

Please read first

About this manual

Please note that this manual was produced by Campbell Scientific Inc. primarily for the North American market. Some spellings, weights and measures may reflect this. In addition, while most of the information in the manual is correct for all countries, certain information is specific to the North American market and so may not be applicable to Europe, Middle East, and Africa (EMEA) or Asia Pacific (APAC) users. Differences include the U.S. standard external power supply details where some information (for example the AC transformer input voltage) will not be applicable for EMEA or APAC use. Please note, however, *that when a power supply adapter is ordered from Campbell Scientific it will be suitable for use in your country.*

Reference to some radio transmitters, digital cell phones and aerials (antennas) may also not be applicable according to your locality. Some brackets, shields and enclosure options, including wiring, are not sold as standard items in the EMEA or APAC market; in some cases alternatives are offered.

Recycling information for countries subject to WEEE regulations 2012/19/EU



At the end of this product's life it should not be put in commercial or domestic refuse but sent for recycling. Any batteries contained within the product or used during the products life should be removed from the product and also be sent to an appropriate recycling facility, per [The Waste Electrical and Electronic Equipment \(WEEE\) Regulations 2012/19/EU](#). Campbell Scientific can advise on the recycling of the equipment and in some cases arrange collection and the correct disposal of it, although charges may apply for some items or territories. For further support, please contact Campbell Scientific, or your local agent.

Table of contents

1. Introduction	1
2. Precautions	1
3. QuickStart	2
3.1 Physical setup	2
3.2 Configuring the NL200/201	4
3.3 LoggerNet setup	5
3.4 Connect	6
4. Overview	6
4.1 Bridge mode enabled	8
4.2 Bridge mode disabled	9
5. Specifications	10
6. Configuring the NL200/201	12
6.1 Configuring the NL200/201 with Device Configuration Utility via USB	12
6.2 Configuring the NL200/201 with Device Configuration Utility via network connection	13
6.3 Configuring the NL200/201 with Telnet	13
6.4 Configuring the NL200/201 via RS-232	14
7. Operational mode	15
7.1 PakBus router	15
7.1.1 Physical setup	16
7.1.2 Configuring the NL200/201	16
7.1.2.1 RS-232 PakBus router	16
7.1.2.2 CS I/O PakBus Router	17
7.1.3 LoggerNet setup	17
7.1.4 Connect	18
7.2 Bridge mode	18
7.2.1 Physical setup	18
7.2.2 Configuring the NL200/201	19
7.2.3 Configuring the data logger	19

7.2.4	LoggerNet setup	20
7.2.5	Connect	20
7.3	TCP serial server	21
7.3.1	Physical setup	21
7.3.2	Configuring the NL200/201	21
7.3.2.1	RS-232 Serial server	21
7.3.2.2	CS I/O serial server	21
7.3.3	LoggerNet setup	22
7.3.4	Connect	23
7.3.5	Serial sensors	23
7.4	TCP Serial Client	23
7.5	Modbus TCP/IP to RTU Gateway	24
7.6	TLS	24
7.6.1	TLS proxy server	25
7.6.2	Device Configuration Utility TCP encrypted communications to the NL200/201	28
8.	Working around firewalls	29
8.1	Configuring the NL200/201	29
8.2	Configure the data logger	29
9.	Troubleshooting	30
10.	Attributions	33
Appendix A.	Network examples	34
A.1	NL200/201 with radio network	34
A.1.1	Configure the NL200/201 as a PakBus router	34
A.1.2	Configure radio connected to the NL200/201	35
A.1.2.1	RF407-series	35
A.1.2.2	RF451/452	35
A.1.3	Configure radio connected to the data logger	36
A.1.3.1	RF407-series	36
A.1.3.2	RF451/452	36
A.1.4	Configure the data logger	36
A.1.5	Setup LoggerNet	37
A.2	NL200/201 with cellular network	38
A.2.1	CELL200-series physical setup	38
A.2.2	Configure the CELL200-series as a serial server	38

