$C \in$

i.Server
MicroServer™

ENGINEERING

http://192.168.1.200

ENGINEERING

Temperature: T1 59.7   T2 31.6   F   Difference: T1 - T2 28.1

100   100

10.0/Div   10.0/Div

0   0

Wed Jan 01 12:...   THERMOCOUPLE   9-12 Vdc   Tue Jan 18 11:00:00 PDT 2006
                                      1   2

i.TCX

Dual Thermocouple Input

ΩE OMEGA®

TABLE OF CONTENTS

LIST OF FIGURES:

LIST OF TABLES:

NOTES, WARNINGS and CAUTIONS

Information that is especially important to note is identified by the following labels:

• **NOTE**
• **WARNING or CAUTION**
• **IMPORTANT**
• **TIP**

Note ☞   **NOTE:** Provides you with information that is important to successfully setup and use the iServer.

⚡   **CAUTION or WARNING:** Tells you about the risk of electrical shock.

⚠   **CAUTION, WARNING or IMPORTANT:** Tells you of circumstances or practices that can effect the instrument's functionality and must refer to accompanying documents.

Tip ☞   **TIP:** Provides you helpful hints.

FEATURES

- **Virtual Chart Recorder**
- **Two Thermocouple Channels**
- **Web Server**
- **Ten Popular Thermocouple Types**
- **Accurate**
- **Password Protection**
- **Email Alarms**
- **Data Logging**
- **No Special Software Required**

PART 1
INTRODUCTION

1.1 Safety and EMC Considerations

Refer to the CE Approval Section

EMC Considerations

- Whenever EMC is an issue, always use shielded cables.
- Never run signal and power wires in the same conduit.
- Use twisted-pair wires for signal connections.
- Install Ferrite Bead(s) on signal wires close to the instrument if EMC problems persist.

Failure to follow all instructions and warnings may result in injury!

1.2 Before You Begin

Inspecting Your Shipment: Remove the packing slip and verify that you have received everything listed. Inspect the container and equipment for signs of damage as soon as you receive the shipment. Note any evidence of rough handling in transit. Immediately report any damage to the shipping agent. The carrier will not honor damage claims unless all shipping material is saved for inspection. After examining and removing the contents, save the packing material and carton in the event reshipment is necessary.

Customer Service: If you need assistance, please contact the Customer Service Department nearest you.

Manuals, Software: The latest Operation Manual as well as free configuration software (iConnect), datalogging software (iLog), and Mail Notifier are available at **the website listed on the cover page of this manual**.

1.3 Description

View Temperature from one or two Thermocouples with a Web Browser. The iServer let's you monitor Temperature from two independent Thermocouple channels over an Ethernet network or the Internet with no special software except a Web Browser. The iServer serves Active Web Pages to display real time readings, temperature charts, or log data in standard data formats for use in a spreadsheet or data acquisition program such as Excel or Visual Basic.

Adjustable Charts. The Java™ Applet chart scales are fully adjustable on the fly. For example, the chart can display one minute, one hour, one day, one week, one month or one year. Temperature can be charted across the full span, or within any narrow range such as 20 to 30°C. You can chart temperature from one thermocouple, two thermocouples, and/or the differential between the two.

The iServer transmitters can take Thermocouple Types J, K, T, E, R, S, B, C, N, and L measuring temperatures up to 1,820°C (3,308°F). The iServer can display and chart absolute measurements in two locations and a differential measurement between the two locations.

Award-winning Technology. The iServer is simple to install and use. It features award-winning technology that requires no special software except a Web Browser. The iServer connects to an Ethernet Network with a standard RJ45 connector and sends data in standard TCP/IP packets. It is easily configured with a simple menu using a Web Browser and can be password protected. From within an Ethernet LAN or over the Internet, the user simply types its IP address or an easy to remember name in any Web Browser, and the iServer serves a Web Page with the current readings.

Email Alarms. All iServer models that are on a LAN that is connected to the Internet can trigger an alarm that can be sent by email to a single user or to a group distribution list, including text messages to cell phones and PDA's.

The following example illustrates how you can hookup an iServer to your network:

A standard web browser can be used to monitor and chart Temperature from two independent Thermocouple channels. The browser can also be used to configure the device's IP address, passwords, and overall configuration parameters. An iLD Big Display can be used with an iServer to display readings over the network.

The following example illustrates how you can hookup an iServer and iLD to your network:
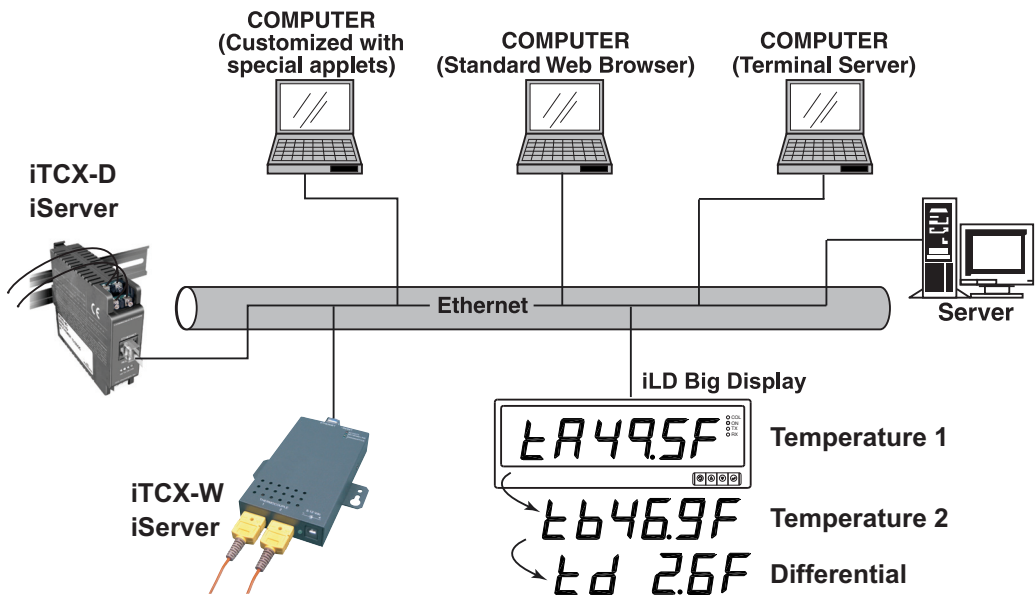
Figure 1.1 iServer sends temperature readings to an iLD Big Display

PART 2   HARDWARE

2.1 Mounting

2.1.1 Mounting the Wall Mount iServer

Note ☞ If unit is to be mounted on a flat surface, you may take the bottom rubber feet off the unit.

Position unit where required. Mark and drill the two #4 screw holes.

After bracket is mounted on the wall, align back of unit over the three bracket clips, once engaged, slide downward, the unit will snap in place.

DRILL 0.125 [3.17]
USE TWO, #4
FLAT HEAD SCREWS
TO MOUNT BRACKET

BRACKET CLIPS (3)

USE #4-40, 3/16"LG SCREW
FOR GROUNDING CASE

2.42 [61.6]
0.52 [13.3]
1.50 [38.1]
1.26 [32.1]
SNAP
4.41 [112.0]

Dimensions are in inches with millimeters in [ ].
0.82 [20.8]
0.10 [2.54]
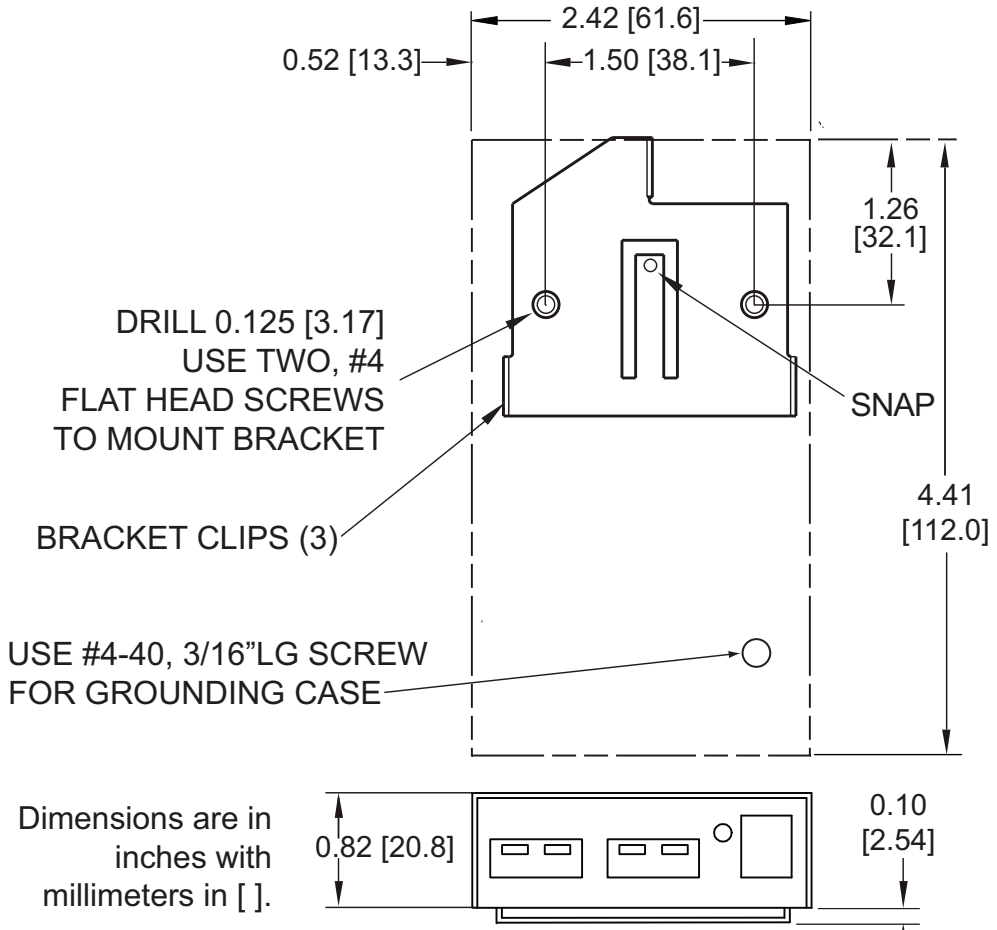
Figure 2.1 Mounting - Wall Mount iServer

Note ☞ It is recommended that you ground your unit by wrapping a wire around a #4-40 screw threaded into the nut located on the case's tray.

2.1.2 Mounting the DIN Rail iServer

To install unit onto DIN Rail:

a) Tilt unit, position mounting slot onto DIN Rail, as shown.
b) Push unit towards DIN Rail and it will snap into place.

1. TILT AND HOOK TO RAIL

35mm RAIL

2. PUSH TO SNAP ON
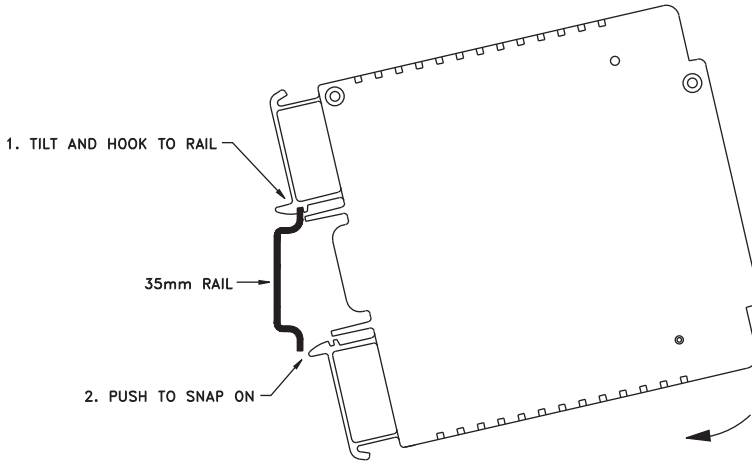
Figure 2.2 Mounting - DIN Rail iServer

2.1.3 Removal from a DIN Rail

a)   Insert flat screw-driver into tab and push downwards.
b)   Unit will detach from DIN Rail.

1. INSERT SCREWDRIVER AT TAB
   PUSH DOWNWARDS.

2. UNIT WILL DETACH
   FROM RAIL

35mm RAIL
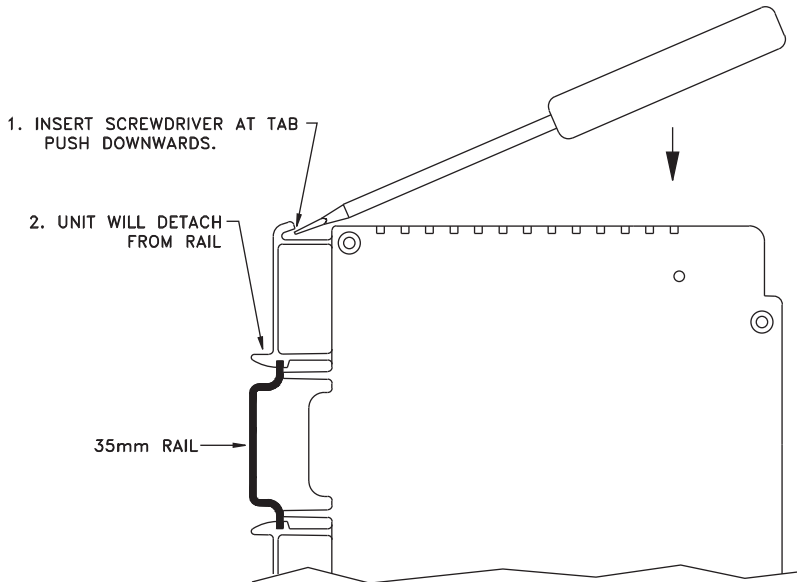
Figure 2.3 Removal - DIN Rail iServer

2.2 DIP Switches
2.2.1 DIP Switch Usage

The iServer is shipped with all DIP switches in **"OFF"** position.

1) N/C - not used
2) To change to default factory settings
3) To enable/disable DHCP
4) N/C - not used

Note ☞ To set the iServer to factory default settings, slide DIP switch **#2** to **ON** position. Power the iServer on and wait about 10 seconds until the iServer fully boots up. Set the DIP switch **#2** back to **OFF** position (it does not matter if the iServer is powered ON or OFF, just make sure that the DIP switch is set to OFF, otherwise, every time the unit is power-cycled the factory settings will take over.

Note ☞ To enable the DHCP, besides using DIP switch **#3**, set the iServer's IP address to **0.0.0.0**. An iServer with IP address of **0.0.0.0** will request an IP address, gateway address, and subnet mask from a DHCP server over the Ethernet.
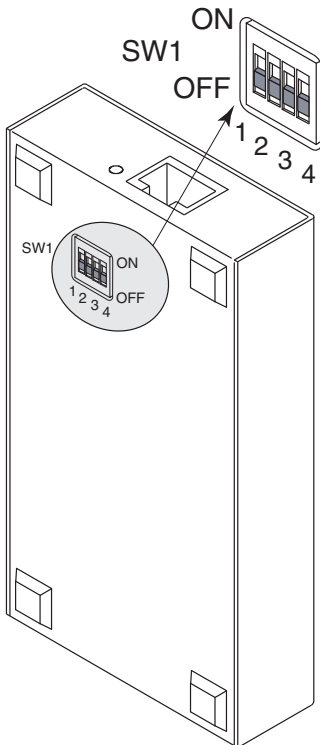
Figure 2.4a DIP Switch
          Wall Mount iServer
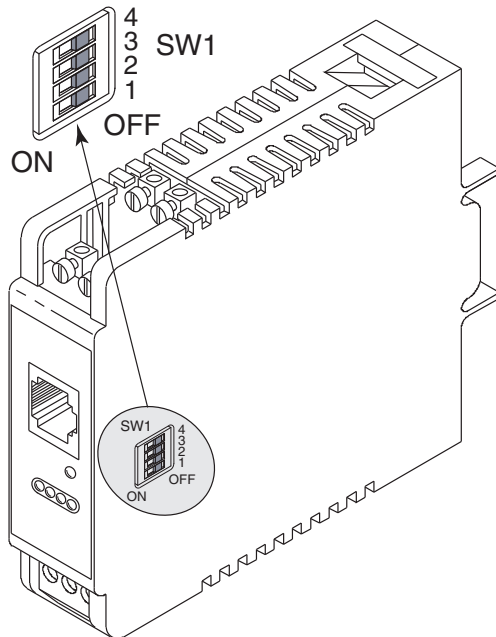
Figure 2.4b DIP Switch
          DIN Rail iServer

2.3 Parts of the iServer Unit
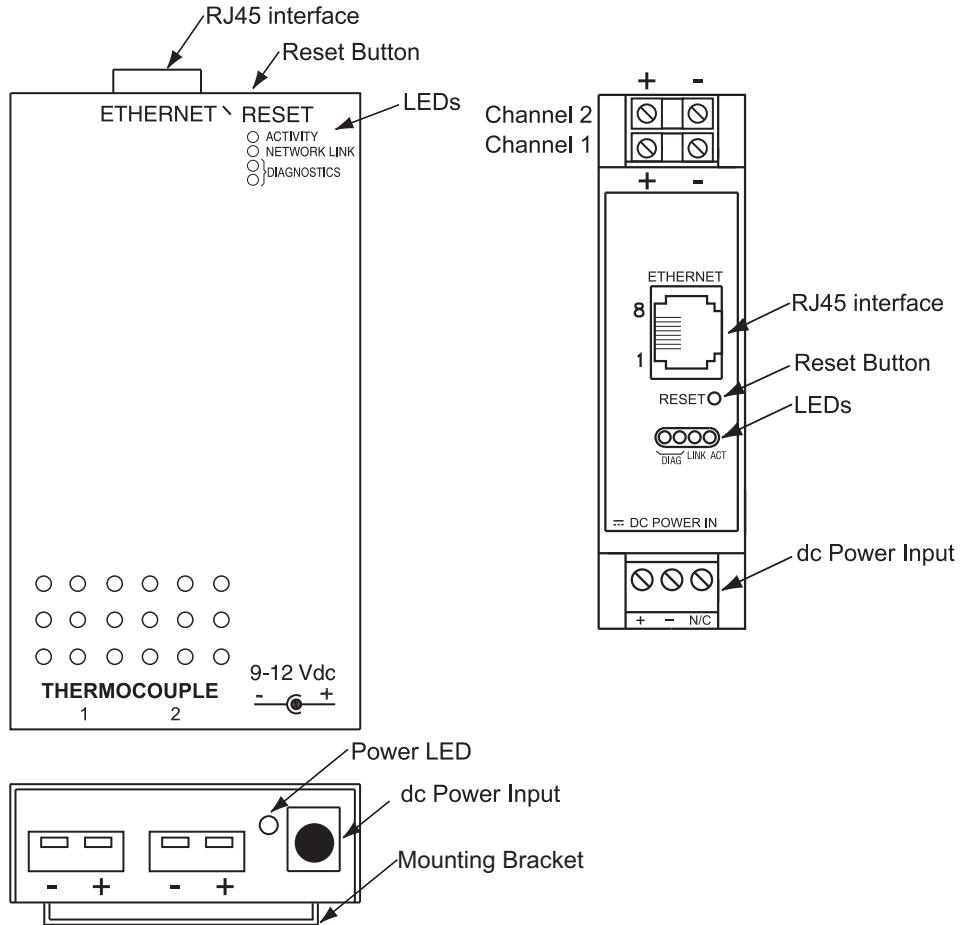
Figure 2.5 Parts of the iServer Unit

Table 2.1 Parts of iServer Unit

SENSOR	Thermocouple Input (supporting up to 2 Thermocouples)
ETHERNET	RJ45 interface for 10BASE-T connection.
RESET	Button: Used for power reseting the iServer.
ACTIVITY	LED (Red) Blinking: Indicates network activities (receiving or sending packets).
NET LINK	LED (Green) Solid: Indicates good network link.
DIAG	LED (Yellow and Green) Diagnostics: at boot-up they light up for 2 seconds, then turn off; DHCP: if DHCP is enabled, they blink and stay solid periodically
POWER	LED (Green) Solid: Indicates Power-ON (for -W version only).
DC Power Supply Section:	
+	Plus power supply wire connection (inside the plug for -W model).
-	Minus power supply wire connection (outside the plug for -W model).

7

2.4 Network Communication Interfaces

2.4.1 10Base-T RJ-45 Pinout

The 10BASE-T Ethernet network (RJ-45) system is used in the iServer for network connectivity. The 10 Mbps twisted-pair Ethernet system operates over two pairs of wires. One pair is used for receiving data signals and the other pair is used for transmitting data signals. This means that four pins of the eight-pin connector are used.

ETHERNET

Pin	Name	Description
1	+Tx	+ Transmit Data
2	-Tx	- Transmit Data
3	+RX	+ Receive Data
4	N/C	Not Connected
5	N/C	Not Connected
6	-Rx	- Receive Data
7	N/C	Not Connected
8	N/C	Not Connected
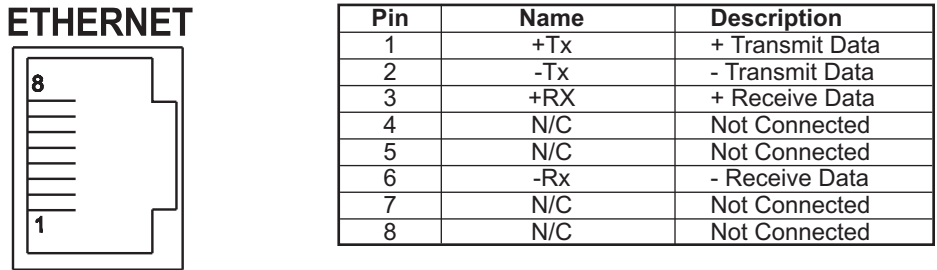
Figure 2.6 RJ45 Pinout

2.4.2 10Base-T Crossover Wiring

When connecting the iServer directly to the computer, the transmit data pins of the computer should be wired to the receive data pins of the iServer, and vice versa. The 10Base-T crossover cable with pin connection assignments are shown below.

Note ☞ Use straight through cable for connecting the iServer to an Ethernet hub. The ports on the hub are already crossed

1	+Tx		+Tx	1
2	-Tx		-Tx	2
3	+Rx		+Rx	3
6	-Rx		-Rx	6
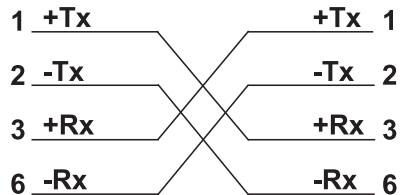
Figure 2.7 10Base-T Crossover Cable Wiring

PART 3
NETWORK CONFIGURATION

3.1 Network Protocols

The iServer can be connected to the network using standard TCP/IP protocols.
It also supports ARP, HTTP (WEB server), DHCP, DNS and Telnet protocols.

3.2 Ethernet (MAC) Address

MAC (Media Access Control) address is your computer's unique hardware number.
When you're connected to the LAN from your computer, a correspondence table relates
your IP address to your computer's physical (MAC) address. The MAC address can be
found on the label of your device and contains 6 bytes (12 characters) of hexadecimal
numbers **XX:XX:XX:XX:XX:XX** hex

For example: 0A:0C:3D:0B:0A:0B

| Note ☞ | Remove the small label with the default IP address and there will be room to put your IP address. See **Figure 3.1** |
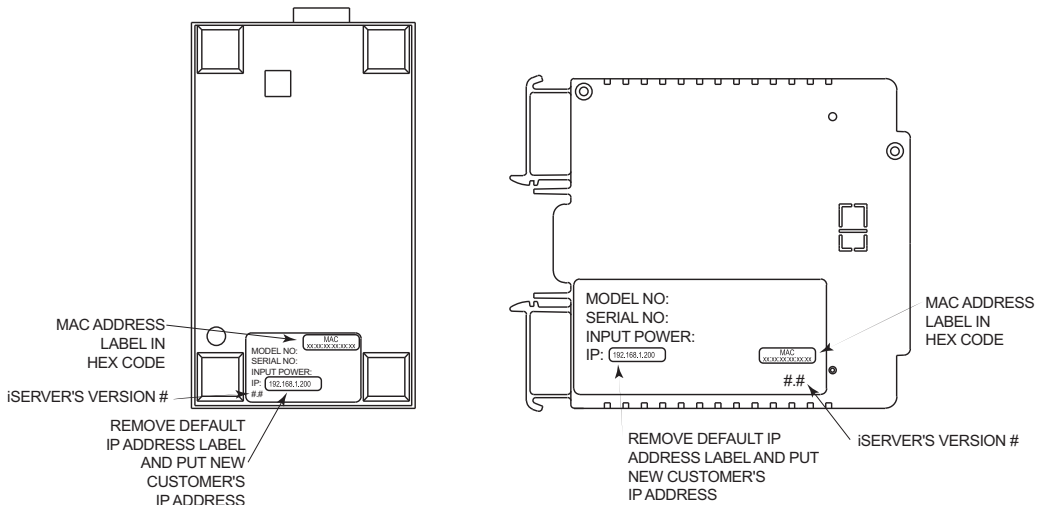
Figure 3.1 Labeling

9

3.3 DHCP

DHCP, Dynamic Host Configuration Protocol enables individual computers or devices to extract their IP configurations from a server (DHCP server). If the DHCP is enabled on your iServer, as soon as the iServer is connected to the network, there is an exchange of information between DHCP server and the iServer. During this process the IP address, the Gateway address, and the Subnet Mask will be assigned to the iServer by the DHCP server. Note that the DHCP server must be configured correctly to do such assignment.

If fixed or static IP address is desired, the DHCP must be disabled. The iServer is shipped with DHCP disabled (factory default). The DHCP can be enabled by setting the DIP switch **# 3** to the **"ON"** position (refer to **Figure 3.2**).

DIP switch # 3 shown in **"ON"** position
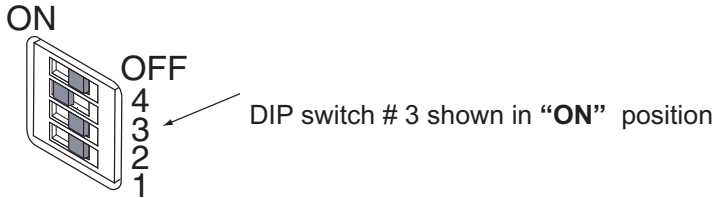
Figure 3.2 DIP Switch on the Bottom Side of iServer

Note ☞   Setting the iServer's IP address to **0.0.0.0** will also enable DHCP.

3.4 DNS

DNS, Domain Name System enables individual computers and devices to be recognized over a network based on a specific name instead of an IP address. For example, instead of having to use ***http://192.168.1.200*** (IP address), you would use only ***http://eis03ec*** or any eight character name stored as Host Name under Access Control menu in the iServer Home Page. The default DNS name for an iServer is **"eis"** followed by the last four digits of the MAC address of that particular iServer.

Note ☞
1. It is very important to communicate with the network administrator in order to understand the DHCP and its existing configurations on the host server, before enabling the DHCP on the iServer.

2. The iServers are shipped with a default static IP address of **192.168.1.200** and Subnet Mask of **255.255.255.0**.

3. On Novell networks or Windows 2000 where the DCHP is an updated function of DNS this feature may be beneficial since a particular name can be assigned eliminating the need for the IP address, as described in **Section 3.4**

3.5 IP Address

Every active device connected to the TCP/IP network must have a unique IP address. This IP address is used to establish a connection to the iServer's sensor. Every computer using TCP/IP should have a unique 32-bit address which is divided into two portions, the network ID and the host ID. For instance, every computer on the same network uses the same network ID. At the same time, all of them have a different host ID. For more details about the IP address see **Appendix B**.

3.5.1 Default IP Address

The iServer is shipped with a default IP address of **192.168.1.200** and Subnet Mask of **255.255.255.0**. If you are going to use a Web browser or Telnet program to access the iServer using its default IP address, make sure that the PC from which you're establishing the connection has an IP address that is in the same range as the iServer's IP address (**192.168.1.x**, where **x** can be any number from 1 to 254).

> **Note** ☞ Your PC's IP address <u>cannot</u> be the same as the iServer's IP address.

You also need to make sure that your PC's Subnet Mask is **255.255.255.0**. This is a good way to access the iServer over the network and make any configuration changes needed. If **192.168.1.200** is already in use on your network, use an Ethernet crossover cable between your computer and the iServer to change the IP address or any other settings within the iServer.

3.6 Port Number

All TCP connections are defined by the IP address and a port number. A port number is an internal address that provides an interface between an application running on your computer and the network through the TCP/IP protocol.

There are three default TCP socket port numbers assigned to the iServer:

1. Port (socket) number 1000 when using HTTPget program (see **Section 4.5**).
2. Port (socket) number 2000 when trying to access the sensor (probe) connected to the port of the iServer to receive ASCII data.
3. Port (socket) number 2002 when trying to access the iServer itself for Power Recycling the iServer remotely. This can be done using Windows standard Telnet application.

Power recycling the iServer can also be done through the iServer's Web Server (see **Section 4.2**).

Telnet stands for Telecommunications Network, it is a protocol that provides a way for users (or clients) to connect to computers (or servers) on a network, whether in the next building or across the world.

Example: C:\>Telnet 192.168.1.200 2002

You will then get the following screen.

Figure 3.3 Telnet Login into the iServer

You can open a Telnet session using other terminal emulation programs like Tera Term Pro (downloadable from the internet), which is a free software for MS-Windows. It supports VT100 emulation, Telnet connection and serial com port connections.

PART 4

OPERATIONS

This iServer can be used and configured in several ways, depending on user's preference and network setup. It can be configured using a Web browser, like Netscape or Internet Explorer. It can also be configured using the iConnect Configuration Software.
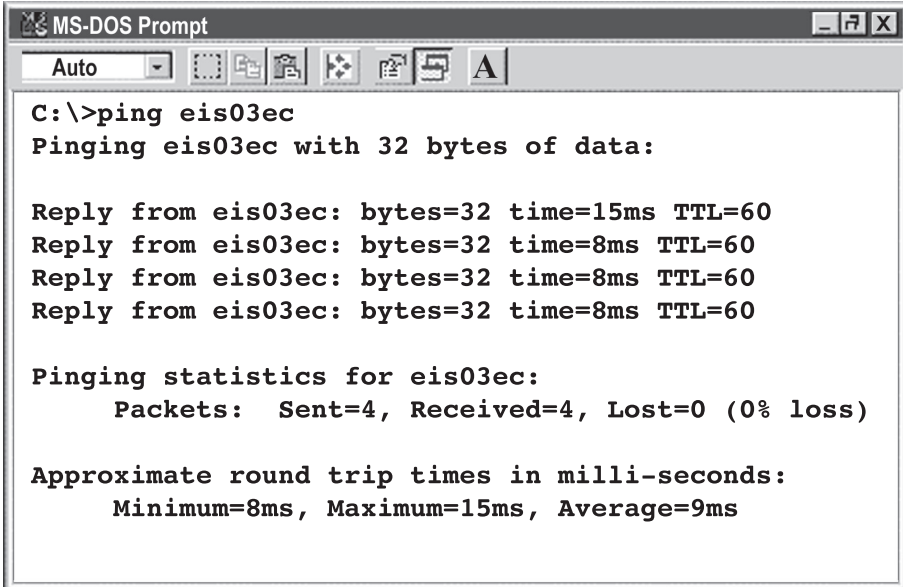
If DHCP and DNS servers are used, the connection is very simple, no need to find the right IP address, or watch for network conflicts, these are all done for you by your network DHCP and DNS server. All that is left for you to do, is to enable DHCP on the iServer (see **Section 2.2**) and use a straight network cable to connect the iServer to a hub and power it up.

If DHCP is not the preferred method, you can configure your PC's network connection with an IP address of **192.168.1.x** that is in the same range as the iServer's default IP address (**192.168.1.200**) and connect to the iServer using a cross-over network cable between your PC's network port and the iServer. After you're done with configuring the iServer, you can always set your PC back to its original settings.

On your computer, from the MS-DOS Prompt window type "**ping 192.168.1.200**" and press Enter. If DHCP and DNS servers are used type **"ping eisxxxx"**, where xxxx are the last four digits of the iServer's MAC address, located on the back of the device. You should get a reply as shown in **Figure 4.1**.

▼ Note ☞ You can use the host name (**eisxxxx**) instead of its IP address only if your DHCP server is configured to communicate with your DNS. Please consult with your IT department for details.

4.0 Testing the Connection

```
MS-DOS Prompt                                        _ ☐ ☒
 Auto  ▾  ▢ ⓑ 🔍 ▷ 🖻 🗗 A

C:\>ping eis03ec
Pinging eis03ec with 32 bytes of data:

Reply from eis03ec: bytes=32 time=15ms TTL=60
Reply from eis03ec: bytes=32 time=8ms TTL=60
Reply from eis03ec: bytes=32 time=8ms TTL=60
Reply from eis03ec: bytes=32 time=8ms TTL=60

Pinging statistics for eis03ec:
     Packets:  Sent=4, Received=4, Lost=0 (0% loss)

Approximate round trip times in milli-seconds:
     Minimum=8ms, Maximum=15ms, Average=9ms
```

Figure 4.1 Pinging the iServer from MS-DOS Prompt

This proves that the connection is proper and you can get into configuration or run mode using the Telnet or Web browser.

4.1 iConnect Software

The iServer may also be assigned an IP Address by using the iConnect software.

a)   Download the iConnect software from the website listed in this manual.

b)   Install iConnect software on a networked PC. This software is compatible with Windows 95, 98, NT, 2000, and XP.

c)   Use iConnect to assign an IP address to the iServer and access its web pages for configuration. You can also use any standard web browser to access the iServer web pages. Consult with your IT department for obtaining an IP address.
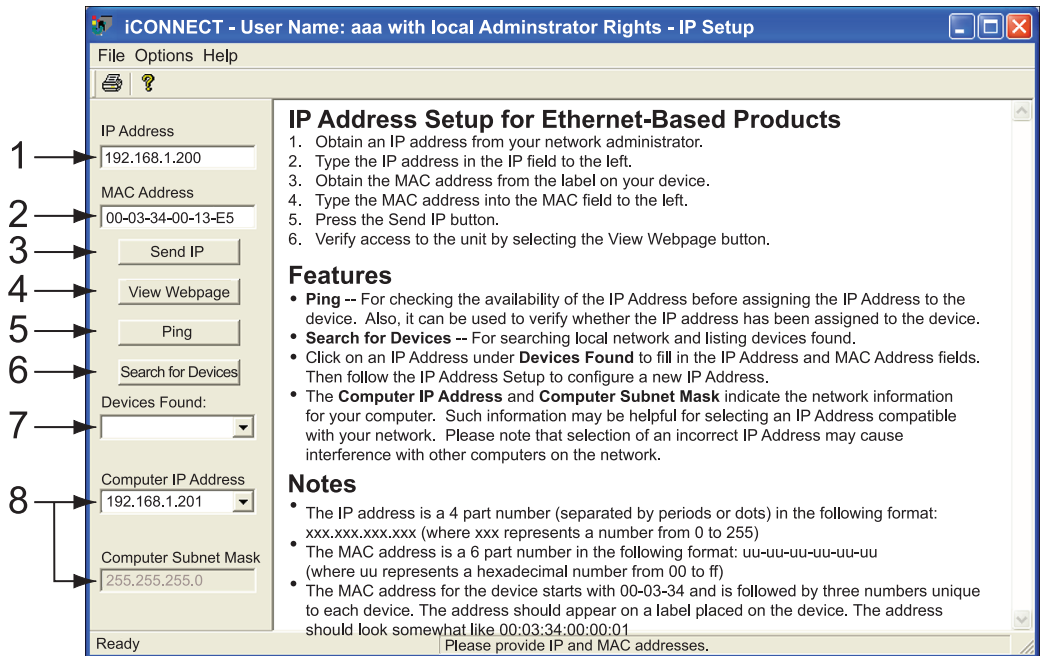
Figure 4.2 Assigning an IP Address using iConnect

1)   Place the IP address in this box.

2)   Take the MAC address from the label attached to the bottom of the iServer and place it in this box.

3)   Click here to send the above IP address to the iServer.

4)   After the IP address is assigned to the iServer, click here to access it's web pages.

5)   Click here to Ping the iServer whose IP address is shown in the IP address box.

6)   Click here to find all the iServer's on your network .

7)   The IP addresses for the iServer's found by the iConnect will be listed here.

8)   These fields indicate the IP address and the subnet mask of the PC on which the iConnect is running.

4.1 iConnect Software (continued)
d)   To access the iServer for Configuration:

Click on the "View Webpage" button, you will access the iServer's home page, refer to **Section 4.3** for details.
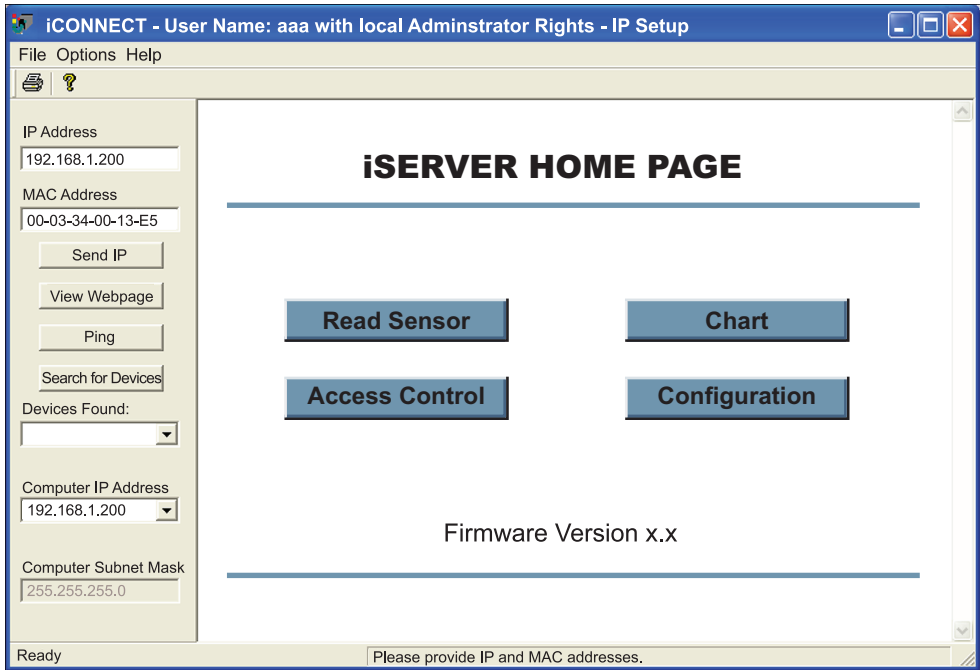
Figure 4.3 Accessing the iServer's Home Page Menu

4.2 Setting a New IP Address over the Network

Besides using the iConnect software, you may use the iServer's default IP address to access it and assign a new IP address to it.

The iServer is shipped with a default IP address of **192.168.1.200** and Subnet Mask of **255.255.255.0**. You can configure your PC's Network connection with an IP address that is in the same range as the iServer's IP address (**192.168.1.x**) and connect to the iServer using a crossover network cable between your PC and the iServer.

With this completed, you can go to the DOS-Prompt and ping **192.168.1.200**. If you receive responses back (**Figure 4.1**), you can go to the Web browser and type in **_http://192.168.1.200_** and it will take you to the iServer's Home Page.

Select ⌐Access Control⌐, button, you'll be asked for the password. First default LOGIN password is "**12345678**" and the ADMINISTRATOR password is "**00000000**", then you should be on the Access Control page were you can simply type in the desired Static IP address, and click Save.

For more details about the "Access Control" page refer to **Section 4.3.5.**
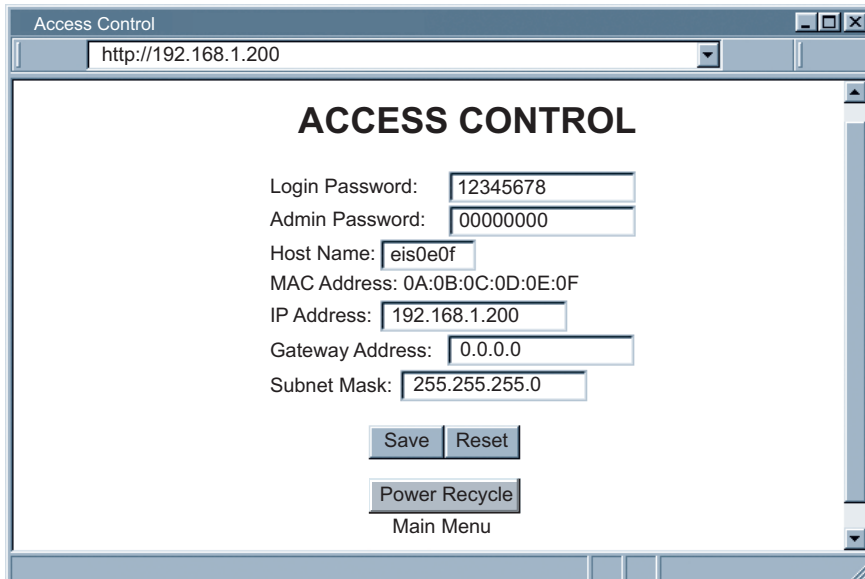
Figure 4.4 Access Control

For the IP address to take effect, the iServer needs to be turned OFF/ON.

Clicking the "Power Recycle" button will turn the iServer OFF and ON.

Pressing the physical button marked "RESET" on the iServer does the same thing.

You can now connect the iServer to an Ethernet hub using a straight through cable, power it up, and follow the ping routine mentioned in the previous section.

4.3 Setup and Operation Using a Web Browser
• Start your web browser.
• From the browser you type ***http://eisxxxx*** using the last four-digits from the MAC
 address label located on the device if DHCP and DNS are used. If a static IP address
 is used, then simply type ***http://x.x.x.x***, where ***x.x.x.x*** is the iServer's IP address.
• The Home Page, shown below, will be displayed.
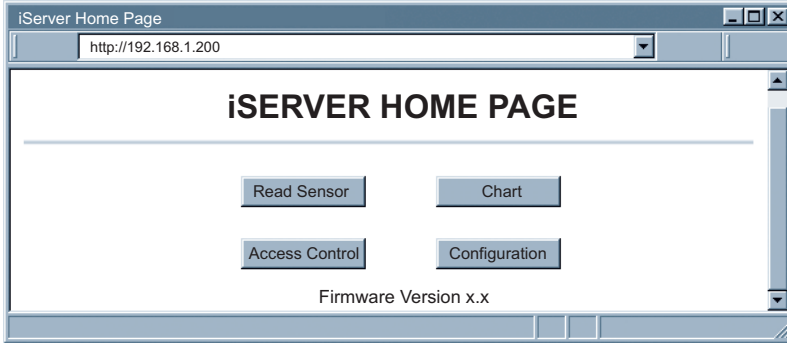
Figure 4.5 iServer Home Page Menu

Note ☞ In order to access certain menu items of the Home Page, users may be
 prompted for a password, as shown in **Figure 4.6**.
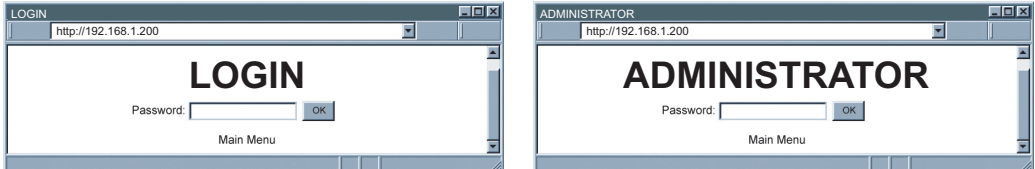
Figure 4.6 LOGIN and ADMINISTRATOR Passwords

There are 2 different access levels:

1. ADMINISTRATOR Password (administrator) allows certain groups and individual users to
 access and modify "entire" iServer parameters without any restrictions.

 The default password is **00000000**. This password can be up to 16 alphanumeric case-
 sensitive characters.

2. LOGIN Password (operator) allows users to access and modify all of the iServer's
parameters, except "Access Control" which requires an Administrator password. The
"Read Sensor" does not require a password.

 The default password is **12345678**. This password can be up to 16 alphanumeric
 case-sensitive characters.

4.3.1 Read Sensor

• Click on [Read Sensor]. In a few seconds the following page (**Figure 4.7**) will appear with all default values of 100.00. Then the actual readings for both temperature sensors and differential value will be displayed. If either thermocouple sensor is disconnected from the iServer unit the "Read Sensor" and "Chart" pages will display "OPEN" and the "Differential" value will be displayed as "N/A".

• This page automatically updates the temperature and differential values.

• Click on Main Menu to return to Home Page.

[Note ☞] While accessing the Read Sensor page, If a blank screen appears without any "java application running" or image of a "Java logo", please verify you have the latest Java Runtime Environment installed and configured according to the following instructions. If you do not have Java Runtime Environment, you may download it from our website or contact the Customer Service Department nearest you.
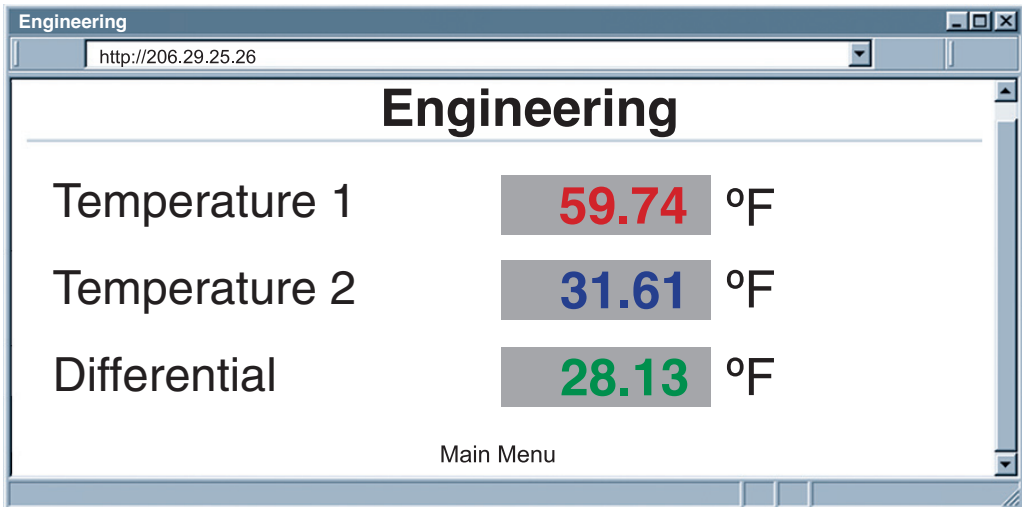
Figure 4.7 Read Sensor

4.3.1.1 Java Runtime Environment Setup

If your computer does not have Java installed, please download from java.sun.com. You can change the Java setting by clicking its icon in Control Panel. To load the applet, you have to enable the web browser and disable cache.

4.3.1.2 Java Runtime Environment 1.7 Setup instructions

    1. Go to your computer's Control Panel. Open the Java Plug-in
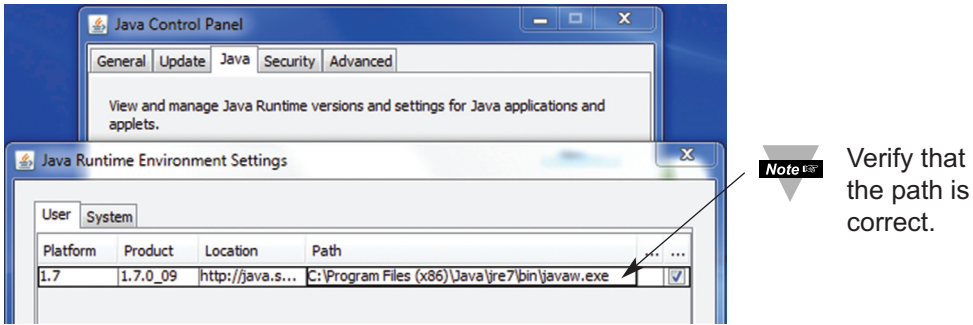
Figure 4.8 Java 1.7 Screen Shot

4.3.1.3   Browser Proxy Selection

Accessing iServer units within your internal network

- Usually when the computer and iServer are on an internal network, you will not use Proxy server access.
- You should un-check the "Use Browser Settings" option on the "Proxy" tab.

Accessing iServer units using the internet

- Often the web browser will use Proxy server access to the internet. In such cases, the default Java runtime settings on the "Proxy" tab should suffice. The default setting is the "Use Browser Settings" option.
- If the default proxy setting doesn't work, then you may have a situation where the proxy settings of the web browser are incorrect.

Diagnostics:

If the web page of the iServer appears, then the HTTP Proxy is working fine.

If the data isn't updated on the iServer upon selecting the Read Sensor web page, there may be a problem with access through a winsock proxy server. In such cases your network administrator will need to provide the winsock proxy server and port #s. (If the administrator requires knowledge of the port # required on the iServer, the value is 2003).

These values should be entered into the Socks line on the "Proxy" tab (of the Java Plugin control panel) or into the "connections" tab on the View,Internet Options dialog and make sure that the Proxy tab shows that the "Use Browser Settings" option is not selected (i.e. when you specify proxy connections in the Java Plugin control panel.

Accessing iServer units over Peer-to-Peer network

A simple peer-to-peer network is setup by disconnecting from the main network (as users will often do when trying to do initial setup of the iServer) and then connecting the iServer to another computer using a ethernet hub, an ethernet switch, or a Cross-over cable connection.

Often when using a peer-to-peer network, the Java plugin and the web browser (such as Internet Explorer) have internet connections configured to connect through proxy servers. In such case, you will need to simply assign the final IP address on this peer to peer network and then view the iServer charts after connecting the iServer into the regular network. Otherwise you can disable the Java plug-in's "Use Browser Settings" temporarily and then reconfigure the Java plug-in settings for regular network access after testing the iServer chart access on your peer-to-peer network.

The "Use Browser Settings" should not be selected. And the HTTP and Socks proxy entries should be blank. Also, setup the internet browser so that proxy servers are disabled.

4.3.2 Chart

- Click on ⌊Chart⌋, the following page (**Figure 4.8**) should appear. The Java™ Applet graph displays temperatures and the differential values, which can be charted across the full span or within any narrow range (such as 20 to 30ºC). The time-base can display one minute, one hour, one day, one week, one month or one year.

Note ☞   If a blank screen appears without any "java application running" or image of a "Java logo", please verify you have the latest Java Runtime Environment installed and configured according to the instructions (refer to **Section 4.3.1.1**). If you do not have Java Runtime Environment, you may download it from our website or contact the Customer Service Department nearest you.


Figure 4.9 Chart

19
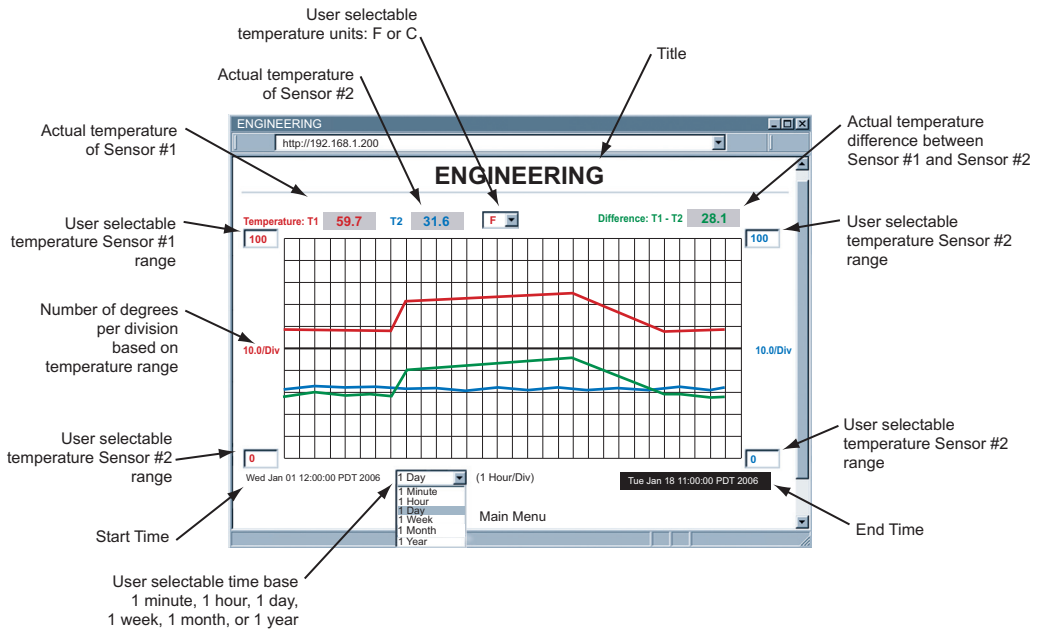
4.3.3 Configuration

• Click on Configuration , the following page should appear.

Figure 4.10 Configuration

Below are the definitions of terms used in the Configuration Page.

A) **Sensor No.:** Clicking on the No. **1** or **2** allows you to modify the Sensor Parameters (See **Section 4.3.4** for more details).

   Secured Applet: If checked, the LOGIN password is required to open "Read Sensor" and "Chart" pages.

   Title: editable field which is the page title on the "Read Sensor" and "Chart" pages.

4.3.3 Configuration (continued)

B) Terminal Server

TCP/UDP*: The iServer supports *TCP* and *UDP* protocols (default is TCP). If UDP is selected, it can be configured either for Broadcast UDP or Directed UDP.

In case of Broadcast UDP, the iServer will transmit the data to every node on the network. This can be accomplished if the Remote IP Address is set to 255.255.255.255.

The Broadcast UDP is a practical solution when one iServer needs to communicate with multiple nodes over the network.

In the case of directed UDP, the iServer will transmit the data to a specific node on the network. This can be accomplished if the Remote IP Address is set to the IP address of that specific node.

Server Type: *Continuous* mode sends the temperature and differential values to the Ethernet every two seconds. It is mainly used to send readings to a remote display or logger.

Command mode needs a command to query the iServer to send the reponse back to querying device.

Number of Connections: The range is from *0 to 5*.

If *0* is selected, the Terminal Server feature is disabled. This means that no network connection can be made to the sensors.

If *1* is selected, only one network connection can be made to the iServer's sensors.

Any number higher than 1 would allow that number of network hosts to read from the iServer simultaneously (default is *5*).

Port: (default 2000) is the default TCP port for the port to which the sensors are connected. Ports 100 (used for HTTPget, refer to **Section 4.5**) , 2002, 2003, and 2004 are reserved for internal use.

> **Note☞** Terminal Server usually describes a device that exchanges data between Ethernet/TCPIP networks and RS232/RS485 systems.   With this iServer, the data is obtained digitally from the sensors and can be accessed from anywhere on the network (irrelevant to RS232 or RS485 interface).
>
> A computer program, such as NEWPORT's Mail Notifier, OPC Server, iLog or HTTPget can send TCP requests and obtain readings using the Terminal Server feature.

C) Remote Access

Remote IP Address: iServer can establish a connection to a remote device (e.g. an iLD Remote Display with an Ethernet iServer embedded board).

Remote Port: (default 2000) the port number for the remote device to which the data is sent (e.g. an iLD Display).

Remote Access:** Remote Access can be enabled and disabled. If enabled, the iServer can send its data to a remote node on the same network (the "Remote IP address" and "Remote Port" must be entered).

> **Note☞** *TCP/UDP: when UDP mode is selected, Remote Access should be disabled and Remote IP and Port are the UDP remote listening IP and Port. If the Remote IP is set to 255.255.255.255, the UDP packet becomes a broadcasting packet which will allow any device listening to the Remote port to receive the packet.
>
> **If Remote Access is enabled, Terminal Server is automatically disabled.

4.3.4 Sensor Parameter

- In the first column of Configuration's page, click on **1** to view and modify Sensor Parameters. See **Figure 4.9**.

Note ☞ You may type any ASCII characters in the text boxes, but you must delete the leading spaces.

Figure 4.11 Sensor Parameters

Below are some definitions of terms used in the Sensor Parameter page.

Sensor Name: a text field shown on the "Read Sensor" page.

TC Type: a list of thermocouple types to select from *J, K, T, E, R, S, B, C, N,* and *L (J Din)*

Temperature Units: unit of temperature in °F or °C shown on the "Read Sensor" page.

Sampling Rate: the number of readings per second. The options are: *2, 4, 8,* and *12*; if the higher sampling rate is selected, you'll have a lower accuracy.

4.3.4 Sensor Parameters (continued)

Remote Display Format: Is used for Terminal Server continuous mode. This determines the data format sent by the iServer to a remote network node (e.g. iLD Display)

Example: If Channel 1 shows temperature of **71.34°F**, the **TA71.34F** will be seen on the remote display. If no format is specified (blank), there is no reading sent out. If temperature is **75.7** and **T00.0F** is used in temperature setting, the remote site will show **T75.7F**.

This format setup was originally made for the iLD Display, which has four or six LEDs. For six LEDs, **T00.00F** format, and for four LEDs, **00.0F** format are appropriate.

Remote End Char: The default value is 0D (Hex representation of <CR>). This means that the iServer sends <CR> after each temperature value. This will be done in Continuous mode.

This is how the data will appear on the host with 0D assigned:

TA71.34F

TA72.48F

TD-1.19F

If the end character, for instance, is 20 (Hex representation of space), the data will then appear as:

TA71.34FTA72.48FTD-1.19F

If nothing is set for the "Remote End Char" field, the iServer will then forward the data to the LAN with no characters followed.

```
Tera Term - 206.29.25.27 VT          _ □ ×
File  Edit  Setup  Control  Window  Help
TA71.34F
TB72.5F
TD-1.14F
TA71.33F
TB72.48F
TD-1.17F
TA71.34F
TB72.5F
TD-1.14F
TA71.34F
TB72.48F
TD-1.17F
TA71.34F
```

Figure 4.12
Remote End Char

Offset: Since the sensing probe is solid state electronics, there is no need for calibration. If it's determined that the readings are slightly off, the user can manually assign numerical values to adjust the readings for temperature values. The unit must be in degree C. The Offset value can either be a positive or negative number

Cold Junction: The options are *Disable* and *Comp_1* for sensor 1 and *Comp_2* for sensor 2. Selecting Comp_1 or Comp_2 will allow you to adjust (calibrate) that sensor in reference to 0°C environment. Cold Junction Compensation is done for type K thermocouple for both sensors before the product is shipped. If a different type of thermocouple is used, we strongly recommend to perform Cold Junction Compensation on that sensor.

Input 2: The options are *Enable* and *Disable* for the second thermocouple sensor only. If it is disabled the thermocouple #2 and the "Differential" value will be shown as "N/A" on the "Read Sensor" and "Chart" pages.

▼
Note ☞   If the second thermocouple channel is not used, it is strongly recommended to disable "Input 2", for faster operation.

4.3.5 Access Control

This section describes the "Access Control" page of the iServers's Web interface. This page allows the users to set up the network and security parameters of the iServer.

At the initial entrance to the "Access Control" page you will be prompted for the LOGIN Password (see **Figure 4.6**) prior to an ADMINISTRATOR Password.

4.3.5 Access Control (continued)

Figure 4.13 Access Control

Login Password: This allows users to access and modify all of the iServer Home Page menu items, except "Access Control", which requires an Administrator password. The default Login password is **12345678**. This password can be up to 16 alpha-numeric case-sensitive characters.

If there is no Login Password assigned (blank box) the iServer will not require a password to access and modify iServer Home page menu items.

Admin (administrator) Password: This allows users to access and modify the "Access Control" page. The default password is **00000000**. This password can be up to 16 alpha-numeric case-sensitive characters.

If there is no Administrator Password assigned (blank box) the iServer will not require password to access and modify "Access Control" page.

Host Name: Refer to **Section 3.4**, DNS.

MAC Address: This is also called Hardware address or Ethernet address, which is assigned to the iServer at production. The MAC (Media Access Control) address is the iServer's unique hardware number and is not changeable.

IP Address: The IP (Internet Protocol) address is a 32-bit number that identifies each sender or receiver of information that is sent in packets across the Ethernet or the Internet. The iServer's default IP address is **192.168.1.200**. The iServer's IP address should be changed to fit user's networking environment. Consult with your IT department for obtaining an IP address.

> Note ☞
>
> The DHCP will be enabled in the iServer if its IP address is set to **0.0.0.0**.
>
> The DHCP can also be enabled by setting the DIP switch **# 3** to **ON** position.

4.3.5 Configure Access Control (continued)

Gateway Address: A gateway is a network point that acts as an entrance to another network. A gateway is often associated with a router, which knows where to direct a given packet of data that arrives at the gateway. If the iServer is sending packets to another network node that is not on the same network on which the iServer is connected, a gateway address needs to be given to the iServer. The gateway address should be the IP address of the router connected to the same LAN to which the iServer is connected. The iServer's default gateway address is **0.0.0.0**.

Consult with your IT department for obtaining a gateway address.

Subnet Mask: It's a 32-bit number that is used to determine which part of the IP address is the network portion and which part is the host portion. The iServer's default subnet mask is **255.255.255.0**.

Consult with your IT department for obtaining a subnet mask.

Note ☞ Changes made in the iServer's Access Control page can be saved permanently by pressing the **Save** button *and* Power Recycling the iServer (press Power Recycle button).

Pressing the **Reset** button will set all the fields back to their default values.

4.4 Telnet Setup

In the Configuration page, set the Number of Connections (Sockets) to 1 - 5 other than 0, and use a telnet simulation program to connect to the iServer (using Port 2000). In *continuous* mode, the telnet teminal will receive continuous data from the iServer. In *command* mode, the command can be sent to query the iServer and get a response back. Refer to **Figure 3.3.**

4.5 HTTPget Program

The HTTPget software is used to send a single HTTP or TCP request to an iServer product.   In contrast, the telnet or Hyperterminal programs allow a continuous connection with multiple requests to be sent to the iServer product.

Generally HTTPget is used for simply programming an IP address to the iServer or for quickly obtaining a reading of from a device.

The iServer product must be configured from the configuration web page so that the "Server Type" value is set to "Command" (This is positioned under the heading of Terminal Server). Also the "Number of Connections" may need to be set to "0" to enable Port 1000 (Port 1000 is for access in a non-standard terminal mode).   To use Port 2000 access (where "2000" is the value stored in "Port"), the Number of Connections should be set to "2" for general usage.   The value of 2 can later be changed to a value from 1 to 5 depending on needs for secure access or fault tolerance.

Whenever Terminal Server service (using Port 2000 by default) is required, the # of connections must be set to a value from 1 to 5. The Terminal Server mode is the recommended mode for the most reliable connection when operating with NEWPORT software or with other programs supporting TCPIP communications. The Port 1000 access can be used with NEWPORT software and may be needed with some iServer products when you need to view readings from the web page while simultaneously collecting data through TCPIP communications.

4.5.1 HTTPget using Port 1000

You can setup and read the information from the iServer by using the HTTPget program. The following program can be used to read data from the iServer by using TCP port **1000**. The command string is sent to this TCP port, then the response can be read back from the same socket.

The HTTPget.exe file is used to setup and read information from the iServer. This file will be automatically installed when you install the MailNotifier software available on our website and CD.

Note ☞ In order to use port 1000, in the Configuration page of the iServer you must set "Number of Connections" to 0. In this case the port number will change to 1000 regardless of what the port number already is.

Notes on using **HTTPget** :

The HTTPget.exe program is installed to the windows directory (usually c:\winnt or c:\windows) when installing the Mail Notifier software.

1. Open up a command window (or have a DOS window)

    a) Click on start menu

    b) Click on "Run"

    c) In the dialog box that appears, type "cmd" or "command" and click on "OK" button.

    d) A command window should now appear.

2. If you now type "httpget" and press the "enter" key, the program options should be displayed.

3. Next run HTTPget with the options displayed below

    ## httpget -r -S "*SRTF\r" 192.168.1.200:1000

where:

-r –S   are parameters needed for the command string

"*SRTF" is the reading command of Channel 1:

*SRTC   Read the temperature in °C - Channel 1

*SRTF   Read the temperature in °F - Channel 1

*SRHF   Read the temperature in °F - Channel 2

*SRHC   Read the temperature in °C - Channel 2

*SRDF   Read the differential in °F

*SRDC   Read the differential in °C

\r   is the carriage return termination character

192.168.1.200   is an IP address

1000   is a socket port number

Response:

   076.6 (in Deg.F format)

4.5.2 HTTPget and ARP to setup Device IP Address

▼ *Tip* ☞ Use the iConnect software, which may be downloaded from our website, to do these IP changes whenever possible.

Use ARP first to assign the mac address to a static IP address in computer arp table by this command:

arp –s 192.168.1.200 00-03-34-00-06-b6

Then use the following command to assign new IP to the device:

httpget –r –S "00000000" 192.168.1.200:1

where:

"**0000000**" is admin. password. If the password is wrong, the unit will ignore the new IP. If the new IP is taken, you will get the message " New IP is Assigned" after the HTTPget command. The device will reset automatically.

"**192.168.1.200**" is an example of an IP address. It is replaced with IP address suitable for your network

"**00-03-34-00-06-b6**" is replaced with your iServer product MAC address.

4.6 ARP Protocol

ARP is the Internet layer protocol responsible for matching or obtaining the MAC (hardware) address that corresponds to a particular IP address. The ARP command allows the user to view the current contents of the ARP cache of the local computer (residing on the same network).

Microsoft includes the ARP.EXE utility for viewing and modifying the ARP cache with its Windows products. The following ARP commands can be used to view cache entries:

*   **arp –a** ➙ Use this command to view all ARP cache entries.
*   **arp –a** plus **IP address** ➙ Use this command to view ARP cache entries associated with one particular interface on a network with multiple adapters.
*   **arp –g** ➙ Same as arp –a.
*   **arp –N** ➙ Use this command to display ARP entries for specific network interface.
*   **arp – s** plus **IP address** plus **Physical address** ➙ Use this command to manually add a permanent static entry to the ARP cache.
*   **arp –d** ➙ Use this command to manually delete a static entry.
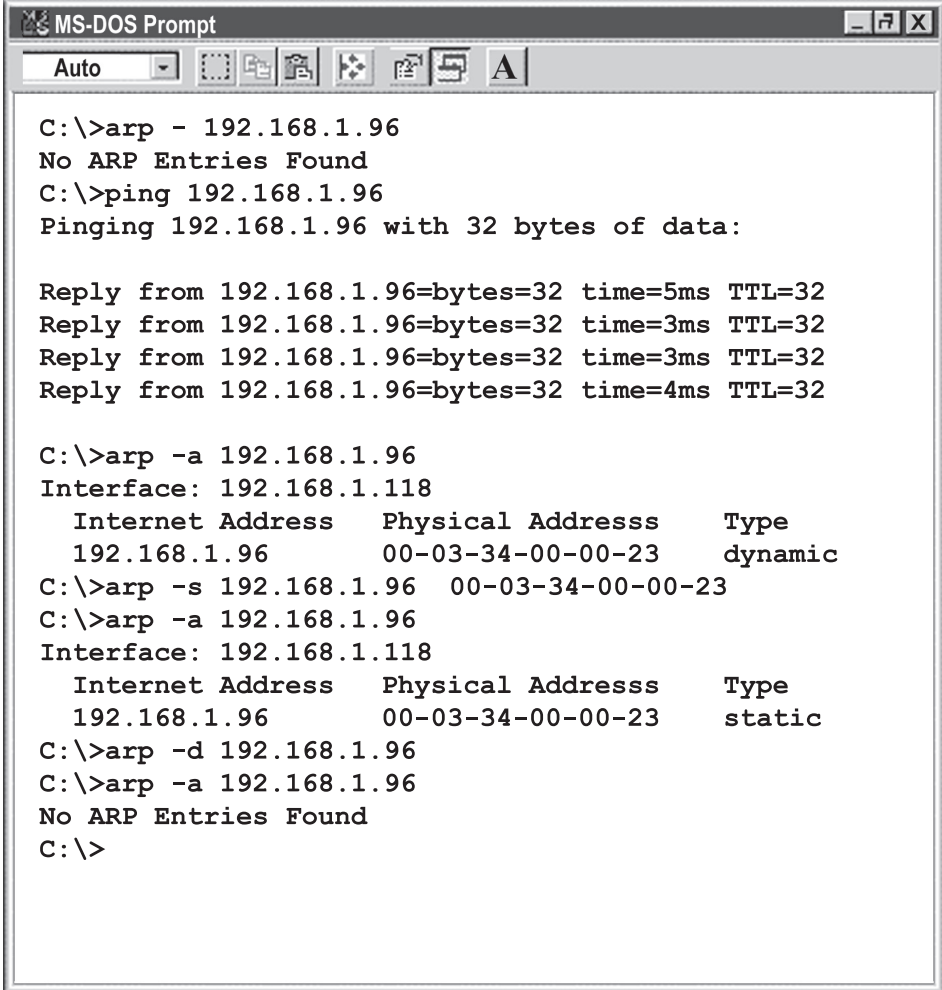
▼ *Note* ☞ Ping the destination computer using IP address first before using the arp -a command.

4.6 ARP Protocol (continued)

The following window shows examples of arp commands and responses.
- Your computer has an IP address of **192.168.1.118**
- The destination computer has an IP address of **192.168.1.96**

```
C:\>arp - 192.168.1.96
No ARP Entries Found
C:\>ping 192.168.1.96
Pinging 192.168.1.96 with 32 bytes of data:

Reply from 192.168.1.96=bytes=32 time=5ms TTL=32
Reply from 192.168.1.96=bytes=32 time=3ms TTL=32
Reply from 192.168.1.96=bytes=32 time=3ms TTL=32
Reply from 192.168.1.96=bytes=32 time=4ms TTL=32

C:\>arp -a 192.168.1.96
Interface: 192.168.1.118
  Internet Address    Physical Addresss    Type
  192.168.1.96        00-03-34-00-00-23    dynamic
C:\>arp -s 192.168.1.96  00-03-34-00-00-23
C:\>arp -a 192.168.1.96
Interface: 192.168.1.118
  Internet Address    Physical Addresss    Type
  192.168.1.96        00-03-34-00-00-23    static
C:\>arp -d 192.168.1.96
C:\>arp -a 192.168.1.96
No ARP Entries Found
C:\>
```

Figure 4.14 ARP Commands and Responses

4.7 Remote Access (Tunneling)

To "tunnel", in this context, is to transmit data between two points through a private conduit on a shared or public network. The network could be an Ethernet LAN, a WAN, or the Internet. There is a Serial-to-Ethernet iServer that allows for a connection between a serial device and a PC, or between two serial devices, using an existing network rather than dedicated wiring.

The connected serial devices to iServer's can communicate with each other back and forth over the networks. This characteristic is called Tunneling and it's illustrated below.
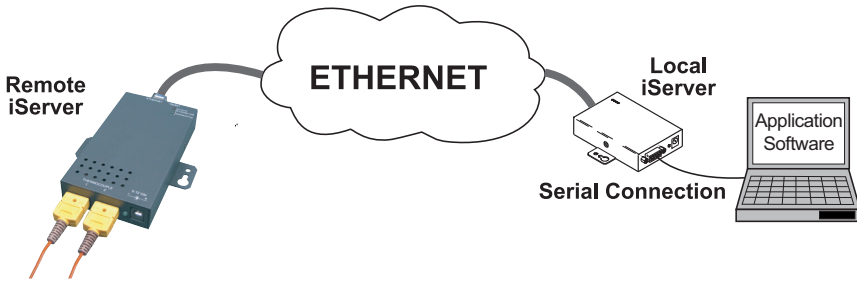
Figure 4.15 PC-to-Device Communication
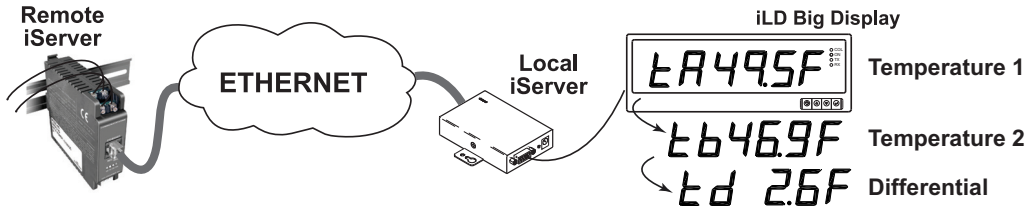
Figure 4.16 Device-to-Device Communication

In order to use this Tunneling feature, some settings are required within the local and remote iServer's.

4.7.1 Local iServer

1. An IP address should be assigned to the iServer dynamically or statically (recommended).
2. Use a browser to access the Local iServer's WEB page. Simply type the iServer's IP address at the browser's URL location (i.e. **192.168.1.49**) followed by an **Enter** key. You should then see the iServer's main WEB page.
3. Click on the **Update** button.
4. Click on **Configuration**, you will be prompted with a **Password** (default is 12345678).
5. On the **Configuration** page, under **Serial Communication** section, make sure the parameters such as Baud Rate, Data Bits, Parity, Stop Bits, Flow Control, etc. match with your attached serial device and its application software.
6. Make sure to set the **End Character (Hex)** to **00** and the **Timeout** to **0**.
7. Under **Terminal Server** section, set **Number of Connections** to **0**.
8. Under **Remote Access** section, set the **Remote Access** to **enable**, Enter the **Remote IP address** (would be the IP address of the remote iServer, **192.168.1.50**), and use the default **Remote Port** number **2000**.
9. Set **Connection Control** to **Reconnect** and set the **Connection Timeout** to a desired value.

> *Note ☞* The **Reconnect** option is used in Serial Tunneling and it applies only to the Local iServer. If the tunneling connection between the two iServers goes down due to network problems, power failure, etc., the Reconnect option will enable the Local iServer to reconnect with the Remote iServer based on the specified time interval in the **Connection Timeout**. For example, based on a timeout of 1000 x 10 ms (10 seconds), the Local iServer will continually attempt to reconnect and re-establish the tunnel with the Remote iServer every 10 seconds.

10. Click on **Save** button for the changes to take place.
11. Initialize the serial device application software to establish the connection.

> *Note ☞* **Figure 4.16** shows the valid values that need to be set in the Local iServer. The Baud Rate, Data Bits, Parity, Stop Bits, Flow Control, and Transceiver values depend on what the attached device to the iServer supports.

CONFIGURATION

Address http://192.168.1.49

CONFIGURATION

Serial Communication

Baud Rate 9600 Data Bit 8 Bits Parity none Stop Bits 1 bit

Flow Control none Transciever RS-232 Modbus/TCP disable

End Char (Hex) 00 Forward End Char enable Timeout 0 msecs

Serial Port Password disable 1234abcd

Terminal Server

TCP/UDP TCP Server Type slave Number of Connections 0 Local Port 02000

Connection Ctrl reconnect Connection Timeout 00100 msecs Device No. 1

Remote Access (Tunneling)

Remote Access enable Remote IP Address 192.168.1.50 Remote Port 02000

Save Reset

Main Menu

Figure 4.17 Local iServer (Serial-to-Ethernet model) - Configuration Page

4.7.2 Remote iServer

1. An IP address should be assigned to the iServer either statically or using a DHCP server. Refer to the DHCP section of the user's manual for details.

2. Use a browser to access the Remote iServer's WEB page. Simply type the iServer's IP address at the browser's URL location (i.e. **192.168.1.50**) followed by an **Enter** key. You should then see the iServer's main WEB page.

3. Click on the **Update** button.

4. Click on **Configuration**, you will be prompted with a **Password** (default is **12345678**).

5. On the **Configuration** page, under Under **Terminal Server** section, set the **Number of Connections (Sockets)** to "**5**".

6. Click on **Save** button for the changes to take place.

At this point, reset the power, first on the remote and then the local iServer and initialize the local serial device to send or request data.

Figure 4.18 Remote iServer Configuration Page

4.8 iLog Software

This is an Excel application software that can log temperature 1, temperature 2 and the differential from the iServer over the local network (Ethernet) or the internet.

a) Download the iLog software from the website listed in this manual.

b) Install iLog software on a networked PC. This software is compatible with Windows 95, 98, NT, 2000, XP, Windows Vista and Windows 7 (32 and 64-bit).

c) If you have Excel 2007 or higher, when installing iLog choose "Custom" installation option and on the next window check the box for "Excel 2007 Apps" and continue the installation to the end.

d) For complete information of how to use the iLog software, click on the HELP button.

e) There is a list of Error Messages in **Appendix E**.

Figure 4.19 iLog Software Logging Data

4.9 Mail Notifier Software

For complete information of how to use the Mail Notifier software, click on the Help menu of the main window.

The Mail Notifier software generates email notifications for alarm conditions. Users can be notified automatically of alarm conditions monitored via internet connections throughout the world. By use of the email forwarding of alarm conditions, alarm conditions can be monitored on a network isolated from the internet and forwarded to connections on the Internet.

The Mail Notifier utility operates under Windows 98, NT 4.0, 2000, and XP in conjunction with existing email that supports the MAPI messaging interface. If MS Outlook has been loaded, the MAPI support should be available.

4.9.1 Installation

The Mail Notifier must be loaded on a computer running Microsoft Windows (versions specified earlier) using an email program that provides MAPI access. Network access must be available between this computer and the iServer. Network access must also be available from this computer to the appropriate email server and from the email server to the recipient's email server.
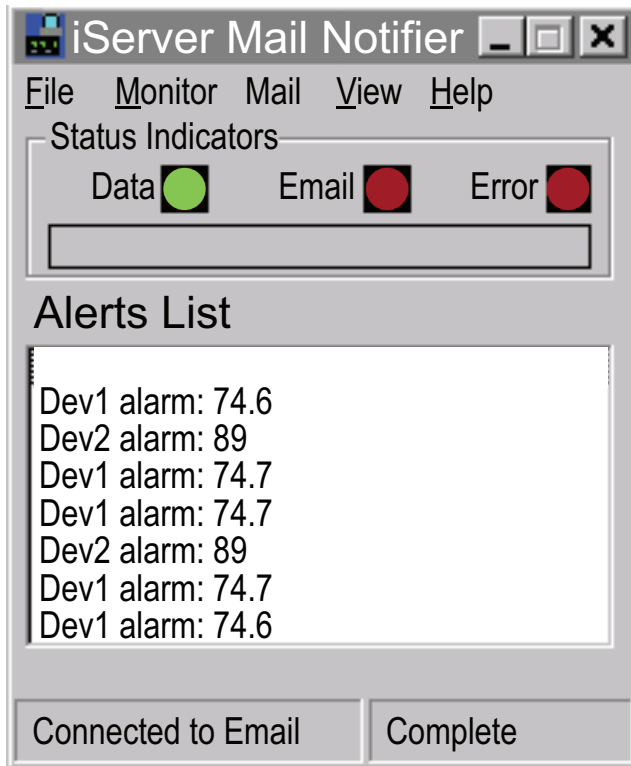
Figure 4.20 iServer Mail Notifier Main Window

4.9.2 Program Options Setup and Configuration

Complete program setup requires:

- Entering a recipient for the email
- Specifying connection details to MAPI services.
- Defining alarms for devices, and selecting how and when the email will be active.

Figure 4.21 iServer Mail Notifier Profile Setup

Email Address Setup

The email addresses must be entered using individual addresses or alias. Select "Options" from the "View" menu and enter the email addresses on the "Send To" screen. This will be the list of email addresses to which alarm notifications will be sent.

Email Setup

The Mail Notifier is compatible with original MS Outlook™ and Outlook™ 2002 to 2005.

The Mail Notifier will attempt to automatically identify whether the Outlook is a newer version. A red bar appears under the Mail Notifier splash window to confirm that the detection of the 2002 or newer version is acceptable. With the newer versions, no additional steps should be taken to enable the connection between the Mail Notifier and the Email server.

> **Note ☞** MS Outlook tends to require that the users respond to a "login box" in order for email access to be activated for Mail Notifier. Some other email clients may allow for Mail Notifier to gain access without user login, as may be desired for a system recovering from a power outage. See the Help files for more information.

4.9.2.1 Sending email Messages to a Cell Phone

In the **Send To** field, you can use the following format to have the Mail Notifier send an email message to your cell phone. Since most cell phones are capable of receiving text messages you just need to find the correct email format for your cell phone provider.

T-Mobile	phone_number@tmomail.net
Virgin Mobile	phone_number@vmobl.com
AT&T	phone_number@txt.att.net
Sprint	phone_number@messaging.sprintpcs.com
Verizon	phone_number@vtext.com
Nextel	phone_number@messaging.nextel.com

"phone_number" is your 10 digit cell phone number.

34

4.9.3 Device Setting and Configuration

Device setup requires:

- Entering the <u>IP address</u> for iServer device (for example **192.168.1.200**).
- Specifying <u>Socket number</u> (1000 or 2000 depending on iServer settings).
- Defining <u>RS485 Unit #</u> interface address (1 to 199). Enter "0" for RS232 interface or for iServer.
- Entering <u>Reading command</u>. Normally set to **SRT** to obtain reading from the devices.If you want to change this setting, refer to HTTPget **Section 4.5**.
- Defining the <u>Alarm setup</u> (High/Low, High value, or Low value).
- Specifying <u>Pause Interval</u>. It determines how many seconds each subsequential alarm notification will be sent.
- Determining <u>Monitor interval</u>. It establishes the interval or time resolution in seconds for which readings will be obtained from the device.

Figure 4.22 iServer Mail Notifier Device Setting

PART 5 SPECIFICATIONS

Thermocouple Input

Temperature Range:
refer to Thermocouple Chart

Temperature Accuracy:
refer to Thermocouple Chart

Resolution: 1°/0.1°

Temperature Stability: 0.08°C/°C

Thermocouple Cold End Tracking:
0.05°C/°C

Thermocouple Lead Resistance:
100 ohm max.

Thermocouple Type (ITS 90):
J, K, T, E, R, S, B, C, N, L

Sampling Rate: 2, 4, 8, or 12 samples per second

iSERVER SPECIFICATIONS

Interfaces

Ethernet: 10Base-T (RJ45)

Supported Protocols: TCP/IP, UDP/IP, ARP, ICMP, DHCP, DNS, HTTP, and Telnet

Indicators (LED's): Network Activity, Network Link, and Receive/Transmit Diagnostics

Processor: Enhanced 8051, 22 MHz

Memory: 512 Kbytes Flash, 16 Kbytes SRAM

Management: Device configuration and monitoring through embedded WEB server

Embedded WEB Server: Serves WEB pages containing real-time data and live updated charts within definable time intervals.

Software: Packages available are--iConnect, iLog, and Mail Notifier; compatible with all Windows operating systems.

Field firmware upgradeable..

Agency Approvals: FCC-B, CE

POWER

Input: 9 to 12 Vdc *iTCX-W* ;
10 to 32 Vdc *iTCX-D*

Safety Qualified ac power adapter:
  Nominal Output: 9 Vdc @ 0.5A;
  Input: 100 to 240Vac, 50/60 Hz included
  for *iTCX-W*

Switching Power Supply sold separately for *iTCX-D*

Consumption: 2.5 W max.

ENVIRONMENTAL

Operating Temp: 0 to 70°C (32 to 158°F)

Storage Temp: -40 to 125°C (-40 to 257°F)

PACKAGING

Material: Metal case, flange mount *iTCX-W*;
Polycarbonate case with DIN Rail mount *iTCX-D*

Dimensions: 21H x 62W x 112D mm (0.83 x 2.42 x 4.41") *iTCX-W*;
90H x 25W x 115D mm (3.54 x 0.99 x 4.53") *iTCX-D*

Weight: 0.11 kg (0.24 lbs) *iTCX-W;*
0.20 kg (0.44 lbs) *iTCX-D*

	Input Type	Range	Accuracy
J	Iron - Constantan	-210 to 760°C / -346 to 1400°F	0.4°C / 0.7°F
K	CHROMEGA®- ALOMEGA®	-270 to -160°C / -160 to 1372°C -454 to -256°F / -256 to 2502°F	1.0°C / 0.4°C 1.8°F / 0.7°F
T	Copper - Constantan	-270 to -190°C / -190 to 400°C -454 to -310°F / -310 to 752°F	1.0°C / 0.4°C 1.8°F / 0.7°F
E	CHROMEGA®- Constantan	-270 to -220°C / -220 to 1000°C -454 to -364°F / -364 to 1832°F	1.0°C / 0.4°C 1.8°F / 0.7°F
R	Pt / 13%Rh-Pt	-50 to 40°C / 40 to 1768°C -58 to 104°F / 104 to 3214°F	1.0°C / 0.5°C 1.8°F / 0.9°F
S	Pt / 10%Rh-Pt	-50 to 100°C / 100 to 1768°C -58 to 212°F / 212 to 3214°F	1.0°C / 0.5°C 1.8°F / 0.9°F
B	30%Rh-Pt / 6%Rh-Pt	100 to 640°C / 640 to 1820°C 212 to 1184°F / 1184 to 3308°F	1.0°C / 0.5°C 1.8°F / 0.9°F
C	5%Re-W / 26%Re-W	0 to 2320°C / 32 to 4208°F	0.4°C / 0.7°F
N	Nicrosil - Nisil	-250 to -100°C / -100 to 1300°C -418 to -148°F / -148 to 2372°F	1.0°C / 0.4°C 1.8°F / 0.7°F
L	J DIN	-200 to 900°C / -328 to 1652°F	0.4°C / 0.7°F

PART 6
FACTORY PRESET VALUES

PRESET PARAMETERS	FACTORY DEFAULTS
Network Interface:	
IP Address	192.168.1.200
Gateway Address	0.0.0.0
Subnet Mask	255.255.255.0
Device Host Name	eis and last 4 digits from the MAC address
Login Password	12345678
Admin Password	00000000
DHCP	Disabled
Flow Control	None
End Character	0D (Hex) (Carridge Return)
Terminal Server:	
Server Type	Continuous
Number of Connections	0
Port #	2000
TCP/UDP	TCP
Remote Access (Tunneling):	
Remote Access	Disabled
Remote Port	2000
Remote IP Address	0.0.0.0

APPENDIX A   GLOSSARY

User of this manual should be familiar with following definitions:

ARP (Address Resolution Protocol) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. For example, the IP address in use today is an address that is 32-bits long. In an Ethernet local area network, however, addresses for attached devices are 48-bits long. (The physical machine address is also known as a Media Access Control or MAC address.) A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions.

Ethernet is a network protocol defined by the IEEE 802.3 standard. Ethernet-based networks use MAC Address rather then IP Address to exchange data between computers. By using ARP and adding TCP/IP support, Ethernet devices may be connected as part of the Internet. An Ethernet LAN typically uses coaxial cable or special grades of twisted pair wires. The most commonly installed Ethernet systems are called 10BASE-T and provide transmission speeds up to 10 Mbps. Devices are connected to the cable and compete for access using a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol.

IP (Internet Protocol) is the method or protocol by which data is sent from one computer to another on the Internet.

IP address (Internet Protocol address) is a 32-bit number that identifies each sender or receiver of information that is sent in packets across the Internet.

IP Netmask is a 32-bit pattern of bits used to determine which part of the IP address is the network portion and which part is the host portion.

MAC (Media Access Control) Address is your computer's unique hardware number. When you're connected to the Internet from your computer, a correspondence table relates your IP address to your computer's physical (MAC) address on the LAN.

Ping is a utility that tests the network connectivity. It is used to determine if the host is capable of exchanging information with another host.

Port number/Socket number is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a server. It is a predefined address that serves as a route from the application to the Transport layer or from the Transport layer to the application of the TCP/IP system.

Sockets are a method for communication between a client program and a server program in a network and defined as "the endpoint in a connection." Information transferred across the Internet primarily occurs between sockets.

TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP. TCP/IP often is used as a general term to indicate generic access to the Internet.

Appendix B   IP Address

An IP address is a unique 32-bit address assigned to a computer and includes:

- A network ID number identifying a network.
- A host ID number identifying a computer on the network.

All IP addresses have been divided into three smaller groups (classes) A, B and C

- **Class A** addresses have 8-bits of network ID and 24-bits of host ID. They can support a large number of hosts, approximately 2 = 16,777,216 computers per network.

  The IP addresses range in binary from 00000001.xxxxxxxx.xxxxxxxx.xxxxxxxx
  to 01111111.xxxxxxxx.xxxxxxxx.xxxxxxxx

  The IP addresses range in decimal from 1.x.x.x to 127.x.x.x

  Class A network ID's support a very large number of hosts.

- **Class B** addresses have 16-bits of network ID and 16-bits of host ID. They can support approximately 2^{16} = 65,536 computers per network.

The IP addresses range in binary from 10000000 00000000.xxxxxxxx.xxxxxxxx
to 10111111 11111111.xxxxxxxx.xxxxxxxx

  The IP addresses range in decimal from 128.0.x.x to 191.255.xxx.xxx

  Class B network ID's support a medium number of hosts.

- **Class C** addresses have 24-bits of network ID and 8-bits of host ID. They can support approximately 2^8 = 256 computers per network.

  The IP addresses range in binary from 11000000.00000000.00000000.xxxxxxxx
  to 11011111.11111111.11111111.xxxxxxxx

  The IP addresses range in decimal from 192.0.0.xxx to 223.255.255.xxx

  Class C network ID's support a small number of hosts.

Note ☞   The rest of the addresses are divided into two classes, D and E.
Class D networks are not assigned to the host. They are used for multicasting. The address range from 224.x.x.x to 239.x.x.x

Class E networks are experimental or reserved addresses. The address range from 240.x.x.x to 247.x.x.x

Appendix C   **IP Netmask**

IP Netmask or Subnet Mask is a 32-bit pattern of ones and zeros used to determine network portion of an IP address from the host portion of the IP address. Subnet mask is a network ID that is created by borrowing bits from host portion of IP address and using them as part of a network ID. The table below shows a default subnet mask for address Classes A, B, and C. Each bit that is set to "1" in the subnet mask corresponds to the bit in the IP address that is to be used as the network ID. Each bit that is set to "0" in the subnet mask corresponds to a bit in the IP address that is to be used as the host ID.

Address Class	Mask Binary Value	Mask Decimal Value or Dotted Notation
Class A	11111111 00000000 00000000 00000000	255.0.0.0
Class B	11111111 11111111 00000000 00000000	255.255.0.0
Class C	11111111 11111111 11111111 00000000	255.255.255.0

If your network requires more network ID's, you can extend the default subnet mask to include additional bits from the host ID. This allows for additional network ID's within the network. The table below shows some examples of subnet masks and bits moved from the hosts ID to create a new subnet.

Mask Dotted Notation	Mask Binary	Mask Bits
	Class A	
255.0.0.0 (Default)	11111111 00000000 00000000 00000000	0
255.192.0.0	11111111 11000000 00000000 00000000	2
255.224.0.0	11111111 11100000 00000000 00000000	3
255.240.0.0	11111111 11110000 00000000 00000000	4
255.248.0.0	11111111 11111000 00000000 00000000	5
255.252.0.0	11111111 11111100 00000000 00000000	6
255.254.0.0	11111111 11111110 00000000 00000000	7
255.255.0.0	11111111 11111111 00000000 00000000	8
255.255.128.0	11111111 11111111 10000000 00000000	9
255.255.192.0.0	11111111 11111111 11000000 00000000	10
....	....	.
255.255.255.252	11111111 11111111 11111111 11111100	22
	Class B	
255.255.0.0 (Default)	11111111 11111111 00000000 00000000	0
255.255.192.0	11111111 11111111 11000000 00000000	2
....	....	.
255.255.255.252	11111111 11111111 11111111 11111100	14
	Class C	
255.255.255.0 (Default)	11111111 11111111 11111111 00000000	0
255.255.255.192	11111111 11111111 11111111 11000000	2
....	....	.
255.255.255.254	11111111 11111111 11111111 11111100	6

To determine the number of valid hosts ID's remaining after subnetting, use the following equation: $2^n - 2$, where n is the number of octet digits left after the subnet mask.

Appendix D   ASCII Chart

ASCII Char	Dec	Hex	Binary No Parity	ASCII Char	Dec	Hex	Binary No parity
NUL	00	00	00000000	@	64	40	01000000
SOH	01	01	00000001	A	65	41	01000000
STX	02	02	00000010	B	66	42	01000010
ETX	03	03	00000011	C	67	43	01000011
EOT	04	04	00000100	D	68	44	01000100
ENQ	05	05	00000101	E	69	45	01000101
ACK	06	06	00000110	F	70	46	01000110
BEL	07	07	00000111	G	71	47	01000111
BS	08	08	00001000	H	72	48	01001000
HT	09	09	00001001	I	73	49	01001001
LF	10	0A	00001010	J	74	4A	01001010
VT	11	0B	00001011	K	75	4B	01001011
FF	12	0C	00001100	L	76	4C	01001100
CR	13	0D	00001101	M	77	4D	01001101
SO	14	0E	00001110	N	78	4E	01001110
SI	15	0F	00001111	O	79	4F	01001111
DLE	16	10	00010000	P	80	50	01010000
DC1	17	11	00010001	Q	81	51	01010001
DC2	18	12	00010010	R	82	52	01010010
DC3	19	13	00010011	S	83	53	01010011
DC4	20	14	00010100	T	84	54	01010100
NAK	21	15	00010101	U	85	55	01010101
SYN	22	16	00010110	V	86	56	01010110
ETB	23	17	00010111	W	87	57	01010111
CAN	24	18	00011000	X	88	58	01011000
EM	25	19	00011001	Y	89	59	01011001
SUB	26	1A	00011010	Z	90	5A	01011010
ESC	27	1B	00011011	[	91	5B	01011011
FS	28	1C	00011100	\	92	5C	01011100
GS	29	1D	00011101	]	93	5D	01011101
RS	30	1E	00011110	^	94	5E	01011110
US	31	1F	00011111	_	95	5F	01011111
SP	32	20	00100000	`	96	60	01100000
!	33	21	00100001	a	97	61	01100001
"	34	22	00100010	b	98	62	01100010
#	35	23	00100011	c	99	63	01100011
$	36	24	00100100	d	100	64	01100100
%	37	25	00100101	e	101	65	01100101
&	38	26	00100110	f	102	66	01100110
'	39	27	00100111	g	103	67	01100111
(	40	28	00101000	h	104	68	01101000
)	41	29	00101001	I	105	69	01101001
*	42	2A	00101010	j	106	6A	01101010
+	43	2B	00101011	k	107	6B	01101011
,	44	2C	00101100	l	108	6C	01101100
-	45	2D	00101101	m	109	6D	01101101
.	46	2E	00101110	n	110	6E	01101110

Appendix D — ASCII Chart Continuation

/	47	2F	00101111	o	111	6F	01101111
0	48	30	00110000	p	112	70	01110000
1	49	31	00110001	q	113	71	01110001
2	50	32	00110010	r	114	72	01110010
3	51	33	00110011	s	115	73	01110011
4	52	34	00110100	t	116	74	01110100
5	53	35	00110101	u	117	75	01110101
6	54	36	00110110	v	118	76	01110110
7	55	37	00110111	w	119	77	01110111
8	56	38	00111000	x	120	78	01111000
9	57	39	00111001	y	121	79	01111001
:	58	3A	00111010	z	122	7A	01111010
;	59	3B	00111011	{	123	7B	01111011
<	60	3C	00111100			124	7C	01111100
=	61	3D	00111101	}	125	7D	01111101
>	62	3E	00111110	~	126	7E	01111110
?	63	3F	00111111	DEL	127	7F	01111111

ASCII Control Codes

ASCII Char	Dec	Hex	Ctrl Key Equiv.	Definition	ASCII Char	Dec	Hex	Ctrl Key Equiv.	Definition
NUL	00	00	Crtl @	Null Character	DC1	17	11	Crtl Q	Data Control 1 - XON
SOH	01	01	Crtl A	Start of Header	DC2	18	12	Crtl R	Data Control 2
STX	02	02	Crtl B	Start of Text	DC3	19	13	Crtl S	Data Control 3 - XOFF
ETX	03	03	Crtl C	End of Text	DC4	20	14	Crtl T	Data Control 4
EOT	04	04	Crtl D	End of Transmission	NAK	21	15	Crtl U	Negative Acknowledge
ENQ	05	05	Crtl E	Inquiry	SYN	22	16	Crtl V	Synchronous Idle
ACK	06	06	Crtl F	Acknowledge	ETB	23	17	Crtl W	End of Trans Block
BEL	07	07	Crtl G	Bell	CAN	24	18	Crtl X	Cancel
BS	08	08	Crtl H	Back Space	EM	25	19	Crtl Y	End of Medium
HT	09	09	Crtl I	Horizontal Tabulation	SUB	26	1A	Crtl Z	Substitute
LF	10	0A	Crtl J	Line Feed	ESC	27	1B	Crtl [	Escape
VT	11	0B	Crtl K	Vertical Tabulation	FS	28	1C	Crtl \	File Separator
FF	12	0C	Crtl L	Form Feed	GS	29	1D	Crtl]	Group Separator
CR	13	0D	Crtl M	Carriage Return	RS	30	1E	Crtl		Record Separator
SO	14	0E	Crtl N	Shift Out	US	31	1F	Crtl _	Unit Separator
SI	15	0F	Crtl O	Shift In	SP	32	20		Space
DLE	16	10	Crtl P	Data Link Escape					

Appendix E   iLog Error Messages

Error #	Description	Note
-8003	User stopped logging readings.	
-10005	Failed to find the iServer.	Ethernet cable is disconnected, iServer is powered off, connections across the firewall require longer "connection to socket time out" setting.
-10006	Windows socket was closed.	
-10007	Windows socket error.	Wrong IP or wrong Port number was used.
-10008	The iServer failed to respond to a request.	Wrong IP or wrong Port number was used.
-10011	Response came empty.	No data was sent.
-10012	Device responded with "Serial Time Out" string.	Possibly the iLog is configured for wrong product model.
-10014	Terminal Server Mode when the Port is 1000.	Try Port 2000 in iLog configuration.
-15100	Error on obtaining the temperature reading.	Possibly the iLog is configured for wrong product model.
-15105	Error on obtaining the humidity reading.	Possibly the iLog is configured for wrong product model.
-15110	Error on obtaining the dew point reading.	Possibly the iLog is configured for wrong product model.

PART 7
APPROVALS INFORMATION
7.1 CE APPROVAL

CE This product conforms to the EMC directive 89/336/EEC amended by 93/68/EEC, and with the European Low Voltage Directive 72/23/EEC.

Electrical Safety EN61010-1:2001

Safety requirements for electrical equipment for measurement, control and laboratory.

Basic Insulation

Pollution Degree 2

Dielectric withstand Test per 1 min

- Input Power to Ethernet Output: 1500Vac
- Input Power to Sensor Metal Body: 1500Vac
- Ethernet to Sensor Metal Body: 1500Vac

Measurement Category I

Category I are measurements performed on circuits not directly connected to the Mains Supply (power). Unit measures Temperature .

Transients Overvoltage Surge (1.2/50uS Pulse)

- Input Power: 500V Transients Overvoltage
- Sensor :   500V Transients Overvoltage
- Ethernet: 1500V Transients Overvoltage

Note: *The ac power adaptor must have Safety Qualified Agency Approvals for CE with Double Insulation rating.*

The power input rating is 10-32Vdc.

The minimum output current rating is 500mA.

EMC EN61000-6-1:2001 (Immunity) and EN61000-6-3:2001 (Emmissions)

Immunity requirements for residential, commercial and light-industrial environments

- EMC Emissions   Table 1, Class B
- EMC Immunity   Table 1: Enclosure
                    Table 2: Signal Lines Ports
                    Table 3: Dc input/Dc output Ports

EMC EN61326:1997 + and A1:1998 + A2:2001

Immunity and Emissions requirements for electrical equipment for measurement, control and laboratory.

- EMC Emissions   Table 4, Class B of EN61326
- EMC Immunity   Table 1 of EN61326

Note: *I/O lines / sensor cables require shielded cables and these cables must be located on conductive cable trays or in conduits.*

⚠ Refer to the EMC and Safety installation considerations (Guidelines) of this manual for additional information.

7.2   FCC

This device complies with Part 15, Subpart B, Class B of the FCC rules.

NOTES

NOTES

NOTES

NOTES

NOTES

WARRANTY/DISCLAIMER

OMEGA ENGINEERING, INC. warrants this unit to be free of defects in materials and workmanship for a period of **one (1) year** from the date of purchase. In addition to OMEGA's standard warranty period, OMEGA Engineering will extend the warranty period for **one (1) additional year** if the warranty card enclosed with each instrument is returned to OMEGA.

If the unit malfunctions, it must be returned to the factory for evaluation. OMEGA's Customer Service Department will issue an Authorized Return (AR) number immediately upon phone or written request. Upon examination by OMEGA, if the unit is found to be defective, it will be repaired or replaced at no charge. OMEGA's WARRANTY does not apply to defects resulting from any action of the purchaser, including but not limited to mishandling, improper interfacing, operation outside of design limits, improper repair, or unauthorized modification. This WARRANTY is VOID if the unit shows evidence of having been tampered with or shows evidence of having been damaged as a result of excessive corrosion; or current, heat, moisture or vibration; improper specification; misapplication; misuse or other operating conditions outside of OMEGA's control. Components which wear are not warranted, including but not limited to contact points, fuses, and triacs.

OMEGA is pleased to offer suggestions on the use of its various products. However, OMEGA neither assumes responsibility for any omissions or errors nor assumes liability for any damages that result from the use of its products in accordance with information provided by OMEGA, either verbal or written. OMEGA warrants only that the parts manufactured by it will be as specified and free of defects. OMEGA MAKES NO OTHER WARRANTIES OR REPRESENTATIONS OF ANY KIND WHATSOEVER, EXPRESS OR IMPLIED, EXCEPT THAT OF TITLE, AND ALL IMPLIED WARRANTIES INCLUDING ANY WARRANTY OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY DISCLAIMED. LIMITATION OF LIABILITY: The remedies of purchaser set forth herein are exclusive, and the total liability of OMEGA with respect to this order, whether based on contract, warranty, negligence, indemnification, strict liability or otherwise, shall not exceed the purchase price of the component upon which liability is based. In no event shall OMEGA be liable for consequential, incidental or special damages.

CONDITIONS: Equipment sold by OMEGA is not intended to be used, nor shall it be used: (1) as a "Basic Component" under 10 CFR 21 (NRC), used in or with any nuclear installation or activity; or (2) in medical applications or used on humans. Should any Product(s) be used in or with any nuclear installation or activity, medical application, used on humans, or misused in any way, OMEGA assumes no responsibility as set forth in our basic WARRANTY/DISCLAIMER language, and, additionally, purchaser will indemnify OMEGA and hold OMEGA harmless from any liability or damage whatsoever arising out of the use of the Product(s) in such a manner.

RETURN REQUESTS/INQUIRIES

Direct all warranty and repair requests/inquiries to the OMEGA Customer Service Department. BEFORE RETURNING ANY PRODUCT(S) TO OMEGA, PURCHASER MUST OBTAIN AN AUTHORIZED RETURN (AR) NUMBER FROM OMEGA'S CUSTOMER SERVICE DEPARTMENT (IN ORDER TO AVOID PROCESSING DELAYS). The assigned AR number should then be marked on the outside of the return package and on any correspondence.

The purchaser is responsible for shipping charges, freight, insurance and proper packaging to prevent breakage in transit.

FOR <u>WARRANTY</u> RETURNS, please have the following information available BEFORE contacting OMEGA:

1. Purchase Order number under which the product was PURCHASED,
2. Model and serial number of the product under warranty, and
3. Repair instructions and/or specific problems relative to the product.

FOR <u>NON-WARRANTY</u> REPAIRS, consult OMEGA for current repair charges. Have the following information available BEFORE contacting OMEGA:

1. Purchase Order number to cover the COST of the repair,
2. Model and serial number of product, and
3. Repair instructions and/or specific problems relative to the product.

OMEGA's policy is to make running changes, not model changes, whenever an improvement is possible. This affords our customers the latest in technology and engineering.

TRADEMARK NOTICE: ΩΕ ®, *omega.com*®, ΩΕ **OMEGA**®, and ℔ are Trademarks of OMEGA ENGINEERING, INC.

PATENT NOTICE: This product is covered by one or more of the following patents: U.S. Pat. No. Des. 336,895; 5,274,577/ CANADA 2052599; 2052600 / ITALY 1249456; 1250938 / FRANCE BREVET No. 91 12756 / SPAIN 2039150; 2048066 / UK PATENT No. GB2 249 837; GB2 248 954 / GERMANY DE 41 34398 C2. Other US and International Patents pending or applied for.

Where Do I Find Everything I Need for Process Measurement and Control? OMEGA...Of Course!
Shop on line at omega.com

TEMPERATURE
- ☑ Thermocouple, RTD & Thermistor Probes, Connectors, Panels & Assemblies
- ☑ Wire: Thermocouple, RTD & Thermistor
- ☑ Calibrators & Ice Point References
- ☑ Recorders, Controllers & Process Monitors
- ☑ Infrared Pyrometers

PRESSURE, STRAIN AND FORCE
- ☑ Transducers & Strain Gauges
- ☑ Load Cells & Pressure Gauges
- ☑ Displacement Transducers
- ☑ Instrumentation & Accessories

FLOW/LEVEL
- ☑ Rotameters, Gas Mass Flowmeters & Flow Computers
- ☑ Air Velocity Indicators
- ☑ Turbine/Paddlewheel Systems
- ☑ Totalizers & Batch Controllers

pH/CONDUCTIVITY
- ☑ pH Electrodes, Testers & Accessories
- ☑ Benchtop/Laboratory Meters
- ☑ Controllers, Calibrators, Simulators & Pumps
- ☑ Industrial pH & Conductivity Equipment

DATA ACQUISITION
- ☑ Data Acquisition & Engineering Software
- ☑ Communications-Based Acquisition Systems
- ☑ Plug-in Cards for Apple, IBM & Compatibles
- ☑ Datalogging Systems
- ☑ Recorders, Printers & Plotters

HEATERS
- ☑ Heating Cable
- ☑ Cartridge & Strip Heaters
- ☑ Immersion & Band Heaters
- ☑ Flexible Heaters
- ☑ Laboratory Heaters

ENVIRONMENTAL MONITORING AND CONTROL
- ☑ Metering & Control Instrumentation
- ☑ Refractometers
- ☑ Pumps & Tubing
- ☑ Air, Soil & Water Monitors
- ☑ Industrial Water & Wastewater Treatment
- ☑ pH, Conductivity & Dissolved Oxygen Instruments