INSTRUCTION MANUAL

NL200/NL201
Network Link Interface

Revision: 11/17

Limited Warranty

"Products manufactured by CSI are warranted by CSI to be free from defects in materials and workmanship under normal use and service for twelve months from the date of shipment unless otherwise specified in the corresponding product manual. (Product manuals are available for review online at *www.campbellsci.com*.) Products not manufactured by CSI, but that are resold by CSI, are warranted only to the limits extended by the original manufacturer. Batteries, fine-wire thermocouples, desiccant, and other consumables have no warranty. CSI's obligation under this warranty is limited to repairing or replacing (at CSI's option) defective Products, which shall be the sole and exclusive remedy under this warranty. The Customer assumes all costs of removing, reinstalling, and shipping defective Products to CSI. CSI will return such Products by surface carrier prepaid within the continental United States of America. To all other locations, CSI will return such Products best way CIP (port of entry) per Incoterms ® 2010. This warranty shall not apply to any Products which have been subjected to modification, misuse, neglect, improper service, accidents of nature, or shipping damage. This warranty is in lieu of all other warranties, expressed or implied. The warranty for installation services performed by CSI such as programming to customer specifications, electrical connections to Products manufactured by CSI, and Product specific training, is part of CSI's product warranty. **CSI EXPRESSLY DISCLAIMS AND EXCLUDES ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE**. **CSI hereby disclaims, to the fullest extent allowed by applicable law, any and all warranties and conditions with respect to the Products, whether express, implied or statutory, other than those expressly provided herein.**"

Assistance

Products may not be returned without prior authorization. The following contact information is for US and international customers residing in countries served by Campbell Scientific, Inc. directly. Affiliate companies handle repairs for customers within their territories. Please visit *www.campbellsci.com* to determine which Campbell Scientific company serves your country.

To obtain a Returned Materials Authorization (RMA) number, contact CAMPBELL SCIENTIFIC, INC., phone (435) 227-9000. Please write the issued RMA number clearly on the outside of the shipping container. Campbell Scientific's shipping address is:

CAMPBELL SCIENTIFIC, INC.
RMA#_____
815 West 1800 North
Logan, Utah 84321-1784

For all returns, the customer must fill out a "Statement of Product Cleanliness and Decontamination" form and comply with the requirements specified in it. The form is available from our website at *www.campbellsci.com/repair*. A completed form must be either emailed to *repair@campbellsci.com* or faxed to (435) 227-9106. Campbell Scientific is unable to process any returns until we receive this form. If the form is not received within three days of product receipt or is incomplete, the product will be returned to the customer at the customer's expense. Campbell Scientific reserves the right to refuse service on products that were exposed to contaminants that may cause health or safety concerns for our employees.

Safety

DANGER — MANY HAZARDS ARE ASSOCIATED WITH INSTALLING, USING, MAINTAINING, AND WORKING ON OR AROUND **TRIPODS, TOWERS, AND ANY ATTACHMENTS TO TRIPODS AND TOWERS SUCH AS SENSORS, CROSSARMS, ENCLOSURES, ANTENNAS, ETC**. FAILURE TO PROPERLY AND COMPLETELY ASSEMBLE, INSTALL, OPERATE, USE, AND MAINTAIN TRIPODS, TOWERS, AND ATTACHMENTS, AND FAILURE TO HEED WARNINGS, INCREASES THE RISK OF DEATH, ACCIDENT, SERIOUS INJURY, PROPERTY DAMAGE, AND PRODUCT FAILURE. TAKE ALL REASONABLE PRECAUTIONS TO AVOID THESE HAZARDS. CHECK WITH YOUR ORGANIZATION'S SAFETY COORDINATOR (OR POLICY) FOR PROCEDURES AND REQUIRED PROTECTIVE EQUIPMENT PRIOR TO PERFORMING ANY WORK.

Use tripods, towers, and attachments to tripods and towers only for purposes for which they are designed. Do not exceed design limits. Be familiar and comply with all instructions provided in product manuals. Manuals are available at www.campbellsci.com or by telephoning (435) 227-9000 (USA). You are responsible for conformance with governing codes and regulations, including safety regulations, and the integrity and location of structures or land to which towers, tripods, and any attachments are attached. Installation sites should be evaluated and approved by a qualified engineer. If questions or concerns arise regarding installation, use, or maintenance of tripods, towers, attachments, or electrical connections, consult with a licensed and qualified engineer or electrician.

General

- Prior to performing site or installation work, obtain required approvals and permits. Comply with all governing structure-height regulations, such as those of the FAA in the USA.
- Use only qualified personnel for installation, use, and maintenance of tripods and towers, and any attachments to tripods and towers. The use of licensed and qualified contractors is highly recommended.
- Read all applicable instructions carefully and understand procedures thoroughly before beginning work.
- Wear a **hardhat** and **eye protection**, and take **other appropriate safety precautions** while working on or around tripods and towers.
- **Do not climb** tripods or towers at any time, and prohibit climbing by other persons. Take reasonable precautions to secure tripod and tower sites from trespassers.
- Use only manufacturer recommended parts, materials, and tools.

Utility and Electrical

- **You can be killed** or sustain serious bodily injury if the tripod, tower, or attachments you are installing, constructing, using, or maintaining, or a tool, stake, or anchor, come in **contact with overhead or underground utility lines**.
- Maintain a distance of at least one-and-one-half times structure height, 20 feet, or the distance required by applicable law, **whichever is greater**, between overhead utility lines and the structure (tripod, tower, attachments, or tools).
- Prior to performing site or installation work, inform all utility companies and have all underground utilities marked.
- Comply with all electrical codes. Electrical equipment and related grounding devices should be installed by a licensed and qualified electrician.

Elevated Work and Weather

- Exercise extreme caution when performing elevated work.
- Use appropriate equipment and safety practices.
- During installation and maintenance, keep tower and tripod sites clear of un-trained or non-essential personnel. Take precautions to prevent elevated tools and objects from dropping.
- Do not perform any work in inclement weather, including wind, rain, snow, lightning, etc.

Maintenance

- Periodically (at least yearly) check for wear and damage, including corrosion, stress cracks, frayed cables, loose cable clamps, cable tightness, etc. and take necessary corrective actions.
- Periodically (at least yearly) check electrical ground connections.

WHILE EVERY ATTEMPT IS MADE TO EMBODY THE HIGHEST DEGREE OF SAFETY IN ALL CAMPBELL SCIENTIFIC PRODUCTS, THE CUSTOMER ASSUMES ALL RISK FROM ANY INJURY RESULTING FROM IMPROPER INSTALLATION, USE, OR MAINTENANCE OF TRIPODS, TOWERS, OR ATTACHMENTS TO TRIPODS AND TOWERS SUCH AS SENSORS, CROSSARMS, ENCLOSURES, ANTENNAS, ETC.

Table of Contents

PDF viewers: These page numbers refer to the printed version of this document. Use the PDF reader bookmarks tab for links to specific sections.

Tables

NL200/201 Network Link Interface

1. Introduction

The NL200/201 Network Link Interface allows Campbell Scientific dataloggers and peripherals to communicate over a local area network or a dedicated Internet connection. This serial to Ethernet interface can be connected to a datalogger's CS I/O port or other devices via RS-232.

This manual describes how to use *LoggerNet* to connect to your datalogger with an NL200/201. You can also use other software packages, such as *PC400*, *RTDAQ*, or *LoggerLink* Mobile App*s* for iOS and Android.

2. Precautions

- The first time an NL200/201 is attached to a datalogger and Bridge Mode is enabled, the datalogger's memory has to be reorganized to allow room in memory for the IP stack. To avoid the loss of data, **collect your data before enabling Bridge Mode**. Note that once the NL200/201 is attached, it can take up to 10 seconds for the datalogger to recognize it.

- *Device Configuration Utility* (*DevConfig*) 2.05 or higher is required to communicate with the NL200/201. The latest version of *DevConfig* can be downloaded from our website at *www.campbellsci.com/downloads*.

- The device driver for the NL200/201 must be installed on your computer before you can connect to the NL200/201 via USB.

  To install the device driver, verify you have the latest version of *DevConfig* (see previous bullet). Under Device Type, select Network Peripheral | NL200 Series. Click the **Install the device driver for the device** link and follow the prompts.

- CR1000, CR3000, and CR800-series dataloggers require operating system version 23 or higher in order to operate with the NL200/201 in bridge mode. The latest operating systems can be downloaded from our website at *www.campbellsci.com/downloads*.

- The NL200 is **not** powered over CS I/O or USB. An external power adapter or power cable is required. The NL201 can be powered by the CS I/O port or an external power adapter or power cable. If you wish to prevent the NL201 from being powered by the CS I/O port, see Appendix B, *Cables, Pinouts, LED Function, and Jumper* *(p. B-1)*.

- Ensure maximum protection against surges. Use a shielded Ethernet cable. Keep RS-232 and CS I/O connections short. The NL200 may require the use of external surge suppression (pn 28033). The NL201 has integrated surge protection. The NL201 must be well grounded using the ground lug on the case for the surge protection to work properly.

3. QuickStart

Out of the box, the NL200/201 is configured for operation as a PakBus® Router. In this mode, the NL200/201 can be used to communicate with Campbell Scientific PakBus devices over an Ethernet / Internet network connection.

3.1 Physical Setup

Using the supplied serial cable, connect the NL201's CS I/O port to the datalogger's CS I/O port. Alternatively, power the NL200 or NL201 through the barrel-connector jack located on the edge of the device. Connect the NL200/201 to your network using an Ethernet cable, attaching one end of the cable to the NL200/201's Ethernet port and the other end to your network. Ensure that the device is powered up by inspecting the Power LED.

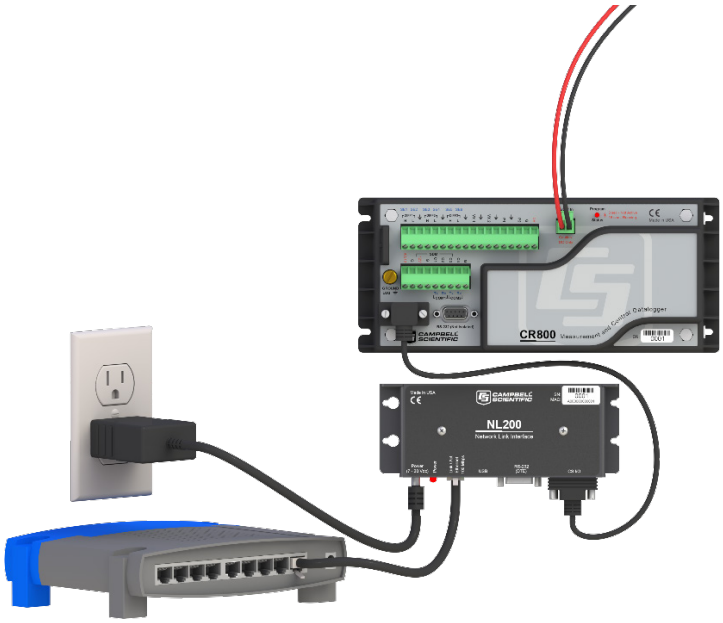


FIGURE 3-1. NL200 with CR800 (external power)

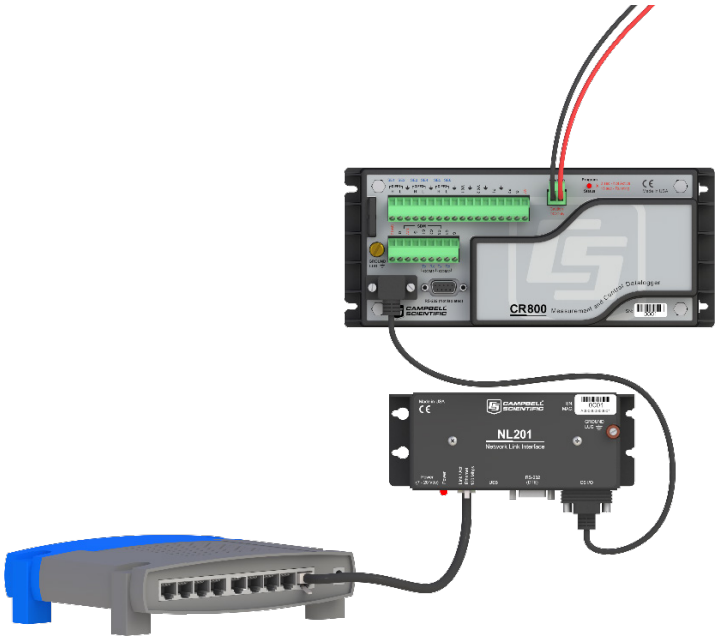


FIGURE 3-2. NL201 with CR800 (powered by datalogger)

3.2 Configuring the NL200/201

NOTE INSTALL THE DEVICE DRIVER BEFORE plugging the NL200/201 into your PC for the first time. You will need the device driver properly installed before you can connect to the NL200/201 via USB.

To install the device driver, download the latest version of *DevConfig* from our website. Under Device Type, select Network Peripheral | NL200 Series. Click the **Install the device driver for the device** link and follow the prompts.

- Ensure the NL200/201 is powered.
- Connect the supplied USB cable between a USB port on your computer and the USB port on the NL200/201.
- Open *DevConfig*.
- Under **Device Type**, select **NL200**.
- Click the **Browse** button next to **Communication Port**.
- Select the port labeled **NL200**.
- Click **OK**.
- Click **Connect**.