A.2.3 NL200/201 physical setup	39
A.2.4 Configure the NL200/201	39
A.2.5 Configure the data logger	40
A.2.6 Setup LoggerNet	40
A.3 CR300 over IP to Konect	41
A.3.1 NL200/201 physical setup	42
A.3.2 Configure the NL200/201	42
A.3.3 Configure the data logger (CR300)	43
A.3.4 Setup LoggerNet	43
Appendix B. Cables, pinouts, LED function, and jumper	45
B.1 CS I/O	45
B.2 RS-232	46
B.3 Ethernet	46
B.4 USB	47
B.5 Power	48
B.6 LEDs	48
B.7 Power jumper (NL201 only)	48
Appendix C. NL200/201 settings	50
C.1 Main tab	50
C.1.1 Model (read only)	50
C.1.2 Serial Number (read only)	50
C.1.3 OS Version (read only)	50
C.1.4 Compile Date (read only)	50
C.1.5 Bridge Mode	50
C.1.6 CS I/O IP Interface Identifier	51
C.1.7 Bridge Mode Forward Code	51
C.1.8 DHCP	52
C.1.9 IP Address	52
C.1.10 Subnet Mask	53
C.1.11 Default Gateway	53
C.1.12 DNS Servers	53
C.1.13 IP Info	53
C.1.14 Ethernet Speed / Duplex Configuration	53
C.1.15 Admin Password	54
C.1.16 TCP Configuration Port Number	54
C.2 RS-232 tab	54


C.2.1 RS-232 Configuration	54
C.2.2 RS-232 Service Port	55
C.2.3 RS-232 Baud Rate	55
C.2.4 RS-232 RTS	55
C.2.5 RS-232 TCP Timeout (seconds)	56
C.2.6 RS-232 PakBus Beacon Interval	56
C.2.7 RS-232 PakBus Verify Interval	56
C.2.8 Neighbors Allowed RS-232	56
C.2.9 RS-232 Modbus Timeout	57
C.2.10 RS-232 TCP Serial Client IP Address	57
C.2.11 RS-232 TCP Serial Client Port	57
C.3 CS I/O tab	57
C.3.1 CS I/O Configuration	57
C.3.2 CS I/O Service Port	58
C.3.3 SDC Address	58
C.3.4 CS I/O TCP Timeout	58
C.3.5 CS I/O PakBus Beacon Interval	58
C.3.6 CS I/O PakBus Verify Interval	58
C.3.7 CS I/O Modbus Timeout	59
C.4 Net Services tab	59
C.4.1 Telnet	59
C.4.2 Telnet Port Number	59
C.4.3 Telnet Timeout	59
C.4.4 Ping (ICMP)	59
C.4.5 PakBus Address	59
C.4.6 PakBus/TCP Service Port	60
C.4.7 PakBus/TCP Password	60
C.4.8 PakBus/TCP Client Address (1-4)	60
C.4.9 PakBus/TCP Client Port (1-4)	60
C.4.10 PakBus Routes (read only)	60
C.4.11 Central Routers	61
C.5 TLS Proxy Server tab	61
C.5.1 TLS Proxy Server	61
C.5.2 TLS Proxy Service Port	61
C.5.3 TLS Proxy Forward Physical Port	62
C.5.4 TLS Proxy Forward IP Address	62
C.5.5 TLS Proxy Forward Port	62

C.5.6 TLS Proxy Timeout	63
C.6 TLS tab	63
C.6.1 TLS Status (read only)	63
C.6.2 TLS Private Key Password	63
C.6.3 TLS Private Key	64
C.6.4 TLS Certificate	64
Appendix D. Sending a new OS to the NL200/201	65
D.1 Sending an OS via USB	65
D.2 Sending an OS via IP	66
Appendix E. Glossary	67


1. Introduction

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

2. Precautions

- READ AND UNDERSTAND the [Safety](#) section at the back of this manual.
- The first time an NL200/201 is attached to a data logger and bridge mode is enabled, the data logger 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 data logger to recognize it.
- Use the newest version of *Device Configuration Utility* to communicate with the NL200/201. It can be downloaded from our website at www.campbellsci.com/downloads .
- Install the device driver before plugging the NL200/201 into your computer for the first time. The device driver must be properly installed before you can connect to the NL200/201 via USB.

To install the device driver, download the latest version of *Device Configuration Utility* from our website. Under **Device Type**, select **Network Peripheral > NL200 Series**. Click **Install USB Driver** and follow the prompts.

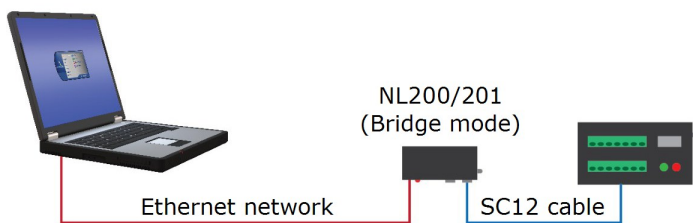
- CR1000, CR3000, and CR800-series data loggers require operating system version 23 or newer in order to operate with the NL200/201 in bridge mode. (OS version 23 or newer is not required to operate as a serial server or PakBus™ router.) The latest operating systems can be downloaded at www.campbellsci.com/downloads .
- 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 [Cables, pinouts, LED function, and jumper](#) (p. 45). The NL200 cannot be powered over CS I/O or USB. An external power adapter or power cable is required.
- Ensure maximum protection against surges. Use a shielded Ethernet cable. Use coaxial surge protection. Keep RS-232 and CS I/O cables short. 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. The NL200 may require the use of external surge suppression.

- When downloading a new operating system to the NL200/201, do not remove power until the LED stops rapidly flashing red and green.

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 **CS I/O** port to the data logger **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 Ethernet port and the other end to your network. Ensure that the device is powered up by inspecting the Power LED.

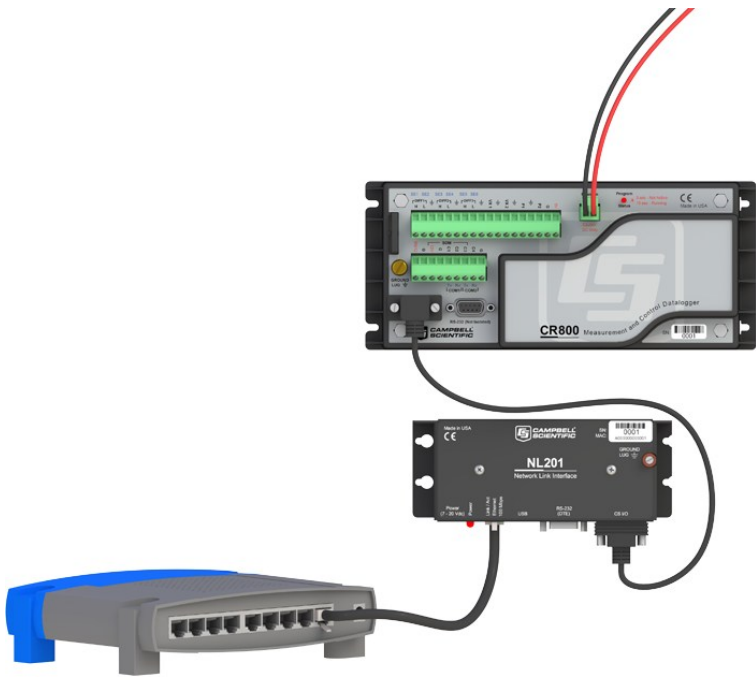


Figure 3-1. NL201 with CR800 (powered by data logger)

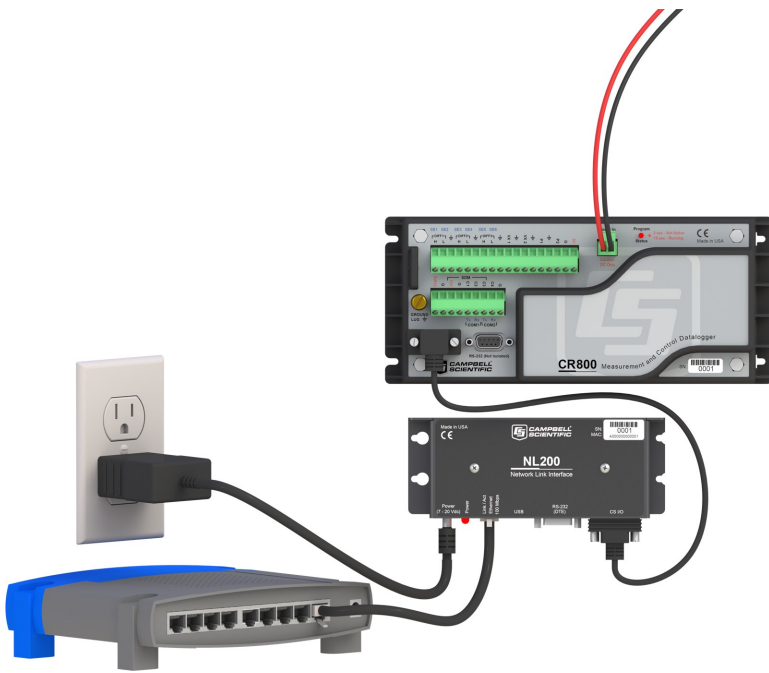


Figure 3-2. NL200 with CR800 (external power)

3.2 Configuring the NL200/201

NOTE:

Install the device driver before plugging the NL200/201 into your computer for the first time. The device driver must be properly installed before you can connect to the NL200/201 via USB.

To install the device driver, download the latest version of *Device Configuration Utility* from our website. Under **Device Type**, select **Network Peripheral > NL200 Series**. Click **Install USB Driver** and follow the prompts.

1. Apply power to the NL200/201.
2. Connect the supplied USB cable between a USB port on your computer and the **USB** port on the NL200/201.
3. Open *Device Configuration Utility*.
4. Under **Device Type**, select **Network Peripheral > NL200 Series**.
5. Click **Browse** next to **Communication Port**.
6. Select the virtual com port labeled **NL200/201**.
7. Click **OK**.
8. Click **Connect**.
9. Click the **NL200 Series** tab.
10. 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. For the purposes of this example assume that both the NL200/201 and data logger are directly connected with an Ethernet cable. Use the following IP info: 192.168.1.2 with a subnet mask of 255.255.255.0.
11. If a dynamic address is to be used, the network information acquired via DHCP can be seen on the NL200 Series tab under **Status**. The **Status** box also displays the MAC address of the NL200/201.
12. Click **Apply** to save the changes.

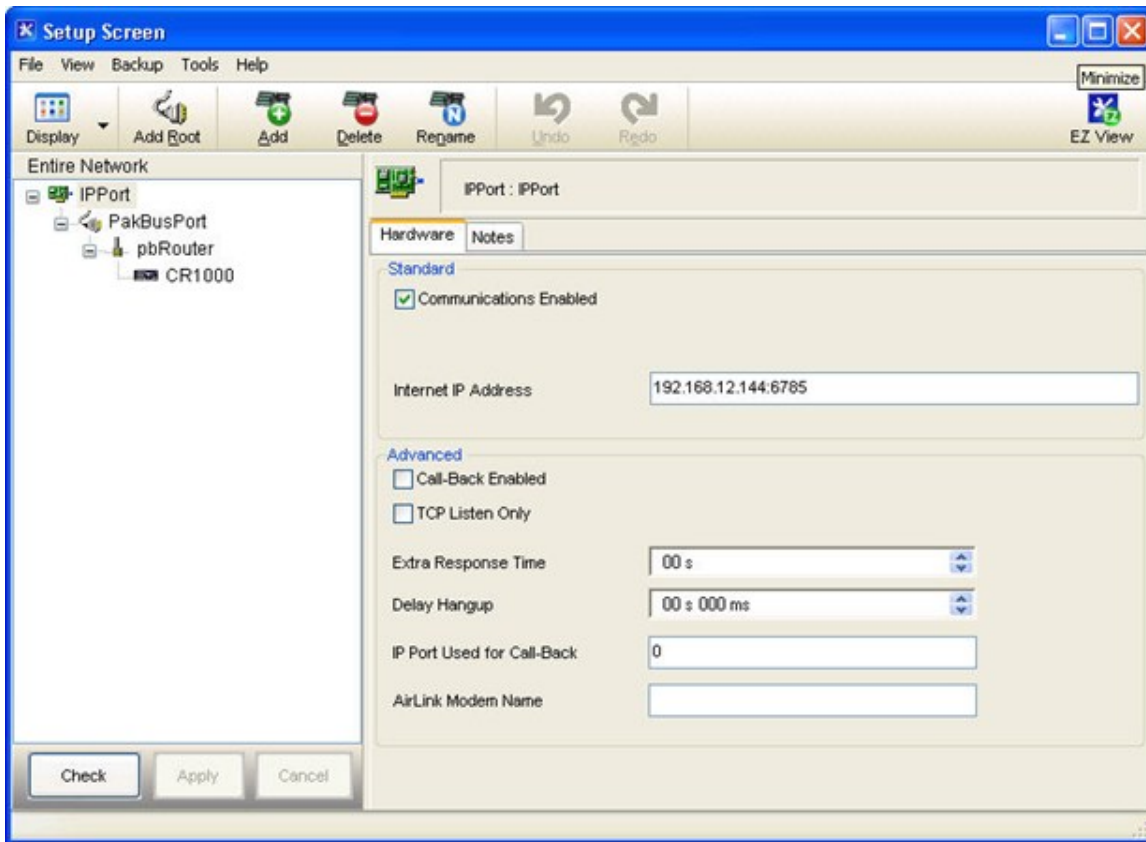
NOTE:

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 data logger via the NL200/201.

1. In the *LoggerNet* Setup screen, click **Add Root** and select **IPPort**. Enter the NL200/201 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.
2. Add **PakBusPort (PakBus Loggers)**.
3. Add a PakBus Router (**pbRouter**). Enter the PakBus address of the NL200/201. The NL200/201 default PakBus address is **678**. Click **Close**.
4. Add the data logger and enter its PakBus address.
5. Click **Apply** to save the changes.
6. You can verify that your settings are correct by selecting the data logger in the **Network Map**, selecting the **Clock** tab, and clicking **Check Clocks**. If your settings are correct, you should see the current clock of your server and data logger.



3.4 Connect

You are now ready to connect to your data logger using *LoggerNet*. Select **Main** and **Connect** on the *LoggerNet* toolbar, select the data logger from the **Stations** list, then **Connect**. From there, you can view and collect data, or manage data logger settings.

4. Overview

The NL200/201 Network Link Interface is designed for communications with Campbell Scientific data loggers 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 communications. A **USB** port is used for configuring the NL200/201 device.

Serial Server

- Allows access to a CR10X over an Ethernet network (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 an Ethernet network (RS-232 serial server).
- Allows access to an RF500M Base over an Ethernet network (RS-232 serial server).

PakBus Router

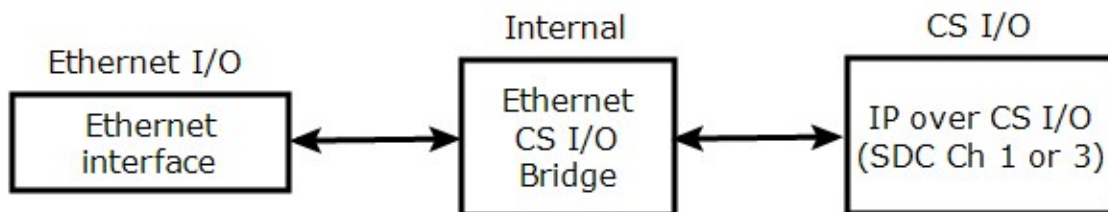
- Allows access to a CR10X-PB over an Ethernet network.
- Allows access to a CR200X over an Ethernet network.
- Allows you to connect to a PakBus device on the **RS-232** port and a PakBus device on the **CS I/O** port using only one TCP port.
- Allows a PakBus device on the **RS-232** port and a PakBus 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 interface to a data logger that supports CS I/O IP (bridge mode) communications.

4.1 Bridge mode enabled

The NL200/201 can be configured to bridge Ethernet and CS I/O communications (see the following figure). This mode is used for providing access to the internal IP functionality of the CR6, CR800/850, CR1000, and CR3000 (for example, webpage access, email, FTP, etc.). Bridge mode does not use PPP. Instead, raw IP packets are transferred between the Ethernet and CS I/O connections.

