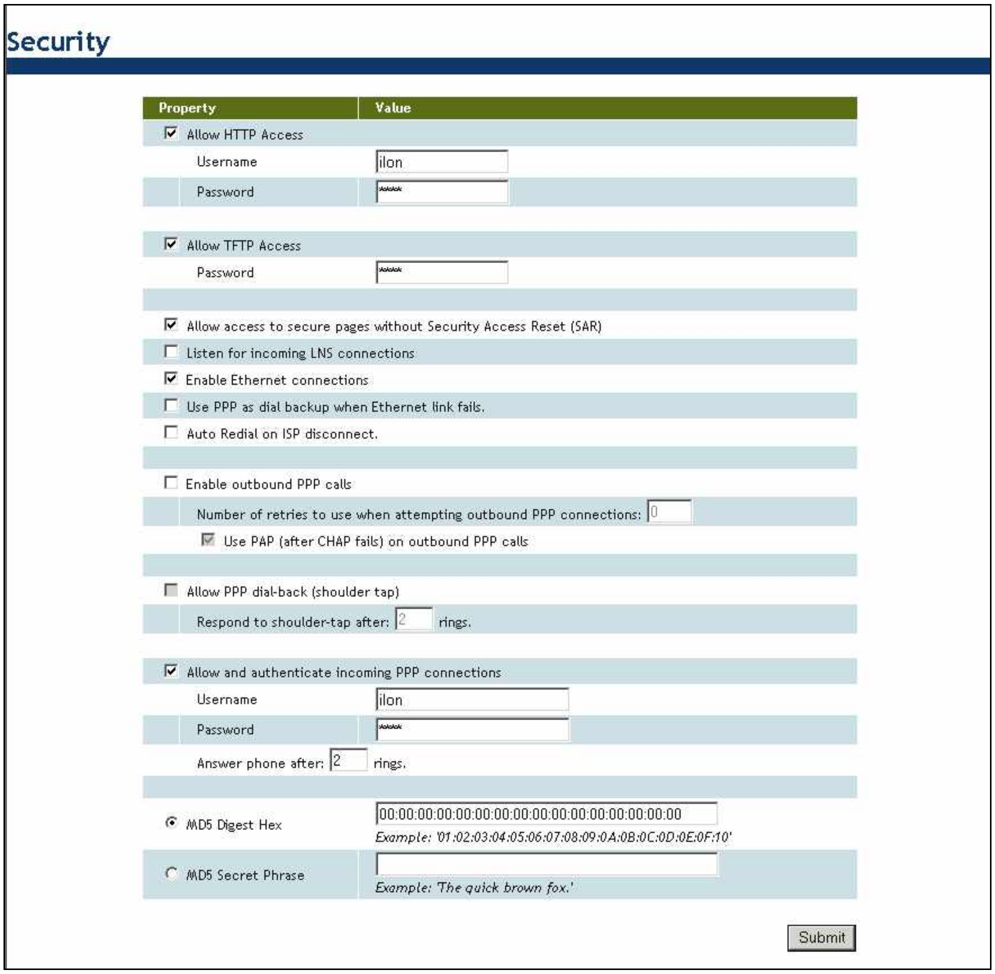
```
route add 192.168.1.0 mask 255.255.255.0
```

When in security access mode you can access the Security Web page and the other features listed above until the *i*.LON 10 is reset.

Once you have made any changes you need to make to the Security Web page, click **Submit**. The *i*.LON 10 will reboot and exit security access mode unless the **Allow Access to Secure Pages Without Security Access Reset (SAR)** option is set.

i.*LON 10 Ethernet Adapter Security Web Page*

Access the Security web page by clicking the Security link on any *i*.LON 10 web page. If the **Allow Access to Secure Pages Without Security Access Reset (SAR)** option is set (see below), this page is accessible even without performing a security access reset. This page appears as shown in the following figure:



Security

Property	Value
☑ Allow HTTP Access	
Username	ilon
Password	****
☑ Allow TFTP Access	
Password	****
☑ Allow access to secure pages without Security Access Reset (SAR)	
□ Listen for incoming LNS connections	
☑ Enable Ethernet connections	
□ Use PPP as dial backup when Ethernet link fails.	
□ Auto Redial on ISP disconnect.	
□ Enable outbound PPP calls	
Number of retries to use when attempting outbound PPP connections: 0	
☑ Use PAP (after CHAP fails) on outbound PPP calls	
□ Allow PPP dial-back (shoulder tap)	
Respond to shoulder-tap after: 2 rings.	
☑ Allow and authenticate incoming PPP connections	
Username	ilon
Password	****
Answer phone after: 2 rings.	
● MD5 Digest Hex	00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00 *Example: '01:02:03:04:05:06:07:08:09:0A:0B:0C:0D:0E:0F:10'*
○ MD5 Secret Phrase	 *Example: 'The quick brown fox.'*

This page contains the following options:

Allow HTTP Access

Set this option to allow users to access the *i*.LON 10 web pages with the exception of the Firmware Page and the Security Page (both of which can only be accessed after a security access reset). If set, enter a **Username** and **Password** that will grant access. The **Username** and **Password** may contain up to 16 alphanumeric characters; they are case sensitive. By default, the **Username** and **Password** are set to `ilon`. If this option is not checked, you will not be able to view any of the *i*.LON 10 web pages without performing a security access reset. Performing a security access reset resets the **Username** and **Password** to `ilon/ilon`. This option is enabled by default, but generally should be disabled once the *i*.LON is placed in the field.

Allow TFTP Access

Set this option to allow users to use TFTP to load new firmware and user web pages (see Uploading a User Web Page in Chapter 6). If set, enter a **Password** that will grant access. The **Password** may contain up to 16 alphanumeric characters; they are case sensitive. **Password** is set to `ilon` by default. Performing a security access reset resets the **Password** to `ilon`. This option is enabled by default, but generally should be disabled once the *i*.LON is placed in the field.

Allow Access to this Page Without Security Access Reset (SAR)

Set this option to allow the Security, Diagnostics, and Firmware Upload Web pages to be opened without a security access reset being performed. This option is enabled by default for ease of set up.

It is strongly recommended that you disable this option before placing the *i*.LON 10 in the field.

Listen for Incoming LNS Server Connections

Set this option to allow downlink connections from external LNS Servers. By default, this option is enabled.

Enable Ethernet Connections

Set this checkbox to allow the i.LON 10 Ethernet Adapter to accept Ethernet connections. This option is enabled by default.

Note: If this option is enabled, the **Allow and Authenticate Incoming PPP Connections** option should be disabled. The *i*.LON 10 does not support simultaneous Ethernet and PPP connections.

Use PPP as Dial Backup when Ethernet Link Fails

Set this checkbox to have the *i*.LON 10 Ethernet Adapter attempt to establish a dial-out connection if an attempt to establish a Ethernet connection fails.

Auto Redial on ISP Disconnect

Set this checkbox to have the *i*.LON 10 Ethernet Adapter automatically attempt to re-establish a dial-out connection if the connection is terminated by the ISP.

Enable Outbound PPP Calls

Set this checkbox to allow the *i*.LON 10 Ethernet Adapter to establish PPP connections. If this checkbox is set, set **Number of Retries to Use When Attempting Outbound PPP Connection Attempts**.

Number of Retries to use when Attempting Outbound PPP Connection Attempts

The number of retries the i.LON 10 Ethernet Adapter will make when attempting to establish a dial-out connection. This value is used any time the *i*.LON 10 makes an outgoing call, whether it initiates the call itself or makes it as a response to a shoulder tap.

Use PAP (After CHAP Fails) on Outbound PPP Connection Attempts

Set this option to allow the *i*.LON 10 Ethernet Adapter to use PAP authentication if the ISP does not support CHAP authentication. This value is used any time the *i*.LON 10 makes an outgoing call, whether it initiates the call itself or makes it as a response to a shoulder tap.

Allow PPP Dial-back (Shoulder Tap)

Set this checkbox to enable shoulder tap on the *i*.LON 10 Ethernet Adapter. If this checkbox is set, set **Respond to Shoulder Tap after <x> Rings** to determine the minimum number of rings that will trigger a dial-out connection. This checkbox cannot be set if **Allow and Authenticate Incoming PPP Connections** is set. See Chapter 4 for more information on shoulder tap connections.

Allow and Authenticate Incoming PPP Connections

Set this checkbox to allow the i.LON 10 Ethernet Adapter to receive incoming calls. If this checkbox is set, set **Username**, **Password**, and **Answer Phone After <x> Rings**. This checkbox cannot be set if **Allow PPP Dial-back (Shoulder Tap)** is set. See Chapter 4 for more information on dial-in connections.

By default **Username** and **Password** are set to 'ilon'.

Some ISPs require additional information (i.e. account ID), or information in a different order (i.e. password, then user name), to log in. In this case, you will need to enter a chat script on the PPP Web page that provides this information in the correct order.

This option is enabled by default, but should be disabled if you do not need to dial into the *i*.LON 10 in the field.

Note: If this option is enabled, the **Enable Ethernet Connections** option should be disabled. The *i*.LON 10 does not support simultaneous Ethernet and PPP connections.

Raw MD5 Authentication Key/Text Shared Secret

A key or phrase used to authenticate communication between the *i*.LON 10 Ethernet adapter and the LNS Server. You can enter either a 16 byte, hexadecimal, colon separated key in **Raw MD5 Authentication** (i.e. `01:02:03:04:05:06:07:08:09:0A:0B 0C:0D:0E:0F:10`) or a word or phrase between 16 and 63 characters long (all white space will be removed) in **Text Shared Secret** (i.e. "the quick brown fox").

If you select **Text Shared Secret**, the **Raw MD5 Authentication Key** will be cleared. If you select **Raw MD5 Authentication Key**, the **Text Shared Secret** will be cleared.

The MD5 authentication key or shared secret entered here must match the key or phrase supplied to the xDriver and LNS Server software with which the *i*.LON 10 Ethernet Adapter communicates.

Using an MD5 authentication key or phrase prevents unauthorized messages from being sent to either the LNS Server or the *i*.LON 10 Ethernet Adapter.

Submit

Click to close this page, write the configuration changes to FLASH memory, and reset the *i*.LON 10 Ethernet Adapter. Configuration changes will take effect upon reboot.