- To enter a static IP address, select **disable** in the **Use DHCP** field. Then input the **IP Address**, **Network Mask**, and **Default Gateway**. These values can be provided by your network administrator.
- If a dynamic address is to be used, the network information acquired via DHCP can be seen on the NL200 tab under **Status**. The **Status** box also displays the MAC address of the NL200/201.
- Click **Apply** to save your changes.

NOTE It is recommended that a static IP address be given to the NL200/201 for most applications so that the path to the device is always known. If using a dynamic IP address acquired via DHCP you may wish to configure the NL200/201 as a PakBus/TCP client.

3.3 *LoggerNet* Setup

The next step is to run *LoggerNet* and configure it to connect to the datalogger via the NL200/201.

- In the *LoggerNet Setup* screen, press **Add Root** and choose **IPPort**. Input the NL200/201's IP address and port number. The IP address and port number are input on the same line separated by a colon. IPv6 addresses will need to be enclosed in square brackets when specifying a port number. An IPv4 address may look like 192.168.1.100:6785. An IPv6 address may look like [2001:db8::1234:5678]:6785. A fully qualified host name entry may look like yourlogger.com:6785.
- Add a PakBus® Port (PakBusPort).
- Add a PakBus® Router (pbRouter). Input the PakBus address of the NL200/201. The NL200/201's default PakBus address is 678.
- Add the datalogger and input the PakBus® address of the datalogger.
- Press **Apply** to save the changes.
- You can verify that your settings are correct by selecting the datalogger in the Network Map, selecting the Clock tab, and pressing **Check Clocks**. If your settings are correct, you should see the current clock of your server and datalogger.

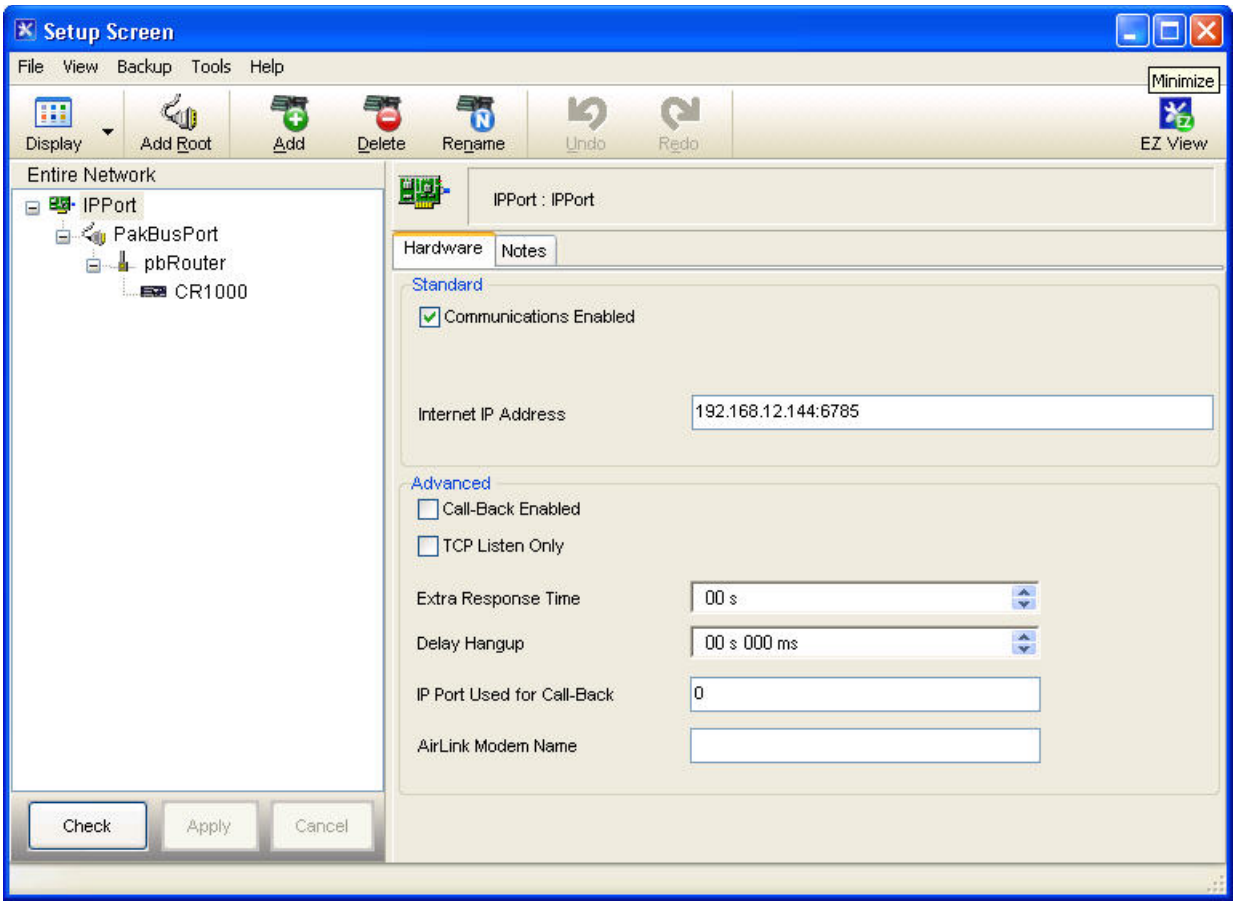


FIGURE 3-3. LoggerNet setup

3.4 Connect

You are now ready to connect to your datalogger using the *LoggerNet Connect* screen.

4. Overview

The NL200/201 Network Link Interface is a device used to communicate with Campbell Scientific dataloggers and peripherals using an Ethernet 10/100 Mbps communications link. The NL200/201 includes a CS I/O port and an RS-232 port for communication. A USB device port is used for configuring the NL200/201 device.

FIGURE 4-1. NL201

Bridge Mode Enabled

The NL200/201 can be configured to bridge Ethernet and CS I/O communications (Bridge Mode enabled). This mode is used for providing access to the internal IP functionality of the CR800/850, CR1000, and CR3000 (e.g., web page access, email, FTP, etc.). Bridge mode does not utilize PPP. Instead, raw IP packets are transferred between the Ethernet and CS I/O connections.

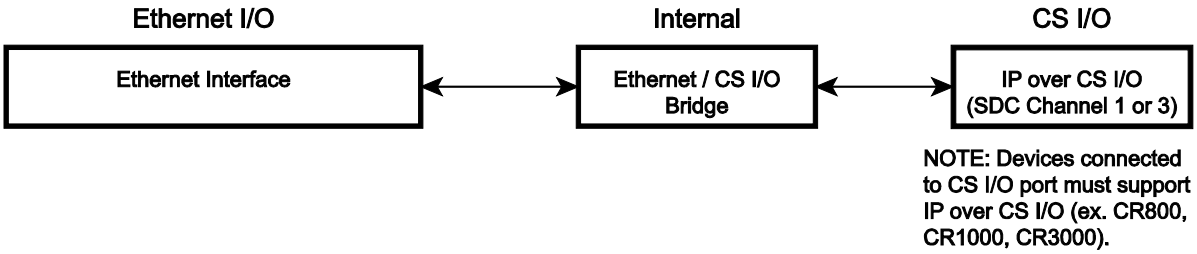


FIGURE 4-2. Bridge Mode enabled

Bridge Mode Disabled

With Bridge Mode disabled, the NL200/201 can provide multiple services simultaneously including TCP Serial Server, TCP Serial Client, Modbus TCP/IP Gateway, and PakBus® router. The NL200/201 can act as a serial server and PakBus router simultaneously. However, each physical port (RS-232 and CS I/O) is only associated with one service (PakBus router, serial server, Modbus/TCP Gateway, etc.) at a time. For example, you can have an RS-232 serial server and a CS I/O serial server, an RS-232 serial server and a CS I/O PakBus router, an RS-232 PakBus router and a CS I/O serial server, or an RS-232 PakBus router and a CS I/O PakBus router. In addition, the NL200/201 can act as TLS proxy server. The TLS proxy server is independent of other modes.

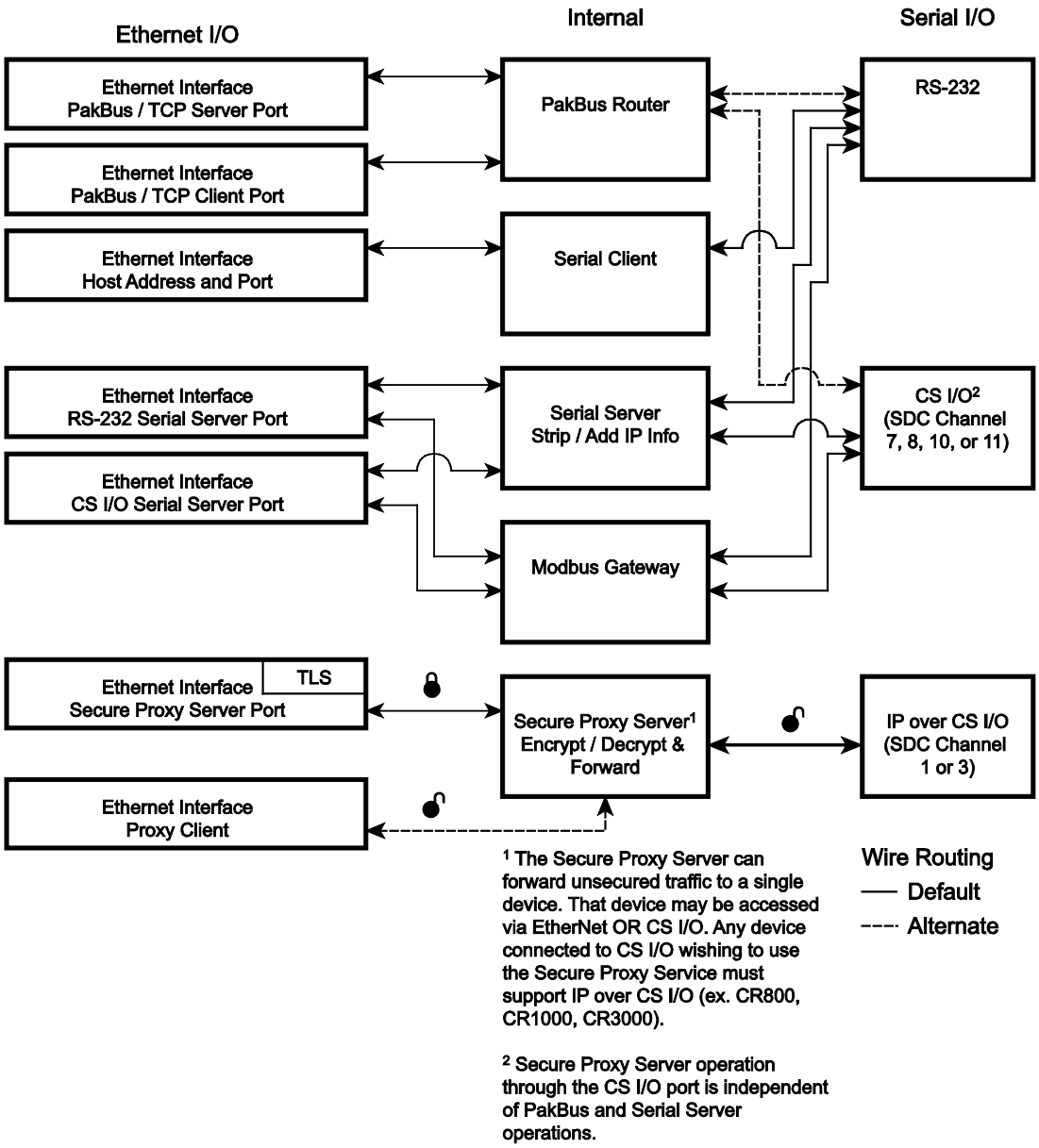


FIGURE 4-3. Bridge Mode disabled

Some reasons you might want to use each of these modes are described below. Refer to Section 6, *Configuring the NL200/201* *(p. 10)*, and Section 7, *Operation* *(p. 12)*, for information on setting up your NL200/201 for each mode.

Campbell Scientific's *LoggerNet* software is used to communicate with the dataloggers once the NL200/201 is configured properly and connected to a network.

Bridge Mode

- Allows access to datalogger's internal IP functionality when a peripheral port is not accessible. For example, accessing the HTTP/webpage, email, and FTP capabilities of a CR800/850, ET107, RAWS, or CS110.

Serial Server

- Allows access to a CR10X over Ethernet (RS-232 serial server) when used in conjunction with an RS-232 to CS I/O (ME) adapter like the SC32B or SC105.
- Allows access to a serial sensor over Ethernet (RS-232 serial server).
- Provides an Ethernet to RF500M Base. (RS-232 serial server).

PakBus® Router

- Allows access to a CR10X-PB over Ethernet.
- Allows access to a CR200X over Ethernet.
- Allows you to connect to a PakBus® Device on the RS-232 port and a PakBus Device on the CS I/O port using only one TCP port.
- Allows a PakBus® device on the RS-232 port and a PakBus device on the CS I/O port to communicate with each other without routing through the Ethernet.
- Allows multiple computers to concurrently talk to PakBus® devices connected to the RS-232 and CS I/O ports.

TLS Proxy Server

- Adds an encrypted Ethernet network interface to a datalogger that supports CS I/O IP (bridge mode) communications.

5. Specifications

General

177 g (6.3 oz)
16 x 6.73 x 2.54 cm (6.3 x 2.65 x 1 in)

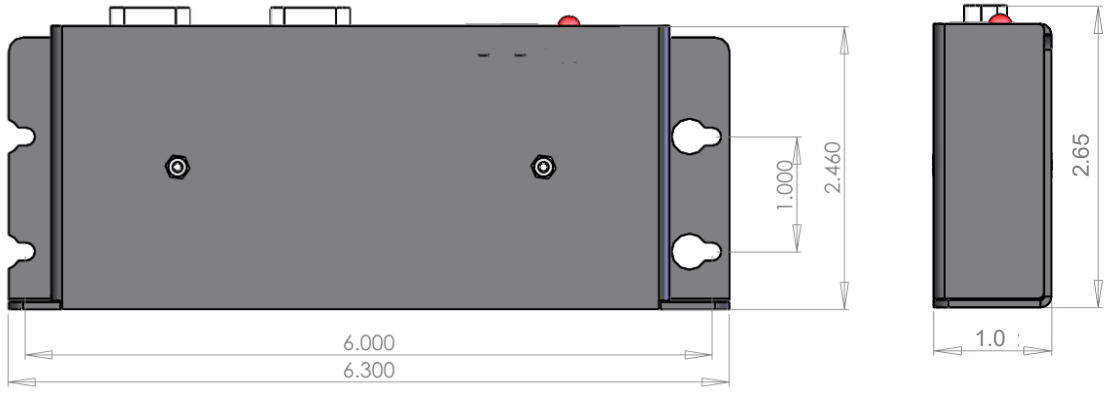


FIGURE 5-1. NL200/201 dimensions in inches

Power Input

NL201: CS I/O or barrel connector jack; not powered over USB
NL200: Barrel connector jack; not powered over CS I/O or USB

Power Requirements

7 to 20 Vdc
600 mW active, 24 mW standby

NOTE

Standby power is when the IPNetPower instruction has been used to turn off power to the Ethernet. See the CRBasic help for an example of using the IPNetPower instruction. Note that the IPNetPower instruction is only applicable when the NL200/201 is configured with Bridge Mode Enabled.

Operating Temperature

Standard: –25 to +50 °C
Extended: –55 to +85 °C

Configuration

DevConfig over USB or Ethernet
Telnet console over Ethernet
Terminal menu over RS-232

CS I/O Port

SDC 7, 8, 10, 11 (does not support ME)
9600 bps to 460.8 kbps

RS-232 Port

DTE
1200 bps to 115.2 kbps

Ethernet

10Base-T (full and half duplex), 100Base-TX (full and half duplex), Auto-MDIX
Auto-IP (APIPA), IPv4, IPv6, ICMP/Ping, ICMPv6/Ping, TCP, DHCP Client, SLAAC, DNS Client, HTTPS Proxy, Telnet Server, TLS, PakBus®, Modbus TCP/IP

Miscellaneous

Supports 50 simultaneous TCP connections
Up to 10 of the 50 TCP connections can be used for TLS
PakBus® router supports 50 routes
Supports up to 15 concurrent Modbus server transactions

Compliance

View the EU Declaration of Conformity at: *www.campbellsci.com/nl201*

6. Configuring the NL200/201

The NL200/201 is configured using *DevConfig*. You can connect your NL200/201 to *DevConfig* using either a network connection or USB.

6.1 Configuring the NL200/201 via USB

NOTE INSTALL the DEVICE DRIVER BEFORE plugging the NL200/201 into your PC for the first time. You will need the device driver properly installed before you can connect to the NL200/201 via USB.

To install the device driver, download the latest version of *DevConfig* from our website. Under Device Type, select Network Peripheral | NL200 Series. Click the "Install the device driver for the device" link and follow the prompts.

- Ensure the NL200/201 is powered.
- Connect the supplied USB cable between a USB port on your computer and the USB port on the NL200/201.
- Open *DevConfig*.
- Under **Device Type**, select **NL200**.
- Click the **Browse** button next to **Communication Port**.
- Select the port labeled **NL200**.
- Click **OK**.
- Click **Connect**.
- Configure the NL200/201 as needed for your application.
- Click **Apply** to save your changes.

6.2 Configuring the NL200/201 via Network Connection

NOTE The NL200/201 must have an IP address before connecting via a network connection. If the address cannot be obtained via DHCP, you will need to configure your NL200/201 via USB the first time it is set up.

- Ensure the NL200/201 is powered and connected to your network.
- Launch *DevConfig*.
- Under **Device Type**, select **NL200**.
- Check the box labeled **Use IP Connection**.

- Click the **Browse** button next to **Communication Port**.
- Select the NL200/NL201 to be configured from the resulting pop-up window.
- Enter **nl200** in the **Administrative Password** box. (**nl200** is the default administrative password. It can be changed via the *DevConfig* Deployment/NL200 tab.)
- Click **OK**.
- Click **Connect**.
- Configure the NL200/201 as needed for your application.
- Click **Apply** to save your changes.

6.3 Configuring the NL200/201 via Telnet

NOTE The NL200/201 must have an IP address before connecting via Telnet. Configuration via Telnet is not available in bridge mode.

- Ensure the NL200/201 is powered and connected to your network.
- Create a Telnet session with the device over port 23.
- Input the NL200/201 administrative password (default password is nl200).
- Type **help** to see a list of the functionality available when connected to the NL200/201 through Telnet.
- Type **edit** and press Enter to edit the settings of the NL200/201.
- As each NL200/201 setting is shown, press Enter to accept the current value shown in parenthesis. Type a new value and press Enter to change the value. The up and down arrow keys on your keyboard can also be used to navigate through the settings.
- After progressing through all of the NL200/201 settings, type **save** to accept the changes or **cancel** to discard the changes.
- Type **bye** to exit Telnet.

6.4 Configuring the NL200/201 via RS-232

NOTE Accessing the configuration terminal menu via RS-232 requires the NL200/201 to be power cycled, so physical access to the device will be required. A null modem serial cable will be needed; one is not provided with the NL200/201.

- Using a null modem serial cable, connect your computer's serial port to the port labeled "RS-232" on the NL200/201.

- Connect to the NL200/201 using a terminal emulator. *DevConfig's* "unknown" device type or HyperTerminal are examples of simple terminal emulators. The default settings for this interface are 115200 baud, 8 data bits, no parity, 1 stop bit, no flow control.
- Power cycle the NL200/201 and repeatedly press Enter at the terminal.
- Type **help** to see a list of the functionality available when connected to the NL200/201 through Telnet.
- Type **edit** and press Enter to edit the settings of the NL200/201.
- As each NL200/201 setting is shown, press Enter to accept the current value shown in parenthesis. Type a new value and press Enter to change the value.
- After progressing through all of the NL200/201 settings, type **save** to accept the changes or **cancel** to discard the changes.
- Disconnect your computer and power cycle the NL200/201.

7. Operation

This section describes how to configure your NL200/201 for different operational modes. See Section 4, *Overview* *(p. 5)*, for help in determining which mode to use.

7.1 PakBus® Router

When the RS-232 or CS I/O port is configured as a PakBus® router, the NL200/201 can route packets to other devices in the network that it has in its routing table. These are devices that the NL200/201 has learned about through beaconing or allowed-neighbor lists.

Beacon Interval – Devices in a PakBus® network may broadcast a hello-message to other devices in order to determine "neighbor" devices. Neighbor devices are devices that can be communicated with directly by the current device without being routed through an intermediate device. A beacon in a PakBus network helps to ensure that all devices in the network are aware of which other devices are viable in the network. The beacon interval determines how often a beacon will be sent out. Set the beacon interval to 0 to disable beacons.

Verify Interval – This interval, in seconds, determines the rate at which the NL200/201 will attempt to start a hello transaction with a neighbor if no other communication has taken place within the interval. If Verify Interval is set to 0, the verify interval becomes 2.5 times the Beacon Interval. If both the Beacon Interval and Verify Interval are set to 0, the verify interval becomes 300 seconds.

PakBus Neighbors Allowed – You can set a list of "acceptable neighbors" which the NL200/201 expects to hear from within set intervals (the **Verify Interval**). If the NL200/201 does not hear from neighbors in this list within the Verify Interval, it will attempt to contact them on its own. It will ignore all devices it hears that are not on the PakBus Neighbors Allowed list except if the

PakBus® address is ≥4000. Hellos from devices with PakBus address ≥4000 are automatically accepted as neighbors.

7.1.1 Physical Setup

Using the supplied serial cable, connect the NL200/201's CS I/O port or RS-232 port to the datalogger's CS I/O or RS-232 port, respectively. The NL201 will be powered if connected via CS I/O. Alternatively, power the NL200 or NL201 through the barrel-connector jack located on the edge of the device. Connect the NL200/201 to your network using an Ethernet cable, attaching one end of the cable to the NL200/201's Ethernet port and the other end to your network. Ensure that the device is powered up by inspecting the Power LED.

7.1.2 Configuring the NL200/201

RS-232 PakBus® Router

- Connect to the NL200/201 in *DevConfig* (see Section 6, *Configuring the NL200/201 (p. 10)*).
- On the NL200 tab:
  - Set **Bridge Mode** to **disable**.
- On the RS-232 tab:
  - Set **Configuration** to **PakBus**.
  - Set **Baud Rate** to baud rate of attached device.
  - Set **Beacon Interval**, **Verify Interval**, and **PakBus Neighbors Allowed** as described above. Often the default values can be used. However, an allowed neighbors list can be useful in restricting communication paths.
- On the Network Services tab:
  - Make note of the **PakBus\TCP Server Port**. (The default **PakBus/TCP Server Port** is 6785. Unless firewall issues exist, it is not necessary to change the port from its default value.)

CS I/O PakBus® Router

- Connect to the NL200/201 in *DevConfig* (see Section 6, *Configuring the NL200/201 (p. 10)*).
- On the NL200 tab:
  - Set **Bridge Mode** to **disable**.
- On the CS I/O tab:
  - Set **Configuration** to **PakBus**.

- Set **SDC address**. (Note that if multiple peripherals are connected to a datalogger's CS I/O port, each must have a unique SDC address.)
- Set **Beacon Interval** and **Verify Interval** as described above. Often the default values can be used.

- On the Network Services tab:
  - Make note of the **PakBus\TCP Server Port**. (The default **PakBus/TCP Server Port** is 6785. Unless firewall issues exist, it is not necessary to change the port from its default value.)

7.1.3 *LoggerNet* Setup

- In the *LoggerNet Setup* screen, press **Add Root** and choose **IPPort**. Input the NL200/201's IP address and port number. The IP address and port number are input on the same line separated by a colon.
- Add a PakBus® Port (PakBusPort).
- Add a PakBus® Router (pbRouter). Input the PakBus address of the NL200/201. The NL200/201's default PakBus address is 678.
- Add the datalogger and input the PakBus® address of the datalogger.
- Press **Apply** to save the changes.

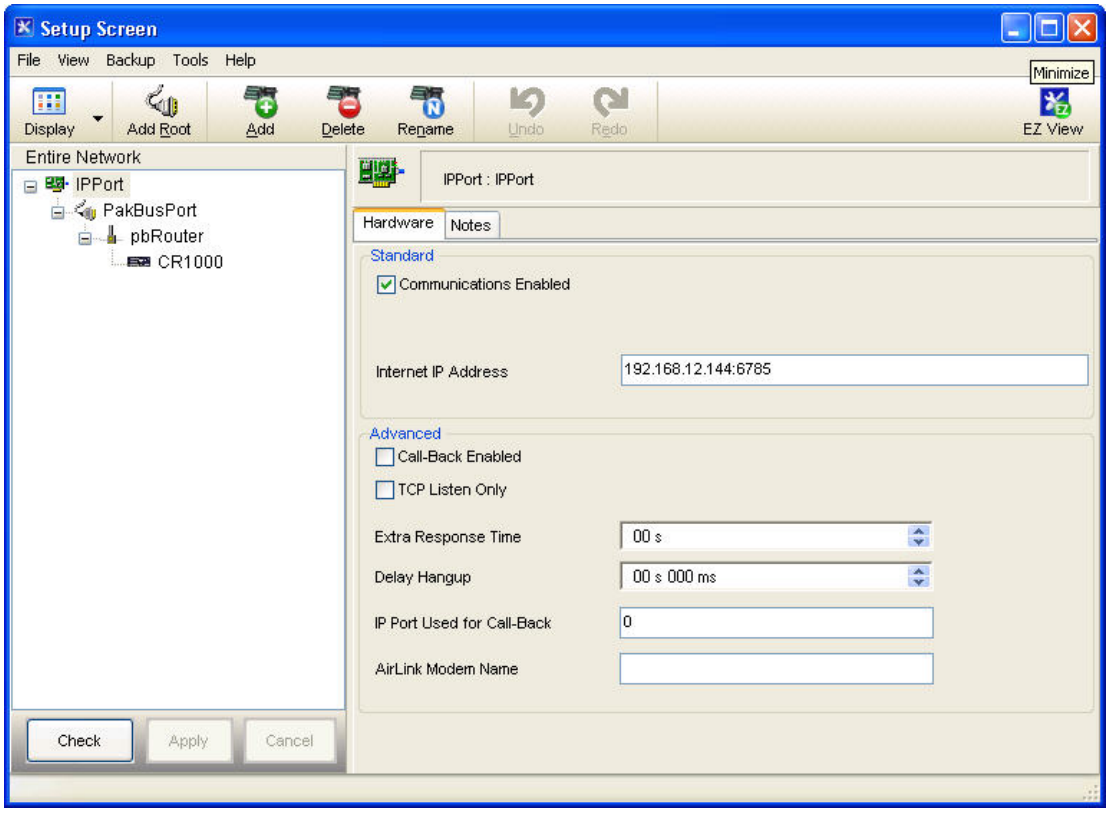


FIGURE 7-1. PakBus® router LoggerNet setup

7.1.4 Connect

You are now ready to connect to your datalogger using the *LoggerNet Connect* screen.

7.2 Bridge Mode

With Bridge Mode Enabled, the device will act as a bridge from Ethernet to CS I/O. All IP packets that come into the device via Ethernet will be communicated as a complete Ethernet/TCP packet to the datalogger over the CS I/O port. This enables the datalogger to use its TCP/IP stack to interpret the packet and, therefore, all of the datalogger's TCP services are available. In bridge mode, none of the other device settings are valid and all other functionality is disabled. All settings (that is, IP, netmask, gateway) are configured in the datalogger. However, in bridge mode, the device will intercept any TCP traffic on the "TCP Configuration Port Number." This allows the device to still be configured remotely by IP connection using *DevConfig*. The "TCP Configuration Port Number" is a user setting with a default value of 6786.

7.2.1 Physical Setup

Using the supplied serial cable, connect the NL201's CS I/O port to the datalogger's CS I/O port. Alternatively, power the NL200 or NL201 through the barrel-connector jack located on the edge of the device. (Note that an NL200 cannot be powered over CS I/O. An external power adaptor or power cable is required.) Connect the NL200/201 to your network using an Ethernet cable, attaching one end of the cable to the NL200/201's Ethernet port and the other end to your network. Ensure that the device is powered up by inspecting the Power LED.

7.2.2 Configuring the NL200/201

Connect to the NL200/201 in *DevConfig* (see Section 6, *Configuring the NL200/201* *(p. 10)*). In the NL200/201 tab, set **Bridge Mode** to **enable**.

7.2.3 Configuring the Datalogger

- Connect a serial cable from the PC COM port to the datalogger's RS-232 port.
- Open *DevConfig*. Select the device type of the datalogger (CR800, CR1000, or CR3000), the appropriate **Communication Port**, and the **Baud Rate**. Press **Connect** to connect to the datalogger.
- If using a static IP address, select the CS I/O IP tab and input the IP address, subnet mask, and IP gateway for the correct CS I/O Interface. The default for the NL200/201 is **CS I/O IP Interface #1** (SDC3). DNS server settings are shared by all active IP interfaces and can be entered on the TCP/IP tab. These values can be provided by your network administrator. If using DHCP, leave the CS I/O IP address settings as 0.0.0.0. You will find the information acquired by DHCP in the info box on the **CS I/O IP** tab. The same info box can be seen on the **Ethernet** tab.
- Press **Apply** to save the changes and then close *DevConfig*.

NOTE The NL200/201 must be connected to the datalogger before configuring the datalogger with *DevConfig*. If it is not connected, the TCP/IP settings will not be displayed.

7.2.4 *LoggerNet* Setup

The next step is to run *LoggerNet* and configure it to connect to the datalogger via the Ethernet port. (See example in FIGURE 7-2 below.)

- In the *LoggerNet Setup* screen, press **Add Root** and choose **IPPort**. Input the datalogger's IP address and port number. The IP address and port number are input on the same line separated by a colon. (The datalogger's default port number is 6785. It can be changed using *DevConfig*. Unless firewall issues exist, the port number does not need to be changed from its default value.)
- Add a PakBus® Port.
- Add the datalogger (CR800, CR1000, or CR3000) and input the PakBus® address of the datalogger.
- You can verify that your settings are correct by selecting the datalogger in the Network Map, selecting the Clock tab, and pressing **Check Clocks**. If your settings are correct, you should see the current clock of your server and datalogger.

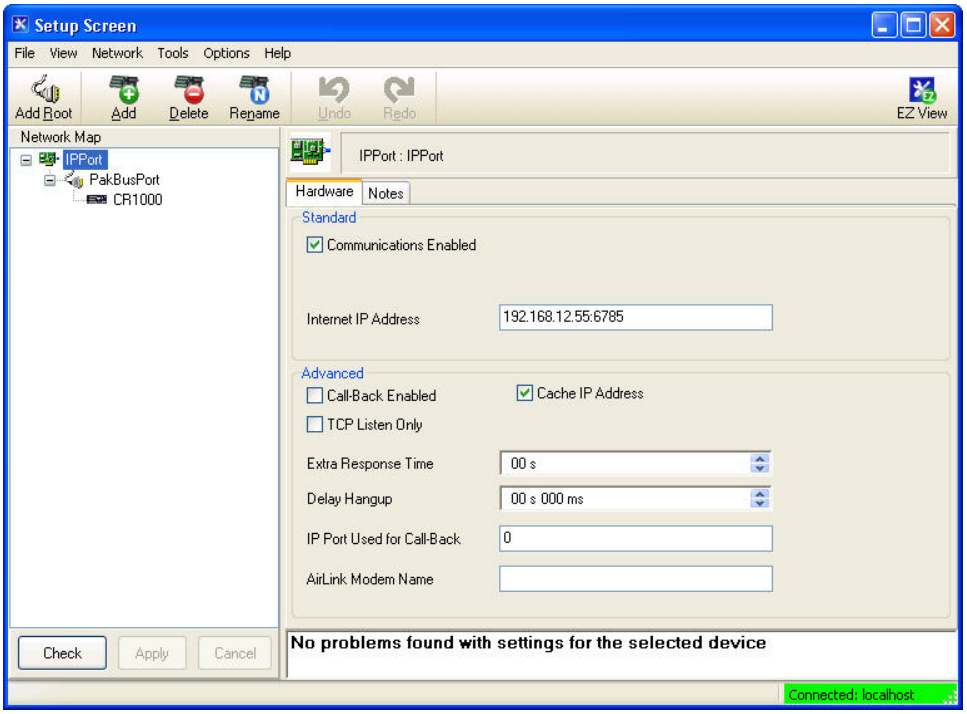


FIGURE 7-2. Bridge mode LoggerNet setup

7.2.5 Connect

You are now ready to connect to your datalogger using the *LoggerNet Connect* screen.

7.3 TCP Serial Server

The NL200/201 can tunnel RS-232 and CS I/O serial communications over Ethernet. Any packet sent to the configured Ethernet IP port will have the IP layer removed, and the serial data is then directed to the serial connection.

7.3.1 Physical Setup

Using the supplied serial cable, connect the NL200/201's CS I/O port or RS-232 port to the datalogger's CS I/O or RS-232 port, respectively. The NL201 will be powered if connected via CS I/O. Alternatively, power the NL200 or NL201 through the barrel-connector jack located on the edge of the device. Connect the NL200/201 to your network using an Ethernet cable, attaching one end of the cable to the NL200/201's Ethernet port and the other end to your network. Ensure that the device is powered up by inspecting the Power LED.

7.3.2 Configuring the NL200/201

RS-232 Serial Server

- Connect to the NL200/201 in *DevConfig* (see Section 6, *Configuring the NL200/201* *(p. 10)*).
- On the NL200 tab:
  - Set **Bridge Mode** to **disable**.
- On the RS-232 tab:
  - Set **Configuration** to **TCP Serial Server**.
  - Set **Baud Rate** to baud rate of attached device.
  - Make note of the **Serial Server Port**. (The default **RS-232 Serial Server Port** is 6784. Typically, it is not necessary to change this entry from its default.)

CS I/O Serial Server

- Connect to the NL200/201 in *DevConfig* (see Section 6, *Configuring the NL200/201* *(p. 10)*).
- On the NL200 tab:
  - Set **Bridge Mode** to **disable**.

- On the CS I/O tab:
  - Set **Configuration** to **TCP Serial Server**.
  - Set **SDC Address**. (Note that if multiple peripherals are connected to a datalogger's CS I/O port, each must have a unique SDC address.)
  - Make note of the **Serial Server Port**. (The default **CS I/O Serial Server Port** is 6783. Typically, it is not necessary to change this entry from its default.)

7.3.3 *LoggerNet* Setup

The next step is to run *LoggerNet* and configure it to connect to the datalogger via the Ethernet port. (See example in FIGURE 7-3 below.)

- In the *LoggerNet Setup* screen, press **Add Root** and choose **IPPort**. Input the NL200/201's IP address and port number. The IP address and port number are input on the same line separated by a colon.
- Add a PakBus® Port.
- Add the datalogger and input the PakBus® address of the datalogger.
- Press **Apply** to save the changes.
- You can verify your settings are correct by selecting the datalogger in the Network Map, selecting the Clock tab, and pressing **Check Clocks**. If your settings are correct, you should see the current clock of your server and datalogger.

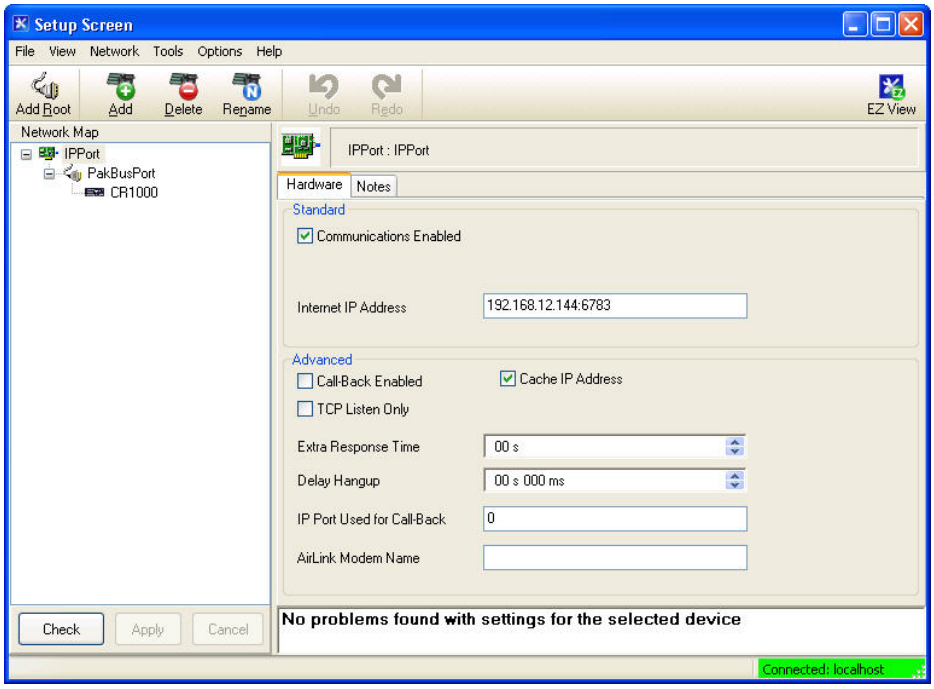


FIGURE 7-3. Serial server LoggerNet setup

7.3.4 Connect

You are now ready to connect to your datalogger using the *LoggerNet Connect* screen.

7.3.5 Serial Sensors

The NL200/201 configured as an RS-232 serial server as described above can be used to communicate with a serial sensor. However, *LoggerNet* is not capable of communicating with the serial sensor. You must have some other method of communicating with the sensor.

7.4 TCP Serial Client

When the RS-232 port is configured as **TCP Serial Client**, the NL200/201 will initiate and maintain a TCP socket connection to the IP address and port number specified by the **Serial Client Address** and **Serial Client Port** settings. Data received on the RS-232 port will be forwarded to this TCP connection, and data received on the TCP connection will be forwarded to the RS-232 port. This mode can be particularly useful when an RF base or serial sensor is behind a firewall and needs to be the party responsible for initiating the TCP socket connection to the data collection server.

The NL200/201 will attempt to open a connection with the remote server, and, if the connection fails to open, the device will continue to retry at an interval of 60 seconds. If data arrives on the RS-232 port when no TCP connection exists, the device will buffer the data (up to 1500 bytes) and immediately attempt to open a connection to deliver the data. If the remote server closes the connection due to error, the NL200/201 will make a best effort to save any data that was in process and re-queue it to be sent on the next successfully-opened TCP connection.

7.5 Modbus TCP/IP to RTU Gateway

The NL200/201 can serve as a Modbus TCP/IP to RTU Gateway. It will listen for incoming Modbus TCP/IP connections from a Modbus TCP/IP master client. The port number of the listening connection is specified in the **RS-232 Service Port Number** setting and is typically set to a value of 502. The NL200/201 will convert incoming Modbus TCP/IP frames to Modbus RTU and forward them to the RS-232 port. The NL200/201 will wait for a response from the Modbus RTU device and forward that response back to the remote Modbus TCP/IP master client over the established TCP connection. The Modbus RTU device is generally a datalogger, such as a CR200(X), connected to the RS-232 port or a datalogger located remotely over a transparent radio (for example, RF450) connection, but can be any Modbus RTU device. When the NL200/201 is connected directly to a CR800 series, CR1000, or CR3000 being polled by a Modbus TCP/IP master client, the NL200/201 is most commonly configured with Bridge Mode enabled instead of as a Modbus TCP/IP to RTU Gateway.

7.6 TLS

The NL200/201 supports transport layer security (TLS) for proxy functions including HTTPS. TLS versions 1.0 and 1.1. are supported. The TLS implementation supports symmetric algorithms AES-256, AES-128, and RC4 and RSA keys up to 4096 bits. For any TLS connection, the unit will

preferentially use AES-256, then AES-128, and finally RC4. X.509 certificates are supported, with the exception of v3 extensions. Certificates should be PEM format. Up to 10 certificates can be chained. 20 KB of space is provided for certificate storage. The Private Key should also be in PEM format and, if encrypted, use AES-256 or AES-128 (SHA).

The implementation of TLS in the NL200/201 is provided so that secure, encrypted communications can be established between a TLS client and the NL200/201. With the TLS Proxy Server enabled, the NL200/201 can act as a TLS proxy server for a datalogger. The NL200/201's TLS Proxy Server maintains a secure TLS connection with a remote TLS client and forwards data onto a datalogger using a standard TCP connection thus enabling communication with TLS clients. The TLS client can be a web browser using HTTPS or other user-supplied TLS client. This offloads from the datalogger the intensive computations that are necessary for a TLS server to perform.

Also, with the NL200/201 configured for TLS, it can establish a secure TLS configuration session with *DevConfig*.

In order to use TLS, the user must configure the NL200/201 with a user-supplied TLS Private Key and TLS Certificate. The key and certificate are loaded using *DevConfig*.

Using *DevConfig*, navigate to the Settings Editor tab and then to the TLS tab.

- Load the user-supplied, PEM-formatted TLS Private key using the **Set TLS Key …** button. A file dialog will open. Navigate to the key file and click **Open**.
- Load the user-supplied, PEM-formatted TLS Certificate using the **Set TLS Certificate …** button. A file dialog will open. Navigate to the certificate file and click **Open**.
- Enter the **TLS Private Key Password** if the TLS Private Key is encrypted. Otherwise, leave the setting blank.
- After loading the key and certificate, click the **Apply** button. The NL200/201 will reboot. Connect with *DevConfig* again and navigate to the Settings Editor tab and then to the TLS tab. The **TLS Status** should say **Initialized**.

NOTE The TLS Settings described above cannot be edited over a standard TCP *DevConfig* link. The TLS Private Key, TLS Private Key Password and TLS Certificate can only be edited/transmitted over a secure *DevConfig* link (USB or TLS).

NOTE If the status of the TLS stack is **Initialized**, the NL200/201 will automatically negotiate a secure TLS connection with *DevConfig* as long as the **Use IP Connection** option is selected.

7.6.1 TLS Proxy Server

A TLS proxy server is a device that acts as a secure intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, web page, or other resource, available from a different server. The proxy server evaluates the request according to its filtering rules. For example, it may filter traffic by IP address or protocol. If the request is validated by the filter, the proxy provides the resource by connecting to the relevant server and requesting the service on behalf of the client.

When the TLS Proxy Server function is enabled, the NL200/201's TLS Proxy Server maintains a secure TLS connection with a remote TLS client and forwards data onto a datalogger using a standard TCP connection thus enabling communication with TLS clients. The TLS client can be a web browser using HTTPS or other user-supplied TLS client. Any other client program that encrypts a standard TCP connection using TLS may be used to establish a connection with the NL200/201 TLS Proxy Server and the NL200/201 will forward unencrypted TCP data to a datalogger. In this way, a remote TLS client can establish a TLS connection with a datalogger.

The settings found in the TLS Proxy Server and TLS tab in *DevConfig* are used to configure the NL200/201 TLS Proxy Server.

Two physical configurations are possible and the required settings differ depending on the configuration chosen. The possible configurations are shown in the following figure.

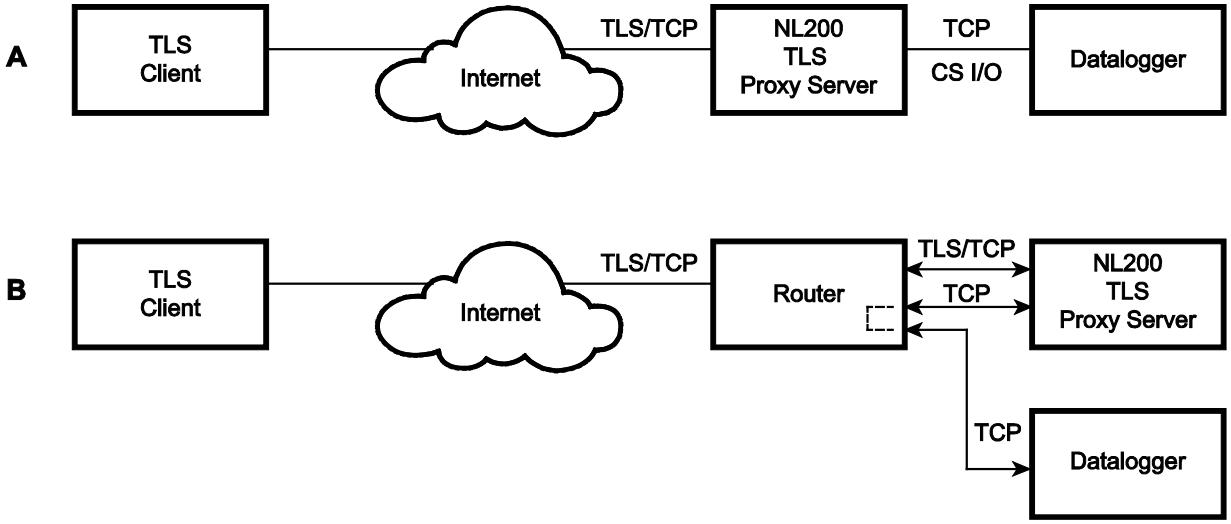


FIGURE 7-4. TLS proxy server configurations

Configuration A

In Configuration A, the NL200/201 decrypts TLS traffic and forwards the unencrypted TCP traffic to the datalogger over the CS I/O port. The NL200/201 is able to "learn" the IP address of the attached datalogger and will open a TCP connection on the "learned" IP address.

Configuration B

In Configuration B, the NL200/201 decrypts TLS traffic and forwards the unencrypted TCP traffic to the datalogger back out on the Ethernet port. The user must specify an IP address and TCP port number for the forwarding TCP connection.

To configure the NL200/201 TLS Proxy Server to communicate with a datalogger attached to the CS I/O port or with a datalogger over an Ethernet connection, open *DevConfig* and configure the following settings.

Settings Editor | TLS Proxy Server Tab

- Set the **TLS Proxy Server** setting to **enable**.

- Set the **TLS Proxy Server Port Number**. This is the TCP port number on which the proxy server will listen for incoming connections. The TLS Client also needs to be set to communicate on this port number. When TLS communications are received on this port number, the NL200/201 will decrypt the data and attempt to open a TCP connection to the datalogger and forward the unencrypted data. In HTTPS communications, web browsers use port 443. The NL200/201 will always listen on port 443 regardless of the value of this setting. Therefore, if HTTPS communications are desired, it is unnecessary to configure this setting.

- Set the **TLS Proxy Forward Physical Port** to **CS I/O Port** for Configuration A or to **Ethernet Port** for Configuration B.

- For Configuration A, leave the **TLS Proxy Forward IP Address** set to 0.0.0.0. For Configuration B, enter the datalogger's IP address in the **TLS Proxy Forward IP Address** setting. This address must be configured in the datalogger. It must be a unique, static IP address on the same subnet as the NL200/201 IP address. For example, if the NL200/201 IP address is 192.168.5.1 with subnet 255.255.255.0, a valid IP address for the datalogger would be 192.168.5.2 provided there are no other devices on the subnet with that address.

- Set the **TLS Proxy Forward Port Number**. This is the TCP port number that the proxy server will use when it opens a TCP connection to the datalogger to forward unencrypted data. The datalogger's TCP server port must be set to communicate on this port number. The default value for the datalogger's PakBus/TCP server is 6785, so this setting can likely be left at the default. The datalogger listens for HTTP traffic on port 80. The NL200/201 will always forward TLS traffic received on port 443(HTTPS) to port 80(HTTP) regardless of this setting. Therefore, if HTTPS communications are desired, it is unnecessary to configure this setting.

- It is recommended to leave the **TLS Proxy Timeout** set to **90** seconds although it can be changed if desired. This will determine how fast the NL200/201 proxy server and client connections will timeout if no activity is detected.

To configure the datalogger for Configuration A, connect to the datalogger using *DevConfig* and select the CS I/O IP tab. Set the **CS I/O Interface IP Address** to a static IP address. Use the datalogger's CS I/O Interface that

corresponds to the NL200/NL201's **CS I/O IP Interface Identifier** setting. To configure the datalogger for Configuration B, connect to the datalogger using *DevConfig* and select the TCP/IP tab. Set the **Ethernet Interface IP Address** to a static IP address.

For either configuration, the IP address must not be 0.0.0.0, and it must be unique on the same subnet as the NL200/201 IP address. For example, if the NL200/201 IP address is 192.168.5.1 and Subnet Mask is 255.255.255.0, the datalogger address could be set as 192.168.5.2 provided there are no other devices on the subnet with that address. Also set the datalogger's Subnet Mask to match that of the NL200/201.

The datalogger must be listening on the same TCP port that the NL200/201 is configured to forward TCP traffic on (NL200/201 setting: TLS Proxy Forward Port Number). The datalogger always listens on port 80 for HTTP, therefore, no TCP port configuration is necessary for using HTTP.

7.6.2 *DevConfig* TCP Encrypted Communication to the NL200/201

In order to use *DevConfig* TCP Encrypted Communication to the NL200/201, you will need to load your TLS Private Key and TLS Certificate into the NL200/201. This is done from the Settings Editor | TLS tab in *DevConfig*. Once the private key and certificate are loaded successfully, the TLS Status field should read **Initialized**.

To use TCP Encrypted Communication, select the **Use IP Connection** check box in *DevConfig*. Input the NL200/201's **IP address** (or press the browse button to select it from a list of NL200/201s connected to the network) and press **Connect**.

NOTES

If the status of the TLS stack is **Initialized**, the NL200/201 will automatically negotiate a secure TLS connection with *DevConfig* as long as the **Use IP Connection** option is selected.

Encrypted Communication is required to change the TLS Private Key and/or TLS Certificate via TCP. The private key and certificate cannot be initialized via TCP, since the connection is not encrypted. They must be initialized through a direct USB connection to the NL200/201.

When the NL200/201 is in bridge mode, it cannot be configured via a secure network connection, because in bridge mode the TLS stack is not initialized. It can be configured via USB, RS-232, or an unsecured network connection.

8. Applications

8.1 Working Around Firewalls

The NL200/201 can be used to provide a connection between *LoggerNet* and a datalogger when both are behind firewalls. The NL200/201 must be on a public IP address and will act as a common meeting place for all PakBus® communications.

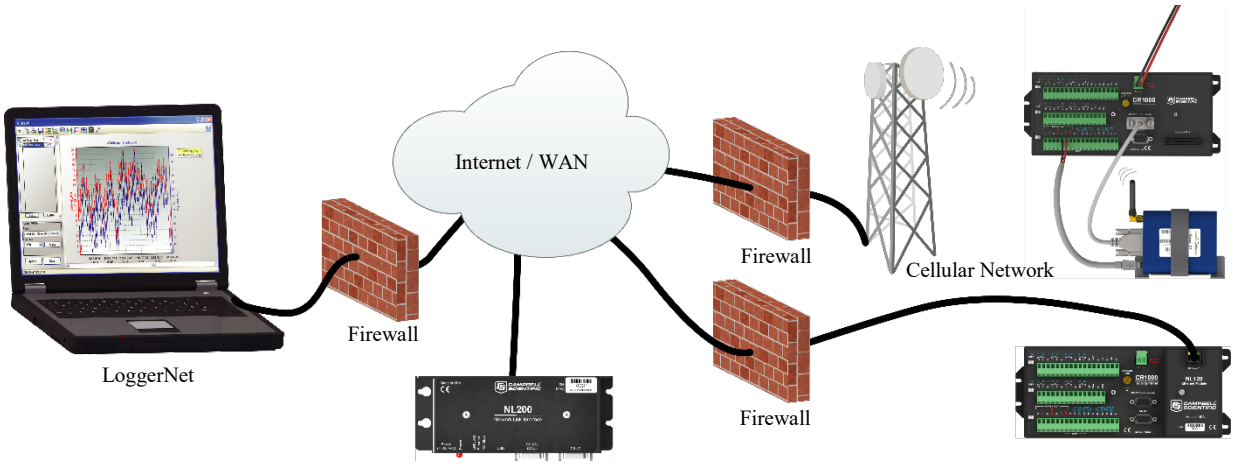


FIGURE 8-1. Working around firewalls

8.1.1 Configuring the NL200/201

- Connect to the NL200/201 in *DevConfig* (see Section 6, *Configuring the NL200/201* (p. 10)).
- On the NL200 tab:
  - Set **Bridge Mode** to **disable**.
  - Set **Use DHCP** to **disable**.
  - Input the **IP Address**, **Network Mask**, and **Default Gateway**. These values can be provided by your network administrator.
- On the Network Services tab:
  - Make note of the **PakBus/TCP Server Port**.

8.1.2 Configuring the Datalogger

NOTE The datalogger must first be configured for internet communication (i.e., through an NL115, an NL120, a second NL200/201, or a cellular modem).

- Connect a serial cable from the PC COM port to the datalogger's RS-232 port.
- Open *DevConfig*. Select the device type of the datalogger (CR800, CR1000, or CR3000), the appropriate **Communication Port**, and **Baud Rate**. Press **Connect** to connect to the datalogger.
- On the Network Services tab:
  - Under **PakBus TCP Client Connections**, input the NL200/201's **IP address** and **PakBus TCP Server Port**.
- Press **Apply** to save the changes and then close *DevConfig*.

9. Troubleshooting

This section covers some common problems that might be encountered when using the NL200/201. This is not comprehensive but should provide some insight and ability to correct simple errors without a call to Campbell Scientific technical support.

When your Campbell Scientific software cannot establish a link to a remote datalogger that is connected to the NL200/201, do the following:

1. Check all your power connections.

   - Your NL200/201 and any hub and/or router being used must be connected to power. Check power indicator lights to make sure your devices are powered.

2. Check all your cables.

   - Verify that your Ethernet cable is securely plugged in between your NL200/201 and your hub, router, or PC. The yellow Link/Act light on the NL200/201 should start blinking when it is connected to the Ethernet.

   - If an Ethernet cable is connected but the Link/Act light is not blinking, try a new Ethernet cable. You can also try moving the existing Ethernet cable to a functioning system to determine if the cable is working.

3. Power cycle the NL200/201 and your hub/router/PC.

   - Turn off or unplug your hub/router/PC and NL200/201. Wait 10 seconds and then plug them back in or turn them on. A full restart may take 30 to 60 seconds.

4. Check the settings of the NL200/201.

   - Make sure the assigned NL200/201 IP address (DHCP or static) and the IP address of the PC you are trying to connect from are able to communicate with each other. (Your network administrator can help you with this.)

     For example, the following addresses are able to communicate:

     NL200/201: IP address: 192.168.0.2, Network Mask: 255.255.255.0

     PC: IP address: 192.168.0.3, Network Mask: 255.255.255.0

   - If you are using DHCP to assign an IP address to the NL200/201, use *DevConfig* to read the IP address assigned to your NL200/201. This is done through a USB connection to the NL200/201 while the NL200/201 is connected to your network.

   - The IP address assigned to the NL200/201 must be unique on your network.

- When Bridge Mode is enabled, the datalogger controls how the IP address is assigned. Make sure your datalogger is connected correctly to the NL200/201.

- Try to ping the NL200/201 from your PC. (From the Windows Start Menu, choose Accessories | Command Prompt. Then type **ping xxx.xxx.xxx.xxx** where xxx.xxx.xxx.xxx is the IP address of your NL200/201.) If no packets are returned, this indicates that there is no network connection to that IP address.

5. Make sure the IP address and port number entered in *LoggerNet*/*PC400*/*RTDAQ* match the settings in the NL200/201.

   - Note that PakBus® and serial server communications use different port numbers. The default port number for PakBus communications is 6785. The default port number for CS I/O serial server communications is 6783. The default port number for RS-232 serial sever communications is 6784. The correct port number must follow the IP address of the NL200/201 in *LoggerNet Setup* in order for *LoggerNet* to communicate through the NL200/201. For example, if the NL200/201 is configured as a CS I/O serial server, in *LoggerNet Setup*, enter the correct IP address of your NL200/201 followed by :6783 (e.g., 192.168.0.3:6783).

6. If you are unable to communicate with the NL200/201 via the USB cable, verify that you have installed the latest drivers for the NL200/201. These can be downloaded from our website at *www.campbellsci.com*.

7. If the NL200/201 is configured as a CS I/O serial server, verify that any other SDC device attached to the datalogger is using a different SDC address. For example, if the NL200/201 is configured for SDC7, any other device attached to the datalogger cannot use SDC7.

8. If communicating over a slow or intermittent connection, it may be necessary to lower the Maximum Packet Size of the datalogger in *LoggerNet Setup* and/or add Extra Response Time to the PakBus® Port in *LoggerNet Setup*.

9. Reset the NL200/201 to its default settings.

   - If none of the above steps correct your communication problems, reset the NL200/201 to its default settings. This can be done using the **Factory Defaults** button in *DevConfig* or by using the **Defaults** command in a telnet session with the NL200/201.

10. Verify you are running the latest revision of firmware (operating system). It is possible that an issue affecting your ability to communicate via the NL2xx is resolved in the latest version. The latest firmware version and its revision history can be found at *www.campbellsci.com/downloads*. There is no charge for this download. See Appendix D, *Sending a New OS to the NL200/201* *(p. D-1)*, for instructions on downloading the firmware revision to the NL2XX.

11. If the above steps do not resolve the issue, please call Campbell Scientific, for help. Before calling, it would be helpful to do the following:

    - Obtain a detailed description of your network setup including TCP/IP address, port number, PakBus® settings, and other pertinent information regarding all of the devices in the NL200's communication network.

    - Save a copy of the NL2xx settings (in XML format) using *DevConfig*.

    - Save a copy of the NL2XX event log. This is low-level code that can be used by Campbell Scientific's engineering staff to help troubleshoot the NL2XX. To obtain the event log, the NL2XX must not be in Bridge Mode. Telnet into the NL2XX using your favorite telnet program. Once you have logged in, type "eventlog" at the prompt. Record the date and time that you did this. Copy and paste the output into a text file.

    - If running NL2xx firmware revision v.4 or greater, you can also type "eventloga" at the prompt to obtain an ASCII version of the low-level log. Copy and paste the output into a text file.

    - Once the eventlogs have been copied, you can type "eventlog erase" at the prompt to clear the log. If you want to add a date to indicate when the logs were last cleared, you can enter "eventlog erase date" where date is a string of up to 8 characters.

After calling Campbell Scientific for help, email your network description, the newly created text files, and the saved XML settings file to the person you are working with.

10. Attributions

PakBus is a registered trademark of Campbell Scientific, Inc.

lwIP

SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Appendix A. Glossary

Auto-IP

A method of automatically assigning IP addresses to a device without the use of a DHCP server.

It is used in the NL200/NL201 when DHCP is enabled but the NL200/NL201 is not able to access a DHCP server. A local IP address is assigned in the 169.254.XXX.XXX range. This process can take up to 2 minutes.

Beacon Interval

Devices in a PakBus® network may broadcast a hello-message to other devices in order to determine "neighbor" devices. Neighbor devices are devices that can be communicated with directly by the current device without being routed through an intermediate device. A beacon in a PakBus network helps to ensure that all devices in the network are aware of which other devices are viable in the network.

Bridge (Bridging, Network Bridge)

In the context of this manual, bridging is the act of connecting two network interfaces at the data link layer. The NL200/201 acts as a semi-transparent bridge passing, without alteration, IP packets between the Ethernet and CS I/O ports.

DHCP (Dynamic Host Configuration Protocol)

A TCP/IP application protocol in which IP addresses are assigned automatically by a DHCP server. Note that an IP address obtained through DHCP is not static but is leased for a period of time set by the network administrator. The address may change, if the NL200/201 is powered down.

If DHCP is enabled but the NL200/201 is not able to access a DHCP server, an IP address will be automatically assigned via Auto-IP (APIPA). This process can take up to 2 minutes.

Hello Exchange

A communication exchange that establishes two PakBus® devices as neighbors. A hello command packet is sent by one PakBus device (A) to another device (B). Device (B) then sends a hello response (A). The receipt of that packet establishes the two devices as neighbors. Only a hello exchange can establish two devices as neighbors.

Neighbor (PakBus® Neighbor)

A device in a PakBus network that can be communicated with directly (i.e., not via a router). Every PakBus device maintains its own Neighbor List.

PakBus®

Campbell Scientific's packet-switched communications protocol. Packets of information transmitted between PakBus devices contain user data and administrative information (a header) that routing devices use to move the packets to their ultimate destination. PakBus devices examine the header information and then either remove the header (at the packet's final destination) or forward the packet to another PakBus device.

PakBus® Node

A device in a PakBus network. Each device in a network must have a unique PakBus address.

Port Number

A port number is a way to identify a specific process to which a network message is to be forwarded when it arrives at the NL200/201.

SDC (Synchronous Device Communications)

A Campbell Scientific, addressable, and synchronous communications protocol. The protocol allows multiple peripherals to be connected to the same device as long as each peripheral has a unique SDC address.

Serial Server

A serial server (also referred to as a terminal server) allows serial communication over an IP communications link.

Proxy (Proxy Server)

A device that acts as an intermediary for IP communications between two clients. In the context of this manual, the NL200/201 acts an intermediary between two or more clients requiring a secure connection (TLS) and one client requiring an unsecured connection. Communications are encrypted and decrypted as necessary for the two clients to communicate via the proxy.

TLS (Transport Layer Security)

An encryption protocol allowing secure client/server communications. A keyed, message-authentication code is used for message reliability.

Verify Interval

An interval of time that a PakBus® device uses to determine when it is time send a hello message to another device to verify that they can still communicate.

Appendix B. Cables, Pinouts, LED Function, and Jumper

B.1 CS I/O

The CS I/O cable is a 9-pin, straight-through cable with all 9 pins connected. The supplied SC12 cable (part number 16675) is recommended.

TABLE B-1. NL200/201 CS I/O Connector Pinout

Pin	Datalogger (DB9 Female) Function	Peripheral (DB9 Male) Function
1	5 VDC	Not Connected
2	SIGNAL GND	SIGNAL GND
3	RING	RING
4	RXD	TXD
5	ME	ME
6	SDE	SDE
7	CLK/HS	CLK/HS
8	12 VDC (output)	NL200: Not Connected NL201: 12 VDC (input)
9	TXD	RXD

B.2 RS-232

A DB9 female to DB9 male cable (such as Campbell Scientific part number 10873) is used to connect the NL200/201's RS-232 port to the datalogger's RS-232 port. The supplied SC12 cable can also be used. A DB9 female null modem cable (such as Campbell Scientific part number 13657) is used to connect the NL200/201's RS-232 port to a PC's RS-232 port. The RS-232 cable should be kept short when using high baud rates.

TABLE B-2. RS-232 Pinout

Pin	Datalogger (DCE, DB9 Female) Function	Peripheral (DTE, DB9 Male) Function
1	DCD	DCD
2	TXD	RXD
3	RXD	TXD
4	DTR	DTR
5	SIGNAL GND	SIGNAL GND
6	DSR	DSR
7	CTS	RTS
8	RTS	CTS
9	RING	RING

B.3 Ethernet

The Ethernet 10Base-T/100Base-TX cable should be a Category 5 or better twisted pair cable (such as Campbell Scientific part number 13658). The two active pairs are pins 1 and 2 and pins 3 and 6. Use only dedicated wire pairs (such as blue/white and white/blue, orange/white and white/orange) for the active pairs.

NOTE The maximum recommended segment length for 10BaseT and 100BaseTx networks using CAT5 cable is 100 meters. Segment length is the length of cable between the NL device and the Ethernet repeater, hub, switch, or router it is connected to.

TABLE B-3. Ethernet Pinout

Pin	Function
1	TD +
2	TD -
3	RD +
4	Not Connected
5	Not Connected
6	RD -
7	Not Connected
8	Not Connected

B.4 USB

The USB cable is the supplied USB A to micro B style cable (Campbell Scientific part number 27555). This is used only for device configuration.

TABLE B-4. USB Micro-B

Pin	Function
1	VBUS (Not Used)
2	Data -
3	Data +
4	N/C
5	GND

B.5 Power

TABLE B-5. Power In

Pin	Function
Center	7 – 20 VDC
Sleeve	Power GND

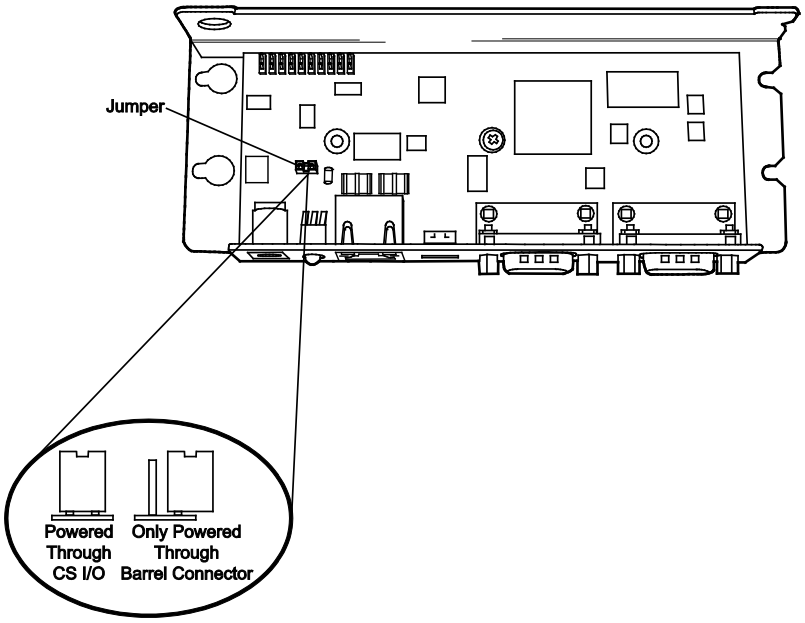
B.6 LEDs

TABLE B-6. Power LED	
State	**Description**
Off	Device powered off
On	Device powered on and ready
Blink	OS Download in progress – DO NOT DISCONNECT POWER

TABLE B-7. Ethernet LED	
State	**Description**
Yellow On	Valid Ethernet link
Yellow Off	Ethernet link not valid
Yellow Blink	Activity on Ethernet port
Green On	100Mbit/s link
Green Off	10Mbit/s link

B.7 Power Jumper (NL201 only)

If you wish to prevent the NL201 from being powered over the CS I/O port, remove the two screws on the top of the NL201, remove the NL201's top cover, remove the jumper indicated below and place it so that it is connected to only one post. With the jumper connected to only one post, the NL201 can only be powered from the barrel connector. With the jumper connected to both posts, the NL201 can be powered from the CS I/O port or from the barrel connector.



Appendix C. NL200/201 Settings

All of the NL200/201 settings available from the Settings Editor in *DevConfig* are described below.

C.1 Main Tab

Model (read only)

Model name.

Serial Number (read only)

Specifies the NL200/201 serial number assigned by the factory.

OS Version (read only)

Operating system version currently in the NL200/201.

Compile Date (read only)

Operating system compile date.

Bridge Mode

This setting is used to configure the device's mode of operation.

Bridge Mode Disabled

With Bridge Mode disabled, the serial server (RS-232 or CS I/O), PakBus®, and secure proxy server functionalities are available. Refer to the respective device settings for the configuration of these functionalities.

Bridge Mode Enabled

With Bridge Mode enabled, the device will act as a bridge from Ethernet to CS I/O. All IP packets that come in to the device via Ethernet will be communicated to a datalogger over the CS I/O port. Some filtering is done in order to minimize the amount of traffic on the CS I/O port but every packet that is transmitted to the datalogger is sent intact as a complete Ethernet/TCP packet. This enables the datalogger to use its TCP/IP stack to interpret the packet, and therefore, all of the datalogger's TCP services are available. In bridge mode, none of the other device settings are valid and all other functionality is disabled. All settings (i.e., IP, netmask, gateway) are configured in the datalogger. However, in bridge mode, the device will intercept any TCP traffic on the "TCP Configuration Port Number." This allows the device to still be configured remotely by IP connection using *DevConfig*. The "TCP Configuration Port Number" is a user setting with a default value of 6786.

NOTE When the device is configured in bridge mode, it is not possible to open a telnet session with it.

CS I/O IP Interface Identifier

When the device is configured to operate in Bridge Mode, the datalogger will address the device using this identifier. The datalogger can address up to two "CS I/O IP" devices. The corresponding CS I/O IP Address settings in the datalogger will control the interface. CS I/O IP Interface 1 uses SDC channel 3. CS I/O IP Interface 2 uses SDC channel 1.

Bridge Mode Forward Code

When the device is configured for bridge mode, it forwards Ethernet packets to the datalogger. Because the device is aware of the MAC address and IP address being used by the datalogger, it is able to do some filtering on incoming packets and only forward relevant packets. This decreases the amount of traffic on the relatively bandwidth-limited CS I/O port and minimizes the amount of Ethernet processing the datalogger needs to perform.

It may be desired to further reduce the amount of CS I/O traffic. This setting allows the filtering by the device to be customized to some degree. The default value of this setting is 65535 (0xFFFF hex) and will forward all packets that have been determined to be relevant for proper datalogger IP communication. If desired, other codes may be entered to filter out certain packet types.

A packet is forwarded to the datalogger if its corresponding bit is set in the "Bridge Mode Forward Code." It will not be forwarded if its corresponding bit is cleared. Single bits or multiple bits may be cleared to accomplish custom filtering. The following are example values of this code.

Forward Code Values

65535 (0xFFFF): Leave all bits set to forward all relevant packets.

65531 (0xFFFB): Clear bit 2 to forward all relevant packets except UDP Broadcast packets. Filtering UDP broadcasts will disable the dataloggers ability to respond to *DevConfig* discovery packets but in many cases will greatly reduce the total number of forwarded packets.

65279 (0xFEFF): Clear bit 8 to forward all relevant packets except IPv6 packets. Filtering these packets may be desired if the datalogger is on an IPv6-enabled network but not required to respond to any IPv6-related traffic.

DHCP

Enable if the device should be configured to use DHCP (Dynamic Host Configuration Protocol) to automatically acquire an IP address, subnet mask, and gateway from the local DHCP server. After DHCP is enabled, the device will reboot and it may take a few moments to acquire the IP settings. In order to see the acquired settings, you may have to refresh by pressing F5.

IP Address

The IP address uniquely identifies this node on an internet. If DHCP is disabled, a static IP address must be obtained from your network administrator for use with this device. If DHCP is enabled, the IP address obtained from the local DHCP server will be displayed in the Status window. (It is recommended to configure a static IP address.)

NOTE In bridge mode, this setting is obtained from the datalogger and cannot be edited here. It must be edited in the datalogger settings. The setting obtained from the datalogger will be displayed in the Status window.

Subnet Mask

The Subnet Mask is used to select that portion of the IP address which identifies the network. It is used to facilitate routing and should be obtained from the network administrator along with the IP address. If DHCP is enabled, the Subnet Mask obtained from the local DHCP server will be displayed in the Status window.

NOTE In bridge mode, this setting is obtained from the datalogger and cannot be edited here. It must be edited in the datalogger settings. The setting obtained from the datalogger will be displayed in the Status window.

Default Gateway

Datagrams being sent to an unknown network are routed via the Default Gateway. This entry specifies the Internet address of the Default Gateway. If no Default Gateway exists, set this entry to "0.0.0.0". If DHCP is enabled, the Default Gateway obtained from the local DHCP server will be displayed in the Status window.

NOTE In bridge mode, this setting is obtained from the datalogger and cannot be edited here. It must be edited in the datalogger settings. The setting obtained from the datalogger will be displayed in the Status window.

Name Servers

This setting specifies the addresses of up to three domain name servers that the device can use to resolve domain names to IP addresses. Note that if DHCP is used to resolve IP information, DNS addresses obtained via DHCP will override this list.

IP Info

Reports the IP address, network mask, and default gateway of the network interface. If DHCP is used, this setting will report the values configured by the DHCP server.

Ethernet Speed / Duplex Configuration

Specifies the Ethernet link speed and duplex settings.

Speed: When used as a TCP/IP serial server, the overall data-transfer speed is largely dependent on the speed of the serial port. Setting the Ethernet link speed to 100 Mbps will increase the overall data throughput rate by a relatively small amount, while setting it to 10 Mbps will conserve power.

Duplex: Setting the Duplex to "Full" allows communication in both directions simultaneously, while setting it to "Half" allows communication in only one direction at a time.

Setting the Ethernet Speed/Duplex Configuration to "Auto" will cause the NL200/201 to auto-configure to the faster of the two speeds and fastest duplex setting according to the capabilities of the network.

Admin Password

To help guard against unauthorized access to the NL200/201, it is password-protected by the Admin Password. This password will be required to gain access to the NL200/201 via *DevConfig* over TCP and telnet. The default password is nl200. If the password setting is left blank, no password is required to access the NL200/201. After settings are saved, the new password will be in effect.

TCP Configuration Port Number

The default TCP port number for configuration via TCP is 6786. This entry makes it possible for the user to change the port number used in TCP configuration if desired. Typically, it is not necessary to change this entry from its default. (range 1..65535)

C.2 RS-232 Tab

RS-232 Configuration

This setting controls which process will be associated with the RS-232 port. The following values are defined:

TCP Serial Server
The device will listen for an incoming TCP connection from a remote client. The port number of the listening connection is specified in the "RS-232 Service Port Number" setting. Data received on the TCP connection will be forwarded to the RS-232 port, and data received on the RS-232 port will be forwarded to this TCP connection.

TCP Serial Client
The device will maintain a TCP client connection with a remote server. The IP address and port number of the remote server are configured in the settings "RS-232 TCP Serial Client IP Address" and "RS-232 TCP Serial Client Port". Data received on the RS-232 port will be forwarded to this TCP connection, and data received on the TCP connection will be forwarded to the RS-232 port. The device will attempt to open a

connection with the remote server and if the connection fails to open, the device will continue to retry at an interval of 60 seconds. If data arrives on the RS-232 port when no TCP connection exists, the device will buffer up the data (up to 1500 bytes) and immediately attempt to open a connection to deliver the data. If the remote server closes the connection due to error, the device will make a best effort to save any data that was in process and re-queue it to be sent on the next successfully-opened TCP connection.

PakBus
This port uses the PakBus® protocol.

Modbus/TCP Gateway
The device will listen for incoming MODBUS/TCP connections from a remote client. The port number of the listening connection is specified in the "RS-232 Service Port Number" setting. The device will convert incoming MODBUS/TCP frames to MODBUS/RTU and forward them to the RS-232 port. The device will wait for a response from the MODBUS/RTU device and forward the response back to the remote MODBUS/TCP client over the established TCP connection.

Disabled
This port will not be used.

RS-232 Service Port Number

This setting is used when the RS-232 port is configured as a Serial Server or MODBUS/TCP gateway. To communicate with a TCP/IP server, the client application must open a socket to that server. The socket of a specific server is uniquely identified by an IP address of the host where the server is running and a port number associated with the server application on that host. This entry is where the port number of the server is set. Ensure that the client application is set to use the same port number as configured here. Most MODBUS/TCP applications use port 502. (range 1..65535)

RS-232 Baud Rate

This setting specifies the baud rate of the RS-232 port. The connected device must be set to communicate at the same baud rate.

RS-232 RTS

The NL200/201 asserts the RTS and DTR lines when doing RS-232 communications. This setting allows the user to disable the RTS line if needed so that it will not be asserted. Some hardware will not function if the RTS line is asserted, but typically, it is not necessary to change this setting from its default (enabled).

RS-232 TCP Timeout

This setting will determine how fast the device will timeout on the open TCP connection. For Serial Server and MODBUS/gateway configurations the device will close the TCP connection if no activity is detected for the timeout period. For the TCP Client configuration the device will close the TCP client connection if no activity is detected and then immediately open another connection with the remote server. This behavior helps to ensure that the

connection is functional as the device does not know the frequency or nature of the expected data. Set to 0 for no timeout (not recommended). (range 0..999) (seconds)

RS-232 PakBus Beacon Interval

This setting, in units of seconds, governs the rate at which the NL200/201 will broadcast PakBus® messages on the associated port in order to discover any new PakBus neighboring nodes. It will also govern the default verification interval if the value of the Verify Interval setting for the associated port is zero.

RS-232 PakBus Verify Interval

This setting specifies the interval, in units of seconds, that will be reported as the link verification interval in the PakBus® hello-transaction messages. It will indirectly govern the rate at which the NL200/201 will attempt to start a hello transaction with a neighbor if no other communication has taken place within the interval.

Neighbors Allowed RS-232

Example: (129,129) (1084,1084)

In the example above, nodes 129 and 1084 are assigned as neighbors to the NL200/201.

This setting specifies, for a given port, the explicit list of PakBus® node addresses that the NL200/201 will accept as neighbors. If the list is empty (the default value), any node will be accepted as a neighbor. This setting will not affect the acceptance of a neighbor if that neighbor's address is greater than 3999. The formal syntax for this setting follows:

```
neighbor    := { "(" range-begin "," range-end ")" }.
range-begin := pakbus-address. ;
range-end   := pakbus-address.
pakbus-address := number. ; 0 < number < 4000
```

RS-232 Modbus Timeout

This setting determines how long the MODBUS/TCP to MODBUS/RTU gateway will wait for an answer from the MODBUS slave device(s) attached to the RS-232 port. If no answer is received within the timeout period, the MODBUS/TCP server will reply to the MODBUS/TCP client with error code 0x0B(Target Device Failed to Respond). (milliseconds)

RS-232 TCP Serial Client IP Address

This setting specifies the IP address of the outgoing TCP Serial client connection that the device should maintain. If the connection fails, the device will retry until the connection succeeds. No entry specifies that no client connection will be made.

RS-232 TCP Serial Client Port

This setting specifies the TCP port of the outgoing TCP Serial Client connection. (range 1..65535)

C.3 CS I/O Tab

CS I/O Configuration

This setting controls which process will be associated with the CS I/O port. The following values are defined:

TCP Serial Server
The device will listen for an incoming TCP connection from a remote client. The port number of the listening connection is specified in the "CS I/O Service Port Number" setting. Data received on the TCP connection will be forwarded to the CS I/O port, and data received on the CS I/O port will be forwarded to this TCP connection.

PakBus
This port uses the PakBus® protocol.

Modbus/TCP Gateway
The device will listen for incoming MODBUS/TCP connections from a remote client. The port number of the listening connection is specified in the "CS I/O Service Port Number" setting. The device will convert incoming MODBUS/TCP frames to MODBUS/RTU and forward them to the CS I/O port. The device will wait for a response from the MODBUS/RTU device and forward the response back to the remote MODBUS/TCP client over the established TCP connection.

Disabled
This port will not be used.

CS I/O Service Port Number

To communicate with a TCP/IP server, the client application must open a socket to that server. The socket of a specific server is uniquely identified by an IP address of the host where the server is running and a port number associated with the server application on that host. This entry is where the port number of the serial server is set. Typically, it is not necessary to change this entry from its default. (range 1..65535)

SDC Address

Communication with the datalogger via the CS I/O port is done using SDC (Synchronous Device Comms). The datalogger will address the devices with which it wishes to communicate using an SDC address. The CS I/O port can be configured to respond to SDC address 7, 8, 10, or 11.

CS I/O TCP Timeout

This setting, in units of seconds, will determine how fast the device will time out on the open TCP connection. For Serial Server and MODBUS/gateway configurations, the device will close the TCP connection if no activity is

detected for the timeout period. Set to 0 for no time-out (not recommended). (range 0..999)

CS I/O PakBus Beacon Interval

This setting, in units of seconds, governs the rate at which the NL200/201 will broadcast PakBus® messages on the associated port in order to discover any new PakBus neighboring nodes. It will also govern the default verification interval if the value of the Verify Interval setting for the associated port is zero.

CS I/O PakBus Verify Interval

This setting specifies the interval, in units of seconds, that will be reported as the link verification interval in the PakBus® hello-transaction messages. It will indirectly govern the rate at which the NL200/201 will attempt to start a hello transaction with a neighbor if no other communication has taken place within the interval.

CS I/O Modbus Timeout

This setting determines how long the MODBUS/TCP to MODBUS/RTU gateway will wait for an answer from the MODBUS slave device(s) attached to the CS I/O port. If no answer is received within the timeout period, the MODBUS/TCP server will reply to the MODBUS/TCP client with error code 0x0B(Target Device Failed to Respond). (milliseconds)

C.4 Net Services Tab

Telnet

Enables/Disables the telnet service.

Telnet Port Number

The default TCP port number for the configuration monitor telnet session is 23. This entry makes it possible for the user to change the telnet session port number if desired. Typically, it is not necessary to change this entry from its default. (range 1..65535)

Telnet Timeout

This setting, in units of seconds, will determine how fast the configuration monitor telnet session will time out if no activity is detected. Set to 0 for no time-out (not recommended). (range 0..999)

Ping (ICMP)

The NL200/201 will not respond to “Ping” requests if this setting is disabled.

PakBus Address

This setting specifies the PakBus® address for this device. The value for this setting must be chosen such that the address of the device will be unique in the scope of the datalogger network. Duplication of PakBus addresses in two or more devices can lead to failures and unpredictable behavior in the PakBus

network. When a device has a neighbor list or neighbor filter setting filled in for a port, any device that has an address greater than or equal to 4000 will be allowed to connect to that device regardless of the neighbor filter.

PakBus/TCP Server Port

This setting specifies the TCP service port for PakBus® communications with the datalogger. Unless firewall issues exist, this setting probably does not need to be changed from its default value.

PakBus/TCP Password

Specifies the password that will be used to authenticate any incoming (server) or outgoing (client) PakBus®/TCP sessions. This password is used by the server to generate a challenge to any client that connects to the PakBus/TCP server port. If the client fails to respond appropriately, the connection will be terminated. If this password is blank (the default value), no such authentication will take place.

PakBus/TCP Client Address (1-4)

This setting specifies the IP address of an outgoing PakBus®/TCP client connection that the NL200/201 should maintain. If the connection fails, the NL200/201 will retry until the connection succeeds. No entry or a setting of 0.0.0.0 specifies that no client connection will be made.

PakBus/TCP Client Port (1-4)

This setting specifies the TCP port of the outgoing PakBus®/TCP client connection. Typically, it is not necessary to change this entry from its default. (range 1..65535)

PakBus Routes (read only)

This setting lists the routes that are known to the NL200/201. Each route known to the NL200/201 will be represented by the following four components separated by commas and enclosed in parentheses. The description of each component follows:

Port Number

Specifies a numeric code for the port that the router will use. It will correspond with one of the following:

0 CS I/O

1 RS-232

100 PakBus®/TCP Connection — If the value of the port number is 100 or greater, the connection is made through PakBus/TCP.

Via Neighbor Address

Specifies the address of the neighbor/router that will be used to send messages for this route. If the route is for a neighbor, this value will be the same as the address.

PakBus Address

Specifies the address that the route will reach.

Response Time

Specifies the amount of time (in milliseconds) that will be allowed for the route.

Central Routers

This setting specifies a list of up to eight PakBus® addresses for routers that are able to work as Central Routers. By specifying a non-empty list for this setting, the device will be configured as a Branch Router meaning that it will not be required to keep track of neighbors of any routers except those in its own branch. Configured in this fashion, the device will ignore any neighbor lists received from addresses in the central routers setting and will forward any messages that it receives to the nearest default router if it does not have the destination address for those messages in its routing table.

C.5 TLS Proxy Server Tab

TLS Proxy Server

Enable/Disable the TLS Proxy Server. When doing TLS proxy communications, the device's TLS server maintains a secure TLS connection with a remote TLS client and forwards information onto a datalogger using a standard TCP connection. TCP ports and physical connections are configured below.

NOTE If the TLS Proxy Server is enabled and a datalogger is connected to the CS I/O port, the datalogger will load its TCP stack in case it is required to do TCP communications. Running the TCP stack causes the datalogger to use more memory, leaving less for final storage, etc. So if TCP/TLS server capability is not required, the TLS Proxy Server should be left disabled.

TLS Proxy Server Port Number

When doing TLS Proxy communications, the NL200/201 TLS server maintains a secure connection with a remote client. If the TLS Proxy Forward Physical Port is specified to be the CS I/O port, the NL200/201 will then open a TCP connection with the datalogger over the CS I/O port and do unencrypted data transfer with the datalogger. If the TLS Proxy Forward Physical Port is specified to be the Ethernet port, the NL200/201 will open the TCP connection over Ethernet on the TLS Proxy Forward IP Address.

In order to communicate with the NL200/201 TLS server, the client application must open a socket to that server. The socket of the NL200/201 TLS server is uniquely identified by the IP address and a port number. This entry is where the port number of the NL200/201 TLS server is set.

The TLS client needs to be set to communicate on this port number. If secure communications come in on the Secure Proxy Server Port Number, the NL200/201 will attempt to open a TCP connection to the datalogger on the

Secure Proxy Forward Port Number. Also, regardless of this setting, the NL200/201 Secure Proxy Server will always listen on the secure HTTP (HTTPS) port number 443. If a secure connection is established on this port, the NL200/201 will attempt to communicate to the datalogger on the HTTP port 80. (range 1..65535)

TLS Proxy Forward Physical Port

When doing TLS Proxy communications, the NL200/201 TLS server maintains a secure connection with a remote client. If the TLS Proxy Forward Physical Port is specified to be the CS I/O port, the NL200/201 will then open a TCP connection with the datalogger over the CS I/O port and do unencrypted data transfer with the datalogger. If the TLS Proxy Forward Physical Port is specified to be the Ethernet port, the NL200/201 will open the TCP connection over Ethernet on the TLS Proxy Forward IP Address.

TLS Proxy Forward IP Address

Secure communications received on the NL200/201 TLS Server will be forwarded on a non-secure TCP connection to this IP address. If the TLS Proxy Forward Physical Port is specified to be the CS I/O port, this setting is not set by the user since the NL200/201 will obtain the IP address of the datalogger automatically. If the TLS Proxy Forward Physical Port is specified to be the Ethernet port, the forward IP address must be specified. Enter the IP address of the destination datalogger here.

TLS Proxy Forward Port Number

When doing TLS Proxy communications, the NL200/201 TLS server maintains a secure connection with a remote client. If the TLS Proxy Forward Physical Port is specified to be the CS I/O port, the NL200/201 will then open a TCP connection with the datalogger over the CS I/O port and do unencrypted data transfer with the datalogger. If the TLS Proxy Forward Physical Port is specified to be the Ethernet port, the NL200/201 will open the TCP connection over Ethernet on the TLS Proxy Forward IP Address.

In order to communicate with the connected datalogger's TCP server, the NL200/201's TCP client application must open a socket to that server. The socket of the datalogger's TCP server is uniquely identified by an IP address and a port number. This entry is where the port number of the NL200/201's TCP client is set. The datalogger's TCP server port must be set to communicate on this port number.

If secure communications come in on the TLS Proxy Server Port Number, the NL200/201 will attempt to open a TCP connection to the datalogger on the TLS Proxy Forward Port Number. Also, regardless of this setting, the NL200/201 TLS Proxy Server will always listen on the secure HTTP (HTTPS) port number 443. If a secure connection is established on this port, the NL200/201 will attempt to communicate to the datalogger on the HTTP port 80.

Leave this setting at its default unless the datalogger is expecting communications on a different port. (range 1..65535)

TLS Proxy Timeout

This setting, in units of seconds, will determine how fast the proxy server/client sessions will time out if no activity is detected. Set to 0 for no time-out (not recommended). (range 0..999)

C.6 TLS Tab

TLS Status (read only)

Specifies the current status of the TLS network stack.

NOTE If the status of the TLS stack is "Initialized", the device will automatically negotiate a secure TLS connection with *DevConfig* if the Use TCP option is selected. The TLS Private Key, Private Key Password, and TLS Certificate can only be edited/transmitted over a secure *DevConfig* link (USB or TLS). These settings cannot be edited over a standard TCP *DevConfig* link.

TLS Private Key Password

Specifies the password that is used to decrypt the TLS Private Key.

NOTE This setting can only be edited/transmitted if the *DevConfig* link is considered secure (USB or TLS). If the TLS stack has been initialized, the device will automatically negotiate a secure TLS connection with *DevConfig* if the Use TCP option is selected.

TLS Private Key

Specifies the private key (in PEM format) for the encryption stack.

NOTE This setting can only be edited/transmitted if the *DevConfig* link is considered secure (USB or TLS). If the TLS stack has been initialized, the device will automatically negotiate a secure TLS connection with *DevConfig* if the Use TCP option is selected.

TLS Certificate

Specifies the public certificate (in PEM format) for the encryption stack.

NOTE This setting can only be edited/transmitted if the *DevConfig* link is considered secure (USB or TLS). If the TLS stack has been initialized, the device will automatically negotiate a secure TLS connection with *DevConfig* if the Use TCP option is selected.

Appendix D. Sending a New OS to the NL200/201

Whenever a new operating system is released for the NL200/201, it will be available from our website, *www.campbellsci.com/downloads*.

D.1 Sending an OS via USB

Follow these steps to send the new OS to the NL200/201 via USB:

1. Using the supplied serial cable, connect the NL201's CS I/O port to the datalogger's CS I/O port. Alternatively, power the NL200 or NL201 through the barrel-connector jack located on the edge of the device.
2. Connect a USB cable between one of your computer's USB ports and the USB port on the NL200.
3. Open *DevConfig*.
4. Select the **NL200** under **Device Type**.
5. Select the appropriate **Communication Port**.
6. Go to the **Send OS** tab.
7. Press the **Start** button.
8. In the resulting dialog box, select the file that should be sent to the device as an operating system (this file should have an .obj extension) and press the **OK** button.
9. The operating system will be sent to the NL200/NL201.
10. After the file has been sent, the power LED on the NL200/NL201 will blink repeatedly while the NL200/NL201 copies the OS into its internal flash. This process takes about 10 seconds. While the LED is blinking, the NL200/NL201 is in a vulnerable state where removal of power will leave the NL200/NL201 without a valid operating system to run. DO NOT remove power until the LED stops blinking.

D.2 Sending an OS via IP

Follow these steps to send the new OS to the NL200/201 via IP:

1. Using the supplied serial cable, connect the NL201's CS I/O port to the datalogger's CS I/O port. Alternatively, power the NL200 or NL201 through the barrel-connector jack located on the edge of the device.
2. Using an Ethernet cable, connect the device to your network or directly to your computer Ethernet port. A crossover cable is not required if connecting directly to the computer.

3. Open *DevConfig*.

4. Select the **NL200** under **Device Type**.

5. Ensure that the **Use IP Connection** box is checked on the left hand panel.

6. If the administrative password of the device has been set, you will need to enter that password in the **Administrative Password** control on the left panel in order for the connection to succeed.

7. Enter the IP address or domain name address of the device in the **Communication Port** control on the left panel. If you do not know the address of the device and the device is connected to your local area network, you may be able to use the **…** button to the right of **Communication Port** to discover the list of devices on the network. Whatever address is entered, it must end with :6786 in order to connect the device configuration service.

8. Go to the **Send OS** tab.

9. Press the **Start** button.

10. In the resulting dialog box, select the file that should be sent to the device as an operating system (this file should have an .obj extension) and press the **OK** button.

11. The operating system will be sent to the NL200/NL201.

12. After the file has been sent, the power LED on the NL200/NL201 will blink repeatedly while the NL200/NL201 copies the OS into its internal flash. This process takes about 10 seconds. While the LED is blinking, the NL200/NL201 is in a vulnerable state where a removal of power will leave the NL200/NL201 without a valid operating system to run. DO NOT remove power until the LED stops blinking.

Campbell Scientific Companies

Campbell Scientific, Inc.
815 West 1800 North
Logan, Utah 84321
UNITED STATES
www.campbellsci.com • info@campbellsci.com

Campbell Scientific Canada Corp.
14532 – 131 Avenue NW
Edmonton AB T5L 4X4
CANADA
www.campbellsci.ca • dataloggers@campbellsci.ca

Campbell Scientific Africa Pty. Ltd.
PO Box 2450
Somerset West 7129
SOUTH AFRICA
www.campbellsci.co.za • cleroux@csafrica.co.za

Campbell Scientific Centro Caribe S.A.
300 N Cementerio, Edificio Breller
Santo Domingo, Heredia 40305
COSTA RICA
www.campbellsci.cc • info@campbellsci.cc

Campbell Scientific Southeast Asia Co., Ltd.
877/22 Nirvana@Work, Rama 9 Road
Suan Luang Subdistrict, Suan Luang District
Bangkok 10250
THAILAND
www.campbellsci.asia • info@campbellsci.asia

Campbell Scientific Ltd.
Campbell Park
80 Hathern Road
Shepshed, Loughborough LE12 9GX
UNITED KINGDOM
www.campbellsci.co.uk • sales@campbellsci.co.uk

Campbell Scientific Australia Pty. Ltd.
PO Box 8108
Garbutt Post Shop QLD 4814
AUSTRALIA
www.campbellsci.com.au • info@campbellsci.com.au

Campbell Scientific Ltd.
3 Avenue de la Division Leclerc
92160 ANTONY
FRANCE
www.campbellsci.fr • info@campbellsci.fr

Campbell Scientific (Beijing) Co., Ltd.
8B16, Floor 8 Tower B, Hanwei Plaza
7 Guanghua Road
Chaoyang, Beijing 100004
P.R. CHINA
www.campbellsci.com • info@campbellsci.com.cn

Campbell Scientific Ltda.
Fahrenheitstraße 13
28359 Bremen
GERMANY
www.campbellsci.de • info@campbellsci.de

Campbell Scientific do Brasil Ltda.
Rua Apinagés, nbr. 2018 ─ Perdizes
CEP: 01258-00 ─ São Paulo ─ SP
BRASIL
www.campbellsci.com.br • vendas@campbellsci.com.br

Campbell Scientific Spain, S. L.
Avda. Pompeu Fabra 7-9, local 1
08024 Barcelona
SPAIN
www.campbellsci.es • info@campbellsci.es

Please visit www.campbellsci.com to obtain contact information for your local US or international representative.