Securing the i.LON 10 Ethernet Adapter

By default, the i.LON 10 Ethernet adapter is configured for ease of use – most security features are disabled so as to allow you to access and configure the *i*.LON 10 device as quickly as possible. Once the *i*.LON 10 is configured, you should enable as much security as possible before placing the *i*.LON 10 in a network. It is recommended that you consider disabling the following options on the security page before placing the *i*.LON 10 in the field:

- **Allow Access to Secure Pages without Security Access Reset (SAR)** – It is ***strongly*** recommended that you disable this option before placing the *i*.LON 10 in the field.
- **Enable HTTP** – Disable this option unless you will need to access the *i*.LON 10 web pages in the field. If you leave this option enabled, be sure to change the default **Username** and **Password**.

- **Enable TFTP –** Disable this option unless you will need to update the *i*.LON 10 user web page in the field. If you leave this option enabled, be sure to change the default **Password**.
- **Allow and Authenticate Incoming PPP Connections** – Disable this option unless you will be dialing into your *i*.LON 10 in the field. If you leave this option enabled, be sure to change the default **Username** and **Password**.

If you will not be dialing directly into the *i*.LON 10, you should also disable the **Allow and Authenticate Incoming PPP Connections**.

6

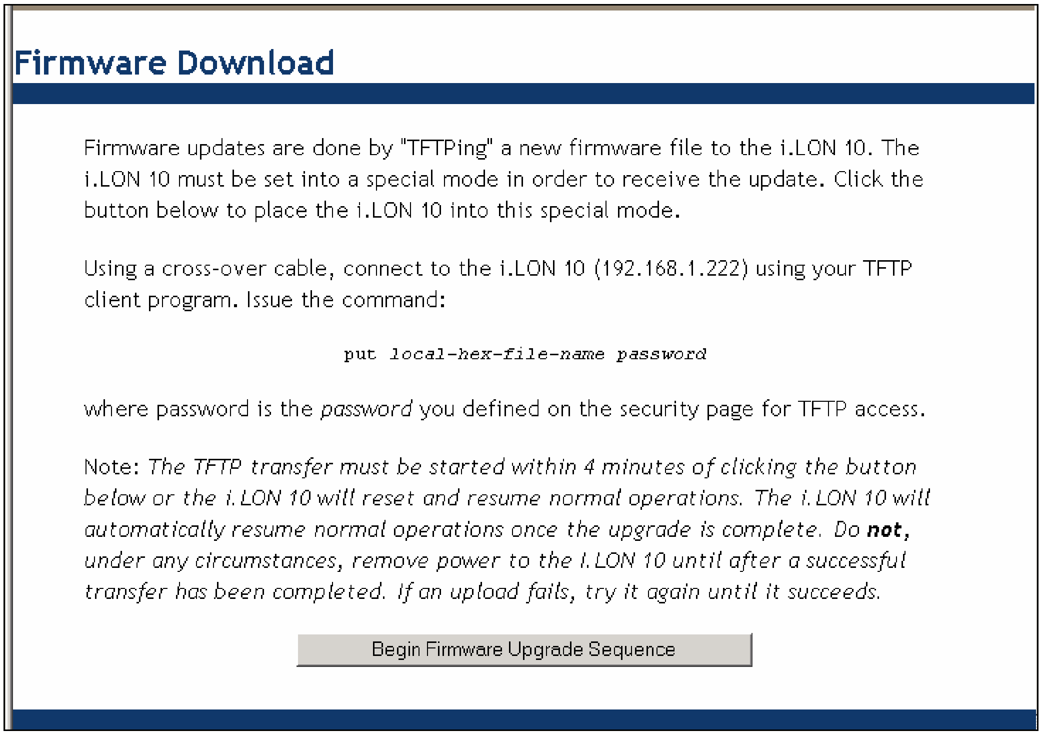
Uploading *i*.LON Network Adapter Firmware and the User Web Page

This chapter describes how to use a TFTP application to upload upgrades to the *i*.LON 10 Ethernet Adapter Firmware and the User Web Page.

Uploading *i*.LON 10 Ethernet Adapter Firmware

Firmware upgrades for the *i*.LON 10 Ethernet Adapter may become available on the Echelon *i*.LON web page (www.echelon.com/ilon). You can check the current version of the firmware on the *i*.LON 10 device's status web page as described in Chapter 7. To upload a firmware upgrade to the *i*.LON 10 Ethernet Adapter hardware, follow these steps:

1. Perform a security access reset (see Performing a Security Access Reset in Chapter 6). Firmware can only be loaded when the *i*.LON 10 is in security access mode.
2. Disconnect the modem cable from the serial port. Otherwise the modem could receive messages from the *i*.LON 10 during download and enter an uncertain state.
3. Access the Firmware Upgrade web page by clicking the Firmware Upgrade link from the Setup web page. This page appears as shown in the following figure:



Firmware Download

Firmware updates are done by "TFTPing" a new firmware file to the i.LON 10. The i.LON 10 must be set into a special mode in order to receive the update. Click the button below to place the i.LON 10 into this special mode.

Using a cross-over cable, connect to the i.LON 10 (192.168.1.222) using your TFTP client program. Issue the command:

```
put local-hex-file-name password
```

where password is the *password* you defined on the security page for TFTP access.

Note: *The TFTP transfer must be started within 4 minutes of clicking the button below or the i.LON 10 will reset and resume normal operations. The i.LON 10 will automatically resume normal operations once the upgrade is complete. Do* ***not***, *under any circumstances, remove power to the I.LON 10 until after a successful transfer has been completed. If an upload fails, try it again until it succeeds.*

4. Click **Begin Firmware Upgrade Sequence**.
5. Open any TFTP client application and point it to 192.168.1.222. You must use this IP address even if you have changed the IP address of the *i*.LON 10 device.
6. Execute the following TFTP command:

   `put <local-hex-file-name> ilon`.

   `local-hex-file-name` is the name of the firmware file obtained from Echelon. The `password` is always `ilon` (the password is set to `ilon` when you enter security access mode).

This command must be executed within 4 minutes of clicking **Begin Firmware Upgrade Sequence**.

Once the upgrade has completed, the Service LED will turn off, indicating the *i*.LON 10 Ethernet Adapter has resumed normal operation. Once you have updated the firmware, you may experience trouble accessing the Setup web page. This is due to Internet Explorer attempting to use a cached version of the setup web page. If this happens, delete your cached web pages (i.e. temporary internet files) and restart Internet Explorer.

Upgrading to Firmware Version 2

When upgrading to version 2 of the *i*.LON 10 firmware, all existing options will be unaffected. The new options will be set to the following defaults:

PPP Properties

PPP Profile 1 Disconnect If Idle For = 20 minutes

PPP profile 2 idletime = 20 minutes

PPP incoming address = 10.0.1.222

PPP answer rings = 2

PPP shoulder tap rings = 2

PPP incoming username = "ilon"

PPP incoming password = "ilon"

PPP profile 1 init string = "E0Q0V1S0=0&C1&M1"

PPP profile 2 init string = "E0Q0V1S0=0&C1&M1"

Security Properties

Allow and Authenticate Incoming PPP Connections = Disabled

Allow Access to this Page (Security) Without Security Access Reset = Disabled

The **Allow and Authenticate Incoming PPP Connections** and **Allow Access to this Page Without Security Access Reset** are disabled to prevent the firmware download from making your *i*.LON 10 less secure. If factory defaults are restored, these options will be enabled.

Uploading a User Web Page

The *i*.LON 10 Ethernet Adapter can host an additional web page of up to 32kB . This feature is provided as a convenience to store information such as the site name or the company logo. This web page cannot serve network variable information (see the *i*.LON 100 and *i*.LON 1000 product lines for devices with this capability).

Your web page must be converted to an Intel hex file (.hex extension) using the Webconvert.exe utility and uploaded to `http://<i.LON 10 IP address>>` using a TFTP client. Assure that TFTP access is enabled on the Security Web page before uploading the file. The Webconvert utility is available on the *i*.LON 10 CD and on Echelon's *i*.LON website. Appendix A describes how to use the Webconvert utility.

Do not overwrite `log.html` or `status.html` in the root directory, as this will overwrite the System Log and Status web pages, respectively.

Using the Microsoft® TFTP Client

You can use Microsoft's TFTP client from a Windows command line to upload a user web page. This can be done using the following format:

```
TFTP -i host PUT source password
```

The –i flag specifies binary image transfer mode, and should always be used when uploading a user web page to the *i*.LON 10 Ethernet Adapter. For example, to upload the file ETH0006.hex from c:\temp to an *i*.LON 10 with an IP address of 192.168.1.222 and a password of `ilon`, you would issue the following command:

```
C:\>tftp –i 192.168.1.222 PUT c:\Program Files\iLON 10
   \iLON 10\Firmware\EethLONb20028.hex
```

7

i.LON 10 Ethernet Adapter Diagnostics

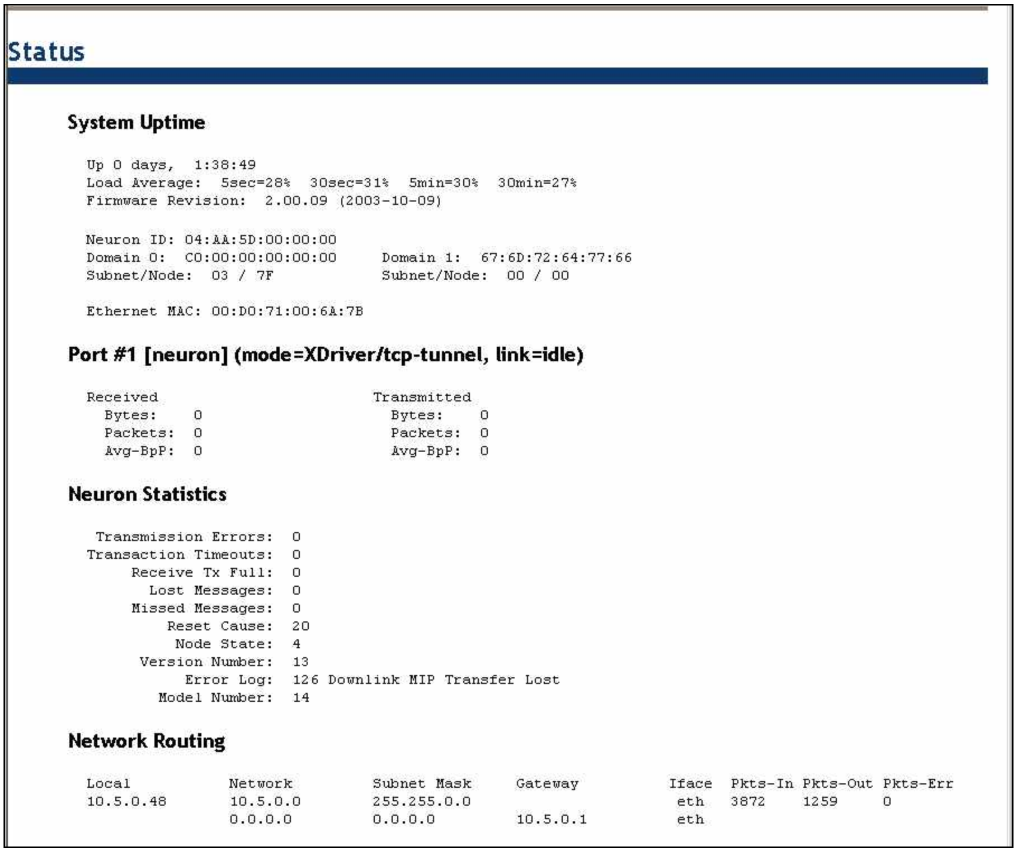
This chapter describes the diagnostic information from the *i*.LON 10 Ethernet Adapter.

i.LON 10 Diagnostics

The *i*.LON 10 Ethernet Adapter provides two web pages that display diagnostic information, the Status page and the Event Log page.

Viewing i.*LON 10 Ethernet Adapter Status*

You can check the status of the *i*.LON 10 Ethernet Adapter by clicking the Status link from the Setup web page. The Status page appears as shown in the following figure:



Status

System Uptime

```
Up 0 days,  1:38:49
Load Average:  5sec=28%  30sec=31%  5min=30%  30min=27%
Firmware Revision:  2.00.09 (2003-10-09)

Neuron ID: 04:AA:5D:00:00:00
Domain 0:  C0:00:00:00:00:00     Domain 1:  67:6D:72:64:77:66
Subnet/Node:  03 / 7F            Subnet/Node:  00 / 00

Ethernet MAC: 00:D0:71:00:6A:7B
```

Port #1 [neuron] (mode=XDriver/tcp-tunnel, link=idle)

```
Received                         Transmitted
  Bytes:    0                      Bytes:    0
  Packets:  0                      Packets:  0
  Avg-BpP:  0                      Avg-BpP:  0
```

Neuron Statistics

```
 Transmission Errors:  0
Transaction Timeouts:  0
     Receive Tx Full:  0
       Lost Messages:  0
     Missed Messages:  0
         Reset Cause:  20
          Node State:  4
      Version Number:  13
           Error Log:  126 Downlink MIP Transfer Lost
        Model Number:  14
```

Network Routing

```
Local          Network        Subnet Mask     Gateway          Iface  Pkts-In Pkts-Out Pkts-Err
10.5.0.48      10.5.0.0       255.255.0.0                       eth   3872    1259     0
               0.0.0.0        0.0.0.0         10.5.0.1          eth
```

This web page displays the status of the *i*.LON 10. This information can be used to troubleshoot communication problems or to verify settings. All information on this page is read-only. This page contains the following information:

System Up Time The time since the last reset.

Load Average The load average as a percentage of the maximum load over the last 5 seconds, 30 seconds, 5 minutes, and 30 minutes.

Firmware Version The current firmware version and the date that firmware was built.

Neuron ID The *i*.LON 10 Ethernet Adapter's 48-bit Neuron ID expressed in hexadecimal.

Domain The LONWORKS Domain address of the *i*.LON 10 Ethernet Adapter. The length of this domain varies and can be set by a network tool such as the LonMaker tool.

Subnet/Node The LONWORKS address associated with the *i*.LON 10 Ethernet Adapter. A network tool such as the LonMaker tool sets this value.

Ethernet MAC The Ethernet MAC address of the *i*.LON 10 Ethernet Adapter.

Transmission Errors The number of CRC errors on the FT or LP channel detected during packet reception since the last reset.

Transmission Timeouts The number of times since the last reset that the *i*.LON 10 Ethernet Adapter expected to receive acknowledgements or responses but did not. These may be due to inaccessible devices, noise on the network, or insufficient buffers on the destination device.

Receive Tx Full The number of times since the last reset that an incoming packet was discarded because there was no room in the *i*.LON 10 device's transaction buffer.

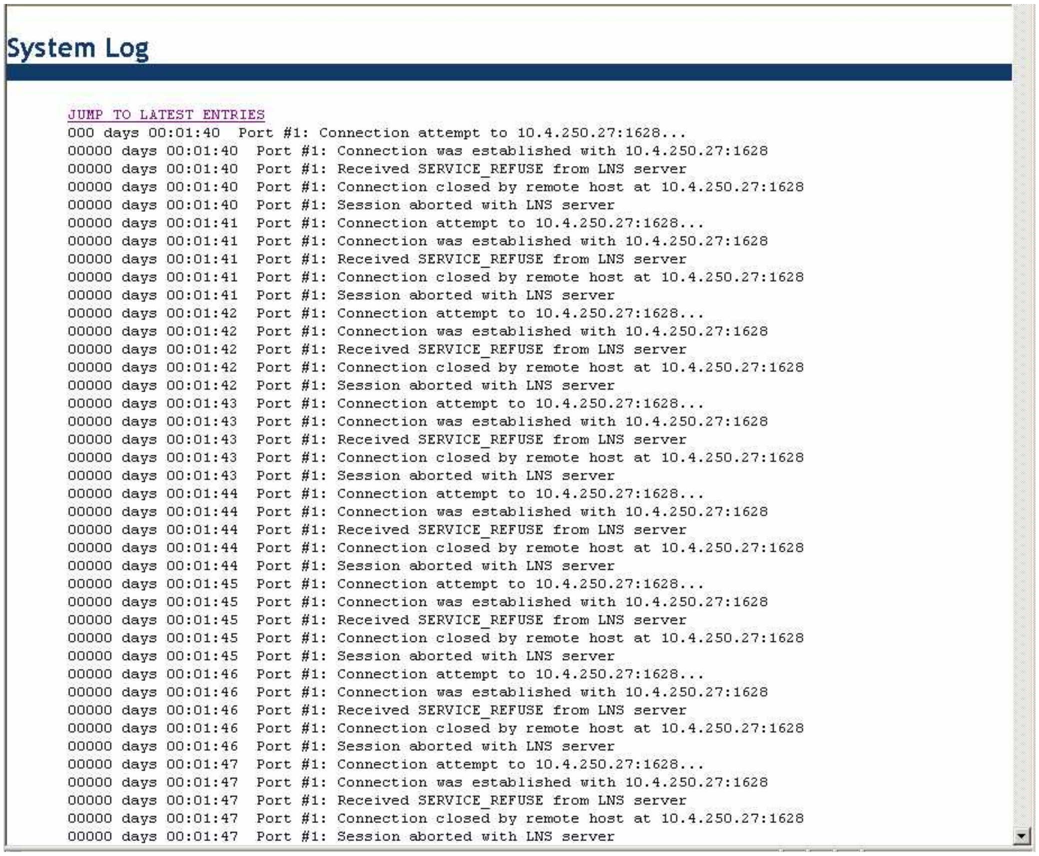
Lost Messages The number of times since the last reset that an incoming packet was discarded because there was no application buffer available.

Missed Messages The number of times since the last reset that an incoming packet was discarded because there was no network buffer available.

Network Routing The local and destination IP addresses, subnet mask, gateway, interface, and packet count since the last reset. The IP addresses, subnet mask, and gateway can be can be set as described in *Using the i.LON 10 Ethernet Adapter* in Chapter 3.

Viewing the i.LON 10 System Log Web Page

The *i*.LON 10 Ethernet Adapter System Log web page lists network events. This web page is accessed by clicking the System Log link on the *i*.LON 10 Ethernet Adapter web page. This web page appears as shown in the following figure:



System Log

JUMP TO LATEST ENTRIES

```
000 days 00:01:40  Port #1: Connection attempt to 10.4.250.27:1628...
00000 days 00:01:40  Port #1: Connection was established with 10.4.250.27:1628
00000 days 00:01:40  Port #1: Received SERVICE_REFUSE from LNS server
00000 days 00:01:40  Port #1: Connection closed by remote host at 10.4.250.27:1628
00000 days 00:01:40  Port #1: Session aborted with LNS server
00000 days 00:01:41  Port #1: Connection attempt to 10.4.250.27:1628...
00000 days 00:01:41  Port #1: Connection was established with 10.4.250.27:1628
00000 days 00:01:41  Port #1: Received SERVICE_REFUSE from LNS server
00000 days 00:01:41  Port #1: Connection closed by remote host at 10.4.250.27:1628
00000 days 00:01:41  Port #1: Session aborted with LNS server
00000 days 00:01:42  Port #1: Connection attempt to 10.4.250.27:1628...
00000 days 00:01:42  Port #1: Connection was established with 10.4.250.27:1628
00000 days 00:01:42  Port #1: Received SERVICE_REFUSE from LNS server
00000 days 00:01:42  Port #1: Connection closed by remote host at 10.4.250.27:1628
00000 days 00:01:42  Port #1: Session aborted with LNS server
00000 days 00:01:43  Port #1: Connection attempt to 10.4.250.27:1628...
00000 days 00:01:43  Port #1: Connection was established with 10.4.250.27:1628
00000 days 00:01:43  Port #1: Received SERVICE_REFUSE from LNS server
00000 days 00:01:43  Port #1: Connection closed by remote host at 10.4.250.27:1628
00000 days 00:01:43  Port #1: Session aborted with LNS server
00000 days 00:01:44  Port #1: Connection attempt to 10.4.250.27:1628...
00000 days 00:01:44  Port #1: Connection was established with 10.4.250.27:1628
00000 days 00:01:44  Port #1: Received SERVICE_REFUSE from LNS server
00000 days 00:01:44  Port #1: Connection closed by remote host at 10.4.250.27:1628
00000 days 00:01:44  Port #1: Session aborted with LNS server
00000 days 00:01:45  Port #1: Connection attempt to 10.4.250.27:1628...
00000 days 00:01:45  Port #1: Connection was established with 10.4.250.27:1628
00000 days 00:01:45  Port #1: Received SERVICE_REFUSE from LNS server
00000 days 00:01:45  Port #1: Connection closed by remote host at 10.4.250.27:1628
00000 days 00:01:45  Port #1: Session aborted with LNS server
00000 days 00:01:46  Port #1: Connection attempt to 10.4.250.27:1628...
00000 days 00:01:46  Port #1: Connection was established with 10.4.250.27:1628
00000 days 00:01:46  Port #1: Received SERVICE_REFUSE from LNS server
00000 days 00:01:46  Port #1: Connection closed by remote host at 10.4.250.27:1628
00000 days 00:01:46  Port #1: Session aborted with LNS server
00000 days 00:01:47  Port #1: Connection attempt to 10.4.250.27:1628...
00000 days 00:01:47  Port #1: Connection was established with 10.4.250.27:1628
00000 days 00:01:47  Port #1: Received SERVICE_REFUSE from LNS server
00000 days 00:01:47  Port #1: Connection closed by remote host at 10.4.250.27:1628
00000 days 00:01:47  Port #1: Session aborted with LNS server
```

The following events are logged in this web page:

Message	Description
`=====iLON-10 Started=====`	The i.LON 10 Ethernet Adapter unit has been started in one of the following ways: • by plugging in the power adapter. • by saving a new configuration.
`===== i.LON-10 Started in SECURE MODE =====`	This message indicates the unit was started in SECURE MODE (holding the Service Pin in for 10 seconds as the unit is powered on).
`===== i.LON-10 Started in MANUFACTURING MODE =====`	This message indicates the unit was started in MANUFACTURING MODE. This message appears only as part of the manufacturing process.
`NEURON: reset detected`	This message indicates that a Neuron Chip reset has occurred. This typically happens after an LNS connection has been established
`NEURON: Chip not responding to Queries.  May be non-functional`	This message indicates that the unit has not been able to receive responses to queries sent to the *i*.LON 10 device's

Message	Description
	internal Neuron Chip for at least 1 minute after startup.
`HTTP: host at <IP Address> failed to authenticate properly`	This message indicates that an attempt was made from <IP Address> to access the configuration web pages, but that attempt was not successful.
`Configuration changes saved -- restarting system`	This message indicates that a configuration change was saved.
`Configuration changes could not be saved -- restarting system`	This message indicates that a configuration change was attempted but could not be saved. This indicates a failure to properly write configuration to flash. This may occur when the flash has exceeded its life expectancy after too many overwrites of the configuration area. The unit should probably be returned for service (new flash chip installed).
`Could not save Configuration after reset of TrafficTest Mode`	This message indicates that after a traffic mode reset was detected, the unit could not modify and save the configuration to disable this mode for the next power up. This indicates a failure to properly write configuration to flash. This may occur when the flash has exceeded its life expectancy after too many overwrites of the configuration area. The unit should probably be returned for service (new flash chip installed).
`current system time`	This message indicates the current time in the unit. This normally indicates the time the unit has been operational since the last power on.
`Port #n: RSN request from Host failed Authentication`	This message indicates that the Authentication for the RSN packet did not pass. Every RSN packet that fails authentication will be logged. The data in the packet is not logged.
`Port #n: Encrypted Data Packet from Host failed Authentication`	This message indicates that the Authentication for the ENCRYPTED packet did not pass. Every ENCRYPTED packet that fails authentication will be logged. The data in the packet is not logged.
`Port #n: Received`	This message indicates that the LNS

Message	Description
`IDENT_UNKNOWN from LNS server`	server has sent an XDRIVER_ACK message with reason code set to IDENT_UNKNOWN.
`Port #n: Received SERVICE_UNAVAIL from LNS server`	This message indicates that the LNS server has sent an XDRIVER_ACK message with reason code set to SERVICE_UNAVAIL.
`Port #n: Received SERVICE_REFUSE from LNS server`	This message indicates that the LNS server has sent an XDRIVER_ACK message with reason code set to SERVICE_REFUSE.
`Port #n: Received UNKNOWN reason code hh from LNS server`	This message indicates that the LNS server sent an XDRIVER_ACK message with reason code set to the hex value indicated.
`Port #n: Could not deliver IP address event to LNS server`	This message indicates that the i.LON 10 could not successfully notify any LNS server of the new IP address.
`Port #n: Session recovery succeeded with LNS server`	This message indicates that the i.LON 10 succeeded in recovering the previous xDriver session with current LNS server.
`Port #n: Session recovery failed with LNS server`	This message indicates that the i.LON 10 failed in recovering the previous xDriver session with current LNS server.
`Port #n: Uplink qualified message received from Neuron Interface`	This message indicates that the i.LON 10 received a qualified uplink message from a Neuron chip.
`Port #n: Session established with LNS server`	This message indicates that initiating message sequence of IDENT - RSN - RSN_RESP has been completed. The i.LON 10 now considers the LNS session active for data transport.
`Port #n: Session closed with LNS server`	This message indicates that the current LNS server shutdown in an orderly manner.
`Port #n: Session aborted with LNS server`	This message indicates that the current LNS server shutdown abruptly without first receiving a TERM command.
`Port #n: sessionid/sequence number invalid on incoming xDriver packet`	This message indicates that the expected sessionid or sequence number does not match the data in the incoming xDriver packet.

Message	Description
Port #n: could not write Configuration data after xDriver INCAUTH command	This message indicates that the new secret key and configuration were not properly saved. This message should never be seen. If it is, the unit should probably be returned for service (ie, a new flash chip installed.)
Port #n: Listening for connection on tcp port <Port Number>	The i.LON 10 Ethernet Adapter is setting up a socket to listen for LNS Servers on the given port number.
Port #n: Connection attempt to ###.###.###.###:#####..."	This message indicates that the system has started the process to contact the remote LNS server at the given IP address given on port number.
Port #n: Incoming connection on tcp port xxxx from ###.###.###.###:#####	The i.LON 10 Ethernet Adapter has detected an incoming communication from a remote host.
Port #n: Keep alive timeout detected on LNS connection	This message indicates that the connection to the LNS server is non-responsive. A keep-alive message was sent with no response from the LNS server.
Port #n: Connection was established with ###.###.###.###:#####	The i.LON 10 Ethernet Adapter detected an incoming communication and a connection has been established.
Port #n: Connection was refused by ###.###.###.###:#####…	The i.LON 10 Ethernet Adapter would not accept a connection.
Port #n: No response connecting to host at ###.###.###.###:#####	This message indicates that the remote system has not responded to any TCP session establishment requests.
Port #n: No response from host at ###.###.###.###:#####	This message indicates that the remote system has stopped responding to TCP traffic we are sending after it had been responding earlier.
Port #n: Connection reset by remote host at ###.###.###.###:#####	This message indicates that the remote host forcibly terminated the TCP session that was started or active.
Port #n: Connection closed by us to host at ###.###.###.###:#####	This message indicates that the TCP session is being closed by the *i*.LON 10.
Port #n: Connection closed by remote host at ###.###.###.###:#####	This message indicates that the remote host has requested a close of TCP communications.

Message	Description
Port #n: Listening for connections on tcp port pppp was not possible (Error #nn) Port #n: Connection attempt to ###.###.###.###:##### was not possible (Error #nn) Port #n: Incoming connection on tcp port <Port Number> from ###.###.###.###:##### (Error #nn)"	This message indicates that a TCP connection was not possible due to error nn. Errors are listed below: 1 - the i/o request has been scheduled but not completed 2 - no more i/o paths are available 3 - requested operation was not supported by the driver 4 - the provided i/o buffer was not valid 5 - requested operation cannot be done in current state 6 - too many connections of this type are already open 7 - socket connection type ("domain") is unknown 8 - socket protocol type is unknown 9 - socket has already been bound to another port 10 - requested port number is already is use 11 - requested address was not valid for operation 12 - operation requires bound port but socket is unbound 13 - device is not ready for the requested operation 14 - cannot open connection because socket is already connected 15 - operation requires connected socket but not connected 16 - data message is too big for transport type (usually udp) 17 - requested operation would block this thread -- try later 18 - incoming data corruption has been detected 19 - no data is available for this operation 20 - no route available from this host to destination host 21 - storage device can accept no more data (eg. disk full) 22 - requested option is not available

Message	Description
`Port #n: Session aborted with LNS server`	This message indicates that the current LNS server shutdown abruptly without first receiving a TERM command.
`Port #n: sessionid/sequence number invalid on incoming Xdriver packet`	This message indicates that the expected `sessionid` or `sequence number` does not match the data in the incoming Xdriver packet.
`Port #n: could not write Configuration data after Xdriver INCAUTH command`	This message indicates that the new secret key and configuration were not properly saved.
`Port #n: Session to LNS server closed since 10BaseT connections are disabled`	This message indicates that the recently-established TCP session over Ethernet on the LNS port has been closed since the configuration disables 10BaseT connections. This message is only encountered when incoming LNS sessions are permitted, but the 10BaseT interface is not allowed to handle the session.
`Port #1: Size of authentication digest incorrect`	This message indicates that the unit received an xDriver packet with unsupported digest size from the LNS server. This error can indicate that a version 2.0 *i*.LON 10 is being used with a version of LNS older than LNS 3 Service Pack 8, Update 1. This message should normally be followed by a further log message indicating the contents of an XDRIVER_ACK packet if this is what caused the error.
`DNS: primary server is <IP Address>; secondary server is <IP Address>; default domain is "<Domain Name>"`	This message indicates that the primary server, secondary server, and default domain have been defined with the given values. Note that the primary or secondary entries are only listed if they have been defined. The default domain will be given even if empty ("").
`DNS: unavailable (no server information provided)"`	This message indicates that no DNS information has been entered into the configuration of the unit.
`DNS: "<Hostname>" does not exist (non-authoritative answer)"`	This message indicates that the DNS server responded to the query but has no entry for the given hostname. The DNS server gave this response as a non-

Message	Description
	authoritative answer.
DNS: "<Hostname>" does not exist (authoritative answer)"	This message indicates that the DNS server responded to the query but has no entry for the given hostname. The DNS server gave this response as an authoritative answer.
DNS: "<Hostname>" resolved to <IP Address> (<Fully qualified name>)"	This message indicates that the DNS server responded to the query with an IP address. The fully-qualified name is given in parenthesis.
DNS: "<Hostname>" lookup failed (no response from DNS servers)	This message indicates that the DNS server did not respond to the query.
PPP: Connection has been terminated.	This message indicates that the PPP connection has been ended.
CHAT: attempting connection to phone number 'xxx-xxxx'	This message indicates that the CHAT system is starting up and attempting to make a connection to the indicated phone number.
CHAT: carrier-detect is still asserted (previous connection won't drop?)	This message indicates that the CHAT system cannot start a new connection attempt as the old one doesn't appear to want to close.
CHAT: could not reset modem with ATZ	This message indicates that the modem did not respond with "OK" after sending the ATZ command to reset.
CHAT: could not init modem with ATiiii	This message indicates that the modem did not respond with "OK" after sending the initialization string ATiiii (where iiii is the configured initialization string).
CHAT: could not dial modem with ATDoooo (reason)	This message indicates that the modem could not dial the number 'oooo' because of the 'reason' given.
CHAT: did not receive expect 'string' (!timeout!)	This message indicates that the chatscript being executed was waiting for 'string', but those characters were not received within the expected time.
CHAT: Modem connected with remote host (CONNECT string)	This message indicates that the modem returned a "CONNECT" string with any 'string' returned by the modem.
AUTOPPP: Shoulder Tap detected. Attempting call...	This message indicates that the i.LON 10 receives a shoulder tap call and is trying

Message	Description
	to dial out.
AUTOPPP: Incoming call accepted	This message indicates that the i.LON 10 has received the configured number of rings and has issued an "ATA" command to the modem to answer the call.
AUTOPPP: Two successive attempts to 'xxx-xxxx' resulted in answer but no carrier (possibly voice)	These messages indicate that there were two consecutive voice answers on the phone number dialed. No further attempts on this number are permitted. These two messages will appear together.
AUTOPPP: The FCC requires that no further attempts to that number be made	
AUTOPPP: Successive calls to 'xxx-xxxx' resulted in no answer from the host"	These messages indicate that there were two consecutive unanswered or uncompleted calls to the number. Due to FCC regulations of a maximum of 10 calls per hour to the same number, each successive call to a number will be delayed by an additional minute to a maximum of 10 minutes between calls. These two messages will appear together.
AUTOPPP: The FCC allows no more than 10 attempts per hour -- number throttled	
AUTOPPP: Shoulder Tap not allowed due to FCC regulations (two previous voice calls)	These messages indicate that the i.LON 10 received a shoulder tap call but detected two voice calls at this number previously. FCC regulations prohibit the i.LON 10 from dialing this number again. These two messages will appear together.
AUTOPPP: The FCC requires that no further attempts to that number be made	
PPP: connection has been terminated	This message indicates that the PPP session has been terminated. Note that a reason may appear in parenthesis in the same System Log message. This message may include a reason in parenthesis, described below.
PPP: could not establish connection	This message indicates that the PPP session was not established for some reason. Note that a reason may appear in parenthesis in the same System Log message. This message may include a reason in parenthesis, described below.
PPP: User id/Password not accepted.	This message indicates that the PPP session was not established for some reason. Note that a reason may appear in

Message	Description
	parenthesis in the same message. This message may include a reason in parenthesis, described below.
	The previous three messages, may include one of the following reasons:
	(ISP_specific_message) – A message sent by the ISP and passed on to the *i*.LON 10 system log. Contact your ISP for more information on this message.
	(no reply to echo requests) – PPP echo requests do not result in a response from the PPP peer.
	(carrier lost) – The carrier has been lost.
	(remote won't assign IP address) – In the IPCP negotiation phase, the peer is not assigning an IP address for requests from the unit.
	(xxx.xxx.xxx.xxx) – The IP address assigned to the unit by the peer.
	(could not negotiate link) – PPP could not be established.
	(could not negotiate authentication) – The peer requests an authentication method that is not supported and will not accept methods the unit suggests.
	(could not negotiate network) – The network could not be negotiated.
	(our standard LCP code was rejected) – The peer rejected the standard LCP codes that the i.LON 10 used during the LCP negotiation.
	(our standard IPCP code was rejected) – The peer rejected the standard IPCP codes that the i.LON 10 used during the network negotiation.
	(modem did not assert DCD) – The modem did not send a DCD (carrier detect) signal after being connected.
`PPP: connection has been idle for xxx seconds`	This message indicates that the PPP session has not seen any significant packets for the amount of time shown. This time is equal to or greater than the configured idle timer and the connection will be terminated.
`PPP: Incoming connection is`	This message indicates that an incoming

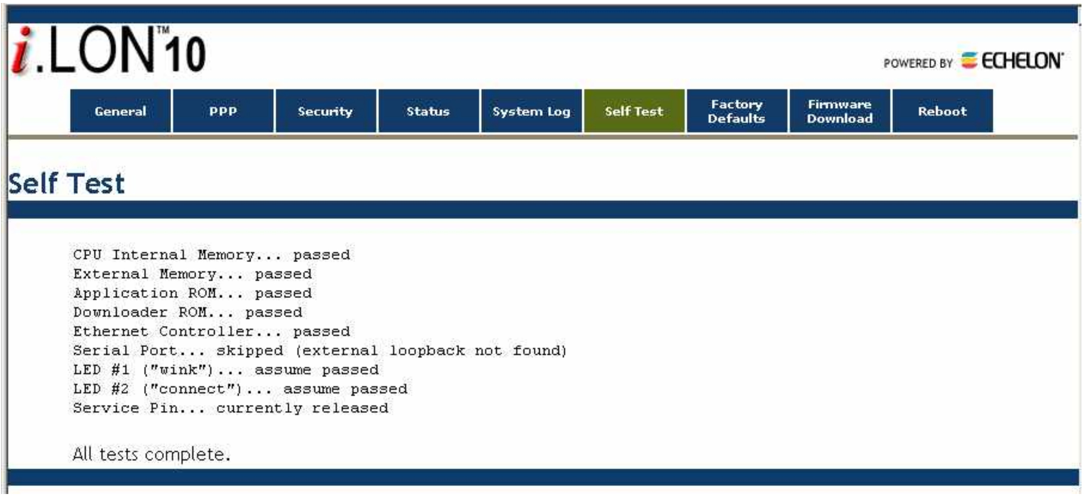
Message	Description
`received`	call has been detected and answered.
`PPP: Network connection established`	This message indicates that a network connection has been established through PPP. The IP address obtained will appear in parenthesis next to the message.
`PPP: Incoming connection authentication succeeded`	This message indicates that an incoming call has been authenticated and a connection has been established.
`PPP: Incoming connection authentication failed`	This message indicates that an incoming call's authentication was rejected. This could be due to an incorrect user name or password.
`PPP: Shoulder tap rings are received`	This message indicates that the *i*.LON 10 has received a call with sufficient rings to begin a shoulder tap response.
`Static IP address change detected`	This message indicates that the unit detects a static IP address change event caused by user configuration.
`Uplink session recovery event detected`	This message indicates that the unit detected a session recovery event when it powers up or during normal operation. A previous uplink connection was terminated abnormally. The i.LON 10 will attempt to reconnect to the LNS server.

Performing a Self-test

To perform a self-test on the i.LON 10, click the Perform Self-Test link on the *i*.LON 10 Ethernet Adapter Web page. The *i*.LON 10 application halts and a self-test procedure begins. A self-test can only be performed when the i.LON 10 is in security access mode.

Note: The self-test procedure can cause connection problems and should not be performed while the *i*.LON 10 is being used as an RNI.

The results of the test are shown in the Perform Self-test web page, shown in the following figure:



Self Test

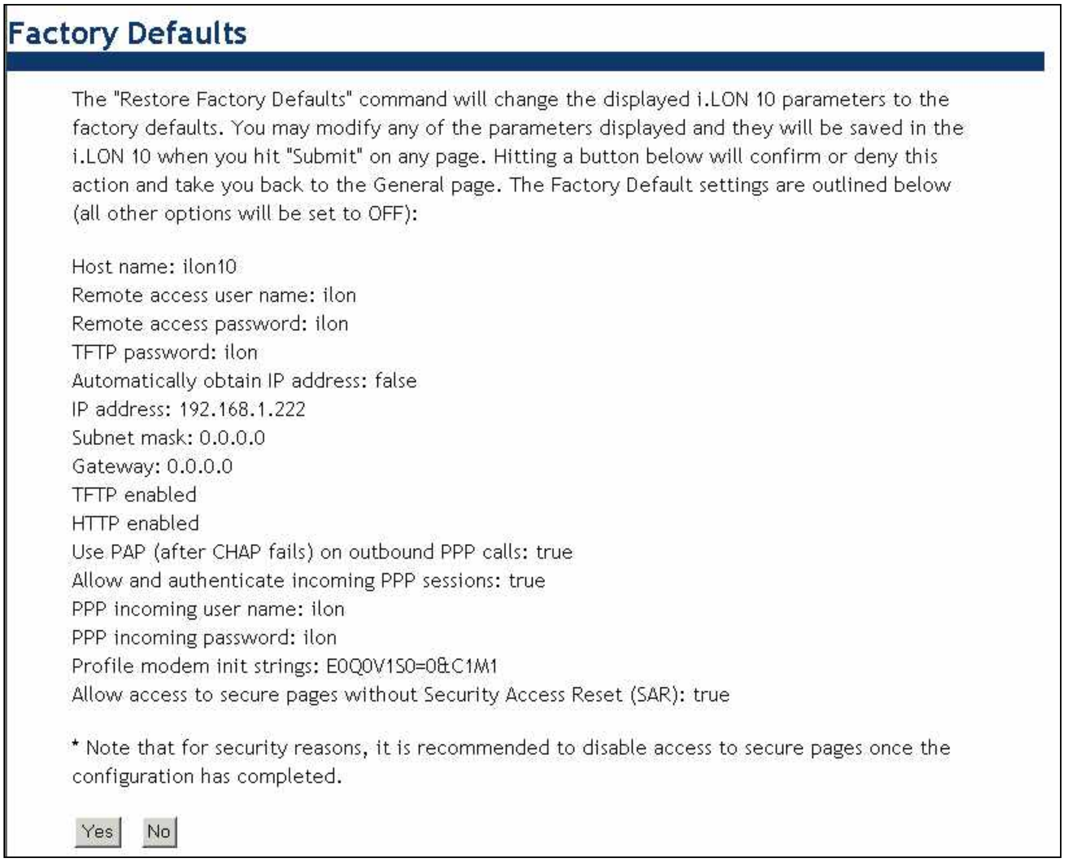
```
CPU Internal Memory... passed
External Memory... passed
Application ROM... passed
Downloader ROM... passed
Ethernet Controller... passed
Serial Port... skipped (external loopback not found)
LED #1 ("wink")... assume passed
LED #2 ("connect")... assume passed
Service Pin... currently released
```

All tests complete.

A series of tests and results will display as shown above. When the LED #1 and LED #2 tests occur, the appropriate LED will flash so you can verify that it is functioning.

Restoring Factory Defaults

To reset the *i*.LON 10 Ethernet Adapter to its factory defaults, click the *Factory Defaults* link on the *i*.LON 10 Web Page. This link is only available after a security access reset. The following web page opens:



Factory Defaults

The "Restore Factory Defaults" command will change the displayed i.LON 10 parameters to the factory defaults. You may modify any of the parameters displayed and they will be saved in the i.LON 10 when you hit "Submit" on any page. Hitting a button below will confirm or deny this action and take you back to the General page. The Factory Default settings are outlined below (all other options will be set to OFF):

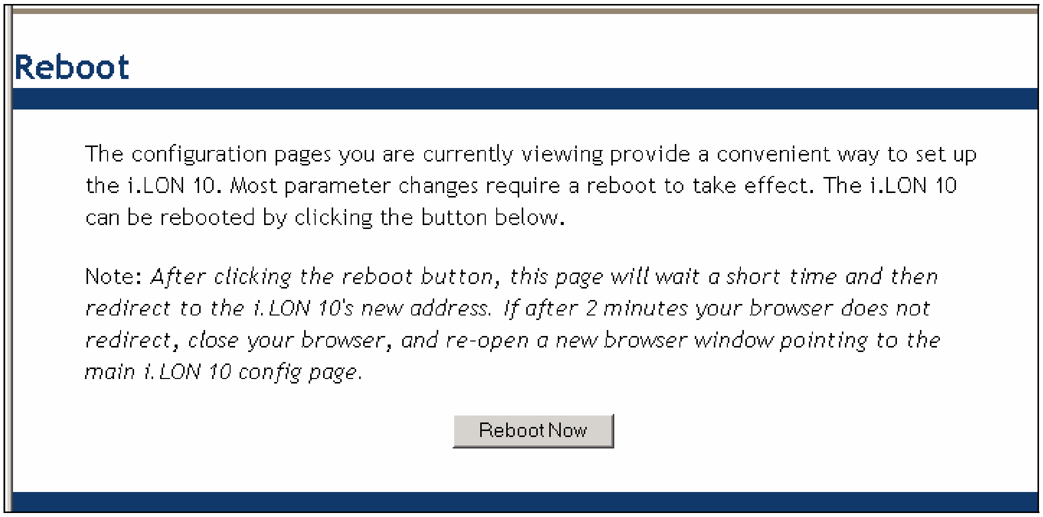
Host name: ilon10
Remote access user name: ilon
Remote access password: ilon
TFTP password: ilon
Automatically obtain IP address: false
IP address: 192.168.1.222
Subnet mask: 0.0.0.0
Gateway: 0.0.0.0
TFTP enabled
HTTP enabled
Use PAP (after CHAP fails) on outbound PPP calls: true
Allow and authenticate incoming PPP sessions: true
PPP incoming user name: ilon
PPP incoming password: ilon
Profile modem init strings: E0Q0V1S0=0&C1M1
Allow access to secure pages without Security Access Reset (SAR): true

* Note that for security reasons, it is recommended to disable access to secure pages once the configuration has completed.

To restore factory defaults, click **Yes**. A confirmation page with a **Submit** button will appear. Click **Submit** to restore defaults and reboot the *i*.LON 10. Note that if your PC is not on the 192.168.1.x subnet, you may have to change the IP settings of your PC to communicate with the *i*.LON 10 Ethernet Adapter or use the route command described in the Quick Start and in *Performing a Security Access Reset*.

Rebooting the i.LON 10 Ethernet Adapter

To reboot the *i*.LON 10 Ethernet Adapter, click the *Reboot* link on the *i*.LON 10 Web page. The following Web page opens:



Reboot

The configuration pages you are currently viewing provide a convenient way to set up the i.LON 10. Most parameter changes require a reboot to take effect. The i.LON 10 can be rebooted by clicking the button below.

Note: *After clicking the reboot button, this page will wait a short time and then redirect to the i.LON 10's new address. If after 2 minutes your browser does not redirect, close your browser, and re-open a new browser window pointing to the main i.LON 10 config page.*

To reboot the *i*.LON 10 Ethernet Adapter, click **Reboot Now**. You will have to wait approximately two minutes for the reboot to complete.

8

Establishing an Uplink Connection Through the *i*.LON 10 Ethernet Adapter

This chapter describes how to establish an uplink connection through the *i*.LON 10 Ethernet Adapter.

Uplink Connections

An uplink connection is a connection initiated by a device on the network attempting to communicate with the LNS Server on the other side of the *i*.LON 10 adapter. This occurs when a device sends data to the LNS Server without the data being requested, such as when one or more network variables are bound to the host (see the *LNS Programmer's Guide*, the *LonMaker User's Guide*, and the *LNS for Windows Programmer's Guide, xDriver Supplement* for more information).

You can determine what sorts of network variable and application messages will cause an uplink to occur as described in *The i.LON 10 Ethernet Adapter General Configuration Page* in Chapter 3.

When an uplink connection is established, the *i*.LON 10 will use a local port between 16384 and 65535 to receive communications from the LNS Server. This port is used only while the uplink session is negotiated. The predetermined downlink port will be used for monitoring or control that following the uplink event. Talk to your ISP or IT department to ensure that the i.LON 10 is able to receive messages on these ports.

LONWORKS broadcast messages will never cause an uplink to be initiated.

Listening for an Ethernet Uplink Connection

To listen for an uplink connection on your computer's Ethernet port (sent by an *i*.LON 10 that is connected to a TCP/IP network or that dials into an ISP), follow these steps:

1. Assure that there is at least one xDriver profile and uplink session handling is enabled. To enable uplink session handling, open the xDriver profile from the LONWORKS Interfaces control panel applet, click the **Properties** button in the **Profile** box, and configure the **Uplink Sessions** tab. For more information, click **Help** or see the *LNS for Windows Programmer's Guide, xDriver Supplement*.
2. Start the xDriver connection broker as described in Chapter 3 of the *LNS for Windows Programmer's Guide, xDriver Supplement*.
3. Start an LNS application that listens for xDriver Broker events. See the *LNS for Windows Programmer's Guide, xDriver Supplement* for more information.

Listening for a PPP Uplink Connection

To listen for a uplink PPP connection on your computer's serial port (sent by an *i*.LON 10 directly dialing the PC), follow these steps:

1. Open your computer's network properties. On Windows 2000 and Windows XP, you do this by opening the **Network and Dial-up Connections** control panel applet.
2. Configure the computer to listen for incoming calls on the port to which the modem is attached. On Windows 2000 and Windows XP, you do this by creating a new connection and using the **New Connection Wizard** to create a connection that accepts incoming calls on the appropriate port.
3. Start the xDriver connection broker as described in Chapter 3 of the *LNS for Windows Programmer's Guide, xDriver Supplement*.

4. Start an LNS application that listens for xDriver Broker events. See the *LNS for Windows Programmer's Guide, xDriver Supplement* for more information.

Appendix A

Using the Webconvert Utility

The Webconvert utility is a program that is used to convert web pages into the Intel hex format (`.hex` extension) that can be downloaded to the *i*.LON 10 Ethernet Adapter. This appendix contains instructions for using the Webconvert utility. See Uploading a User Web Page in Chapter 6 for more information.

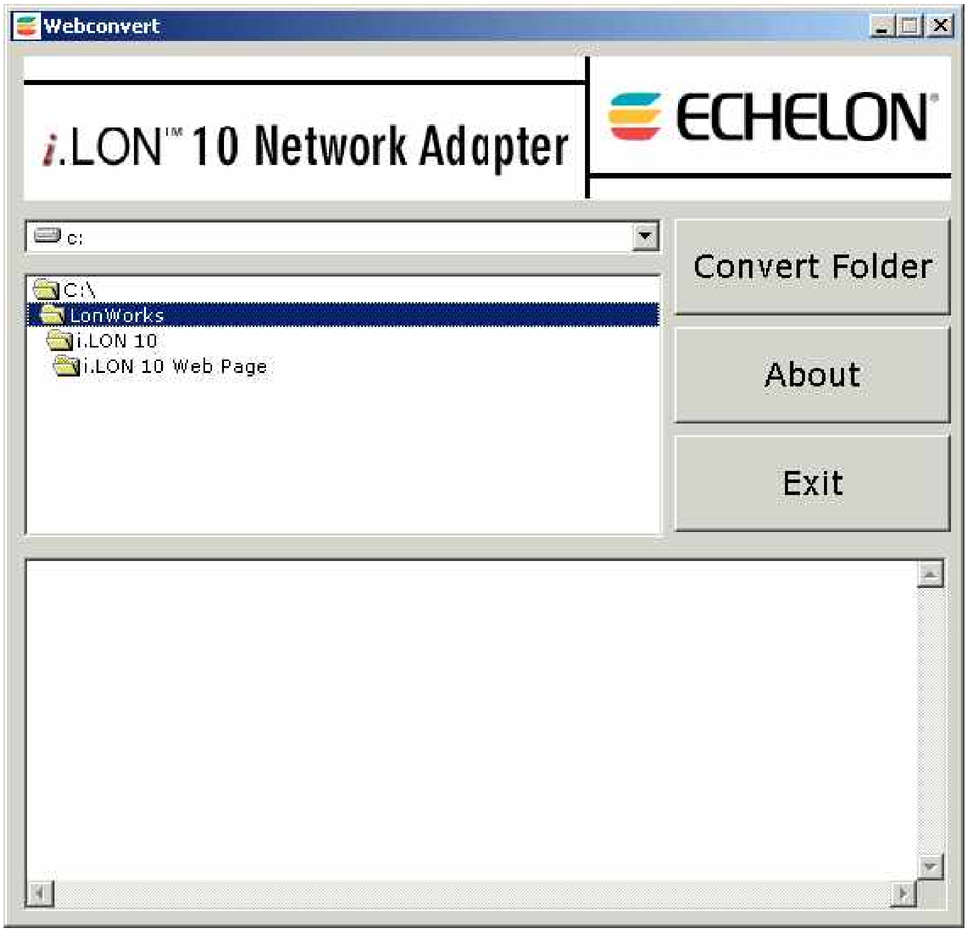
The Webconvert Utility

Webconvert allows the user to select a base directory and location to store the converted file. Webconvert traverses the base directory and all sub-directories. The base directory path is removed from the converted filename or sub-directory (e.g., C:\BaseDir\index.htm becomes index.htm and C:\BaseDir\SubDir\pic1.jpg becomes SubDir/pic1.jpg).

Webconvert handles the following file extensions *.au*, *.jpeg*, *.jpg*, *.gif*, *.htm*, *.html*, *.mov*, *.mp3*, *.mpeg*, *.mpg*, *.png*, *.ps*, *.swf*, *.tif*, *.tiff*, *.zip,* and *.wav* . Webconvert will ignore any *CVS* folders and the following file extensions*.*bak*, *.~, *.*hex*, and *.*cvsignore* . If Webconvert finds a file that is not specified above, it will convert the file using the "plain/text" mime type.

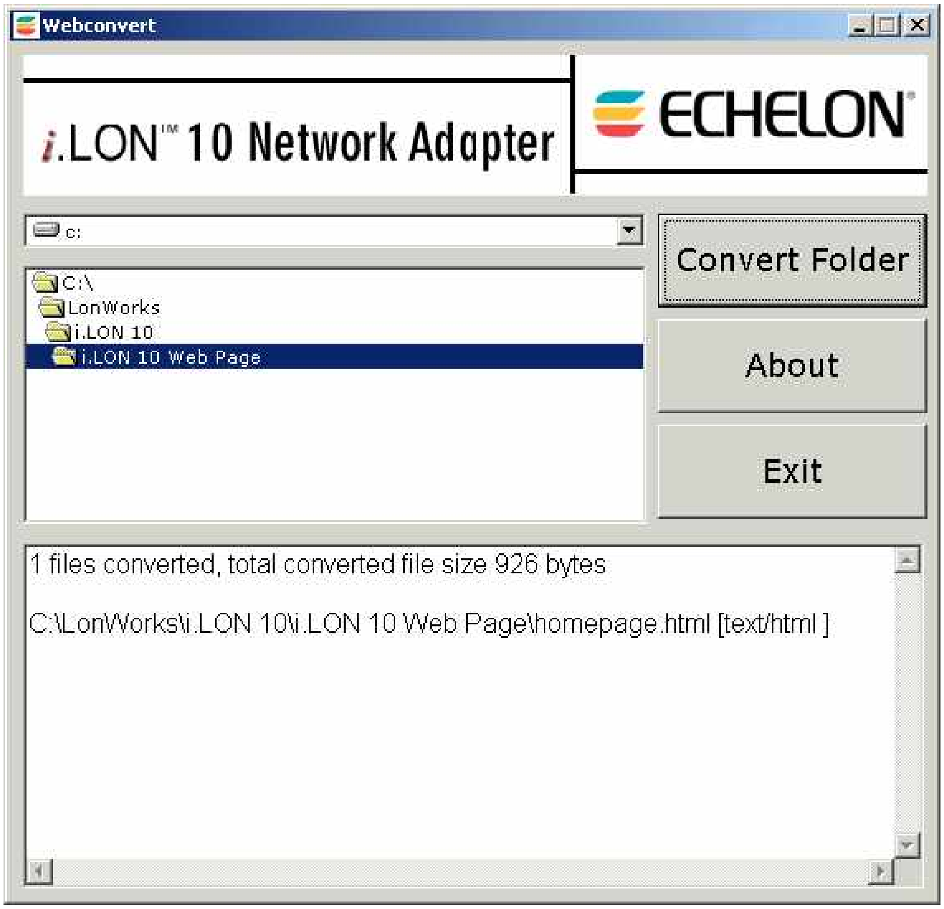
To use the Webconvert utility, follow these steps:

1. Open the i.LON 10 folder on the *i*.LON 10 CD and run `webconvert.exe` (You can also copy this file onto your PC). The Webconvert utility starts, as shown in the following figure:



2. Browse to the folder you want to convert. The folder that will be converted is the last open folder, not the highlighted folder. In the figure above, the `i.LON Web Page` folder would be converted, **not** the `LonWorks` folder.
3. Once you have selected the folder to convert, click **Convert Folder**.
4. A **Save As** dialog will prompt you to choose a location for the converted file.

5. After the conversion has been completed, the log box shows how many files have been converted, the total converted file size, what files have been converted, and any errors that may have occurred (see *Webconvert Utility Log Messages*, below), as shown in the following figure:



1 files converted, total converted file size 926 bytes

C:\LonWorks\i.LON 10\i.LON 10 Web Page\homepage.html [text/html]

6. Once you are finished converting folders, click **Exit** to quit the Webconvert utility.

See *Uploading a User Web Page* in Chapter 6 for information on using a TFTP client to upload a converted Web page to an *i*.LON 10 Ethernet Adapter.

Webconvert Utility Log Messages

The following log messages may appear when attempting to convert a folder:

Message	Explanation
`[`*`type/format`*`]`	The file has successfully been converted. (e.g., *C:\html\index.html [text/html]*)
`[Ignored]`	The file has been ignored because it is not a web file. (e.g., Backup file, Intel Hex File, Executable File.)
`[Folder Ignored]`	The folder has been ignored because it is a backup folder. (e.g., CVS folder)
`No Web Files Found!`	No web files have been found to convert.

`Total Converted Data size is greater than 32 Kb`	The *i*.LON 10 Ethernet Adapter has a maximum size of 32 kB to store web pages. If the size of the files in the folder you selected is greater than 32 kB, this message will appear. The conversion will be cancelled.

Appendix B

The xDriver Software

This appendix describes how to install and configure the xDriver software to allow the *i*.LON 10 Ethernet Adapter to communicate with the LNS Server.

Download and Install the OpenLDV Driver

The OpenLDV driver provides LONWORKS tools and applications with a unified Windows interface for sending and receiving LonTalk messages on your *i*.LON 10 Ethernet Adapter. You can obtain OpenLDV from the download section of the Echelon website at www.echelon.com. Use the OpenLDV ReadMe File, also available at the download site, for an overview of the driver and installation instructions.

NOTE: Uplink connections can only be established using Windows 2000, Windows XP, and Vista.

*Using the **LONWORKS** Interfaces Control Panel Applet*

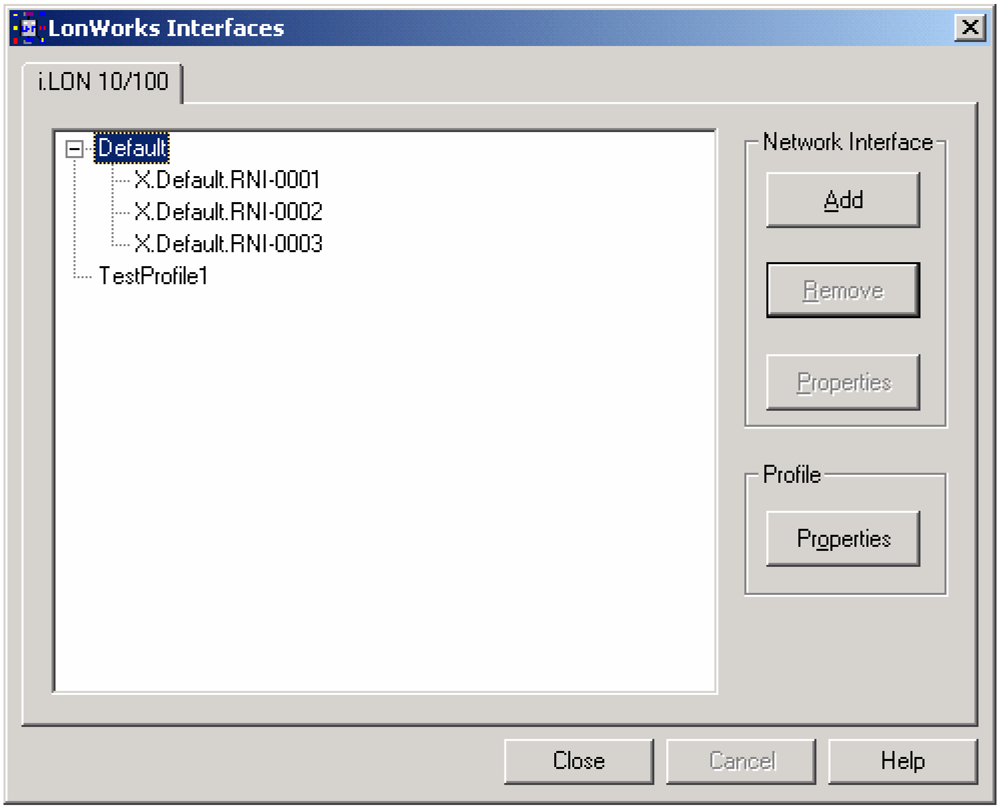
Use the LONWORKS Interfaces Control Panel Applet to create Windows Registry entries that will store the information xDriver will require to connect the LNS server to each of your *i*.LON 10s. A separate entry is required for each *i*.LON 10 you plan to connect to the LNS server with xDriver. The default xDriver will access the appropriate entry each time it initiates a connection to an *i*.LON 10, and extract the information it needs to establish the connection.

If you are managing a large application and will be using more than 50 *i*.LON 10s with xDriver, you should consider using an external database management system to store this information. Please see the *LNS for Windows Programmer's Guide, xDriver Extension* for more information on this.

The following procedure describes how to use the LONWORKS Interfaces Control Panel Applet.

1. Open the Windows Control Panel and double-click the LONWORKS Interfaces icon (LNS). This opens the LONWORKS Interfaces Control Panel Applet.

   NOTE: This is not the same as the LONWORKS/IP Channels control panel applet.

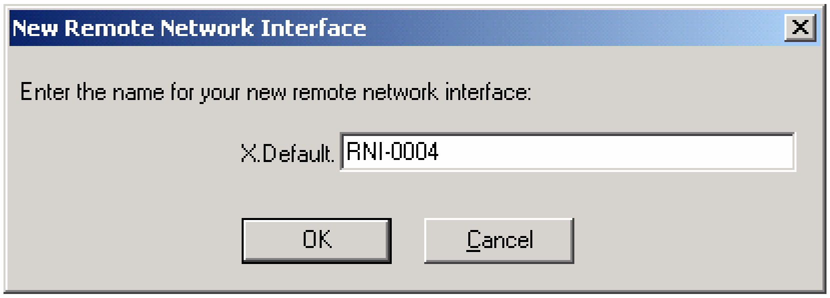


Default
X.Default.RNI-0001
X.Default.RNI-0002
X.Default.RNI-0003
TestProfile1

2. The control panel applet lists the LNS network interface name of all the *i*.LON 10s that have been added to the Registry below the **Default** item. In the figure above three *i*.LON 10s have been added to the Windows Registry.

   Default represents the Default xDriver Profile. This is the set of configuration parameters that determines how the default xDriver will manage connections to your *i*.LON 10s. You can review and edit the configuration of the Default xDriver Profile by clicking **Default**, and then clicking the Profile **Properties** button (see the *LNS Programmer's Guide, xDrvier Extension* for more information..

   Click **Add** to create a Registry entry for a new *i*.LON 10 under the selected profile. This opens the window shown the following figure:



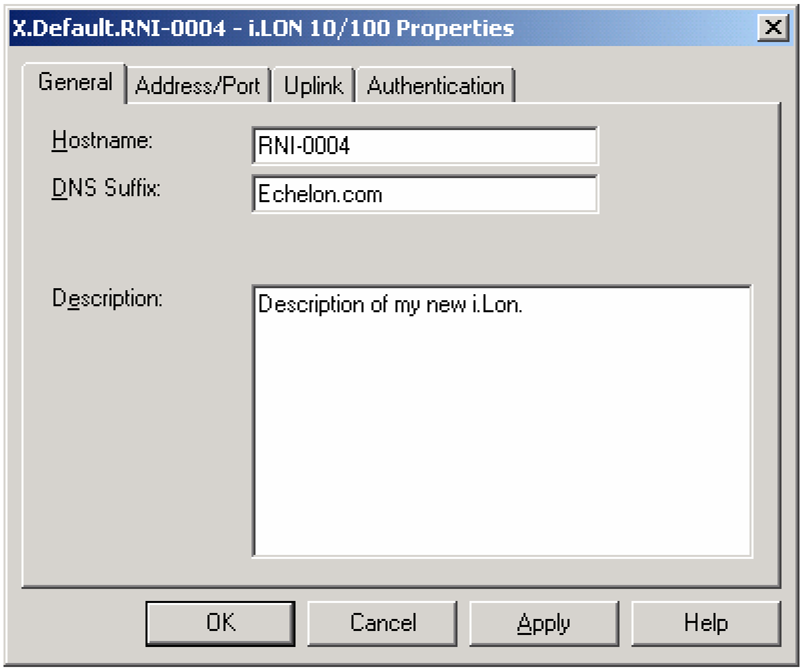
Enter the name for your new remote network interface:

X.Default. RNI-0004

   NOTE: You must be logged in as an Administrative user to create a Registry entry for an *i*.LON 10 if you are using the Windows NT, Windows 2000 or Windows XP platforms.

3. Enter the name for the new *i*.LON 10. This will be used as a lookup key to access the proper Registry entry each time xDriver initiates a connection to this *i*.LON 10. **Each** *i*.LON 10 **must have a unique name.**

4. Click **OK**. This opens the tab shown in the following figure:



Hostname: RNI-0004

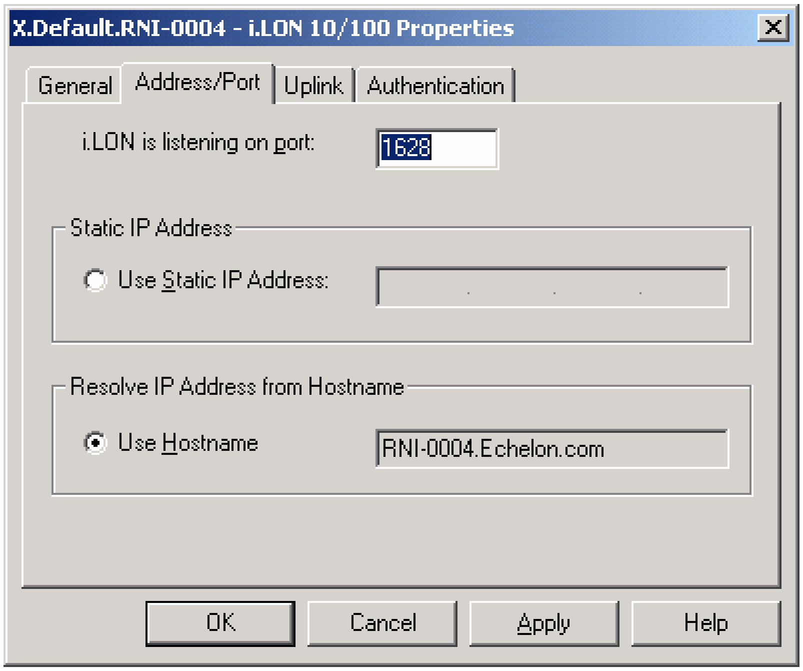
DNS Suffix: Echelon.com

Description: Description of my new i.Lon.

5. Configure the fields on the General tab. The following table describes these fields.

Field	Description
Hostname	**Maximum Length:** 63 chars **Legal Chars:** A-Z, a-z, "-", 0-9 **Comments:** Enter the TCP/IP hostname of the *i*.LON 10. xDriver will use the hostname to connect to the *i*.LON 10.
DNS Suffix	**Maximum Length:** 63 chars **Legal Chars:** A-Z, a-z, "-", 0-9,"." **Comments:** Enter the name of the IP domain on which the *i*.LON 10 is installed.
Description	**Comments:** Optional field. Generally used to describe the site.

6. When you have configured the fields on the General tab, click the **Address/Port** tab. This opens the tab shown in the following figure:



i.LON is listening on port: 1628

Static IP Address

○ Use Static IP Address: . . .

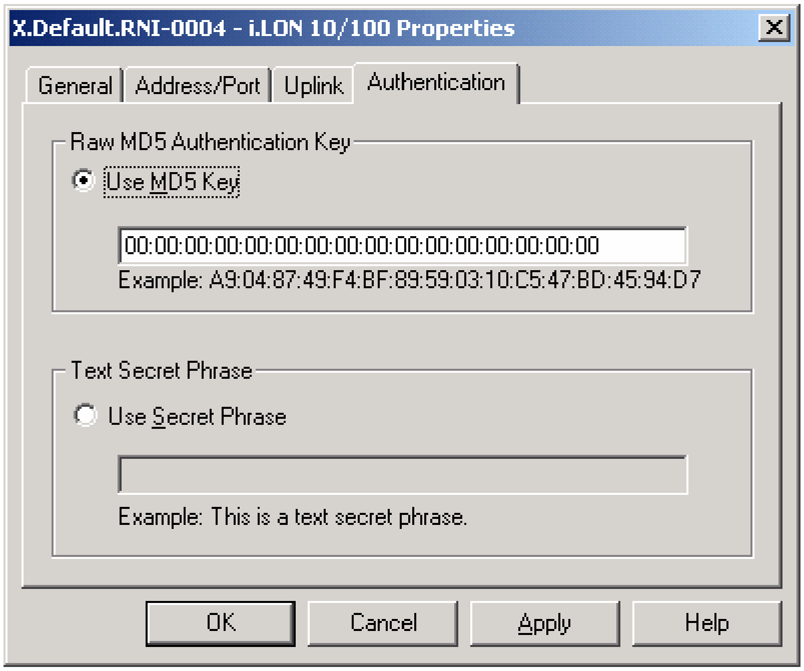
Resolve IP Address from Hostname

● Use Hostname RNI-0004.Echelon.com

7. Configure the fields on the Address/Port tab. The following table describes these fields.

Field	Description
i.Lon is listening on port:	**Default Value:** 1628 **Range:** 1-65,535 **Comments:** Enter the TCP port number the *i*.LON 10 is using to listen for incoming connections from the LNS server.
Use Static IP Address	**Comments:** Click the **Use Static IP Address** button to manually enter the IP address of the *i*.LON 10. You must enter an IP address in the form x.x.x.x, where x is an integer in the range 0-255. You should use this option if your *i*.LON 10's hostname is not configured in any name servers (e.g. DNS servers, HOSTS file).
Use Hostname	**Comments:** Click the **Use Hostname** button to have xDriver resolve the *i*.LON 10's IP address from the hostname and DNS suffix entered in the **General** tab.

When you have configured the fields on the Address/Port tab, click the **Authentication** tab. This opens the tab shown in the following figure :



X.Default.RNI-0004 - i.LON 10/100 Properties

Raw MD5 Authentication Key

● Use MD5 Key

00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00

Example: A9:04:87:49:F4:BF:89:59:03:10:C5:47:BD:45:94:D7

Text Secret Phrase

○ Use Secret Phrase

Example: This is a text secret phrase.

8. You can choose to authenticate connections to this *i*.LON 10 using the MD5 authentication key or the text secret phrase configured into the *i*.LON 10. Using an MD5 authentication key or text secret phrase prevents the LNS Server and the *i*.LON 10 from responding to unauthorized messages during an xDriver session.

   NOTE: This authentication key is not the same as the authentication key used within the LONWORKS network.

   To use the MD5 authentication key, click the **Use MD5 Key** button., and enter the authentication key as a 32-character hexadecimal string representing a 128-bit MD5 key. The 32 characters must be entered in colon-separated pairs. For example:

   A9:04:87:49:F4:BF:89:59:03:10:C5:47:BD:45:94:D7

   This must match the MD5 authentication key configured into the *i*.LON 10. Setting the authentication key to all 0s here will cause xDriver to use the pre-defined, default factory authentication key for the *i*.LON 10. For security reasons, it is not recommended that you use the default authentication key for the *i*.LON 10.

   To use the text secret phrase, click the **Use Secret Phrase** button and enter the text secret phrase. This phrase is a string 16-63 characters long, and must exactly match the text secret phrase used by the *i*.LON 10.

   When you have finished, click **OK** to save the settings for the *i*.LON 10 into the Windows Registry and return to the window shown in Figure 2.1. The new *i*.LON 10 will appear in the list of network interfaces below the **Default** Profile. Or, click **Apply** to save all changes and continue editing the *i*.LON 10's settings.

You can modify an *i*.LON 10's settings later by selecting it from the list of network interfaces, and clicking the Network Interface **Properties** button. You can remove an *i*.LON 10 from the Windows Registry by selecting it from the list, and clicking the Network Interface **Remove** button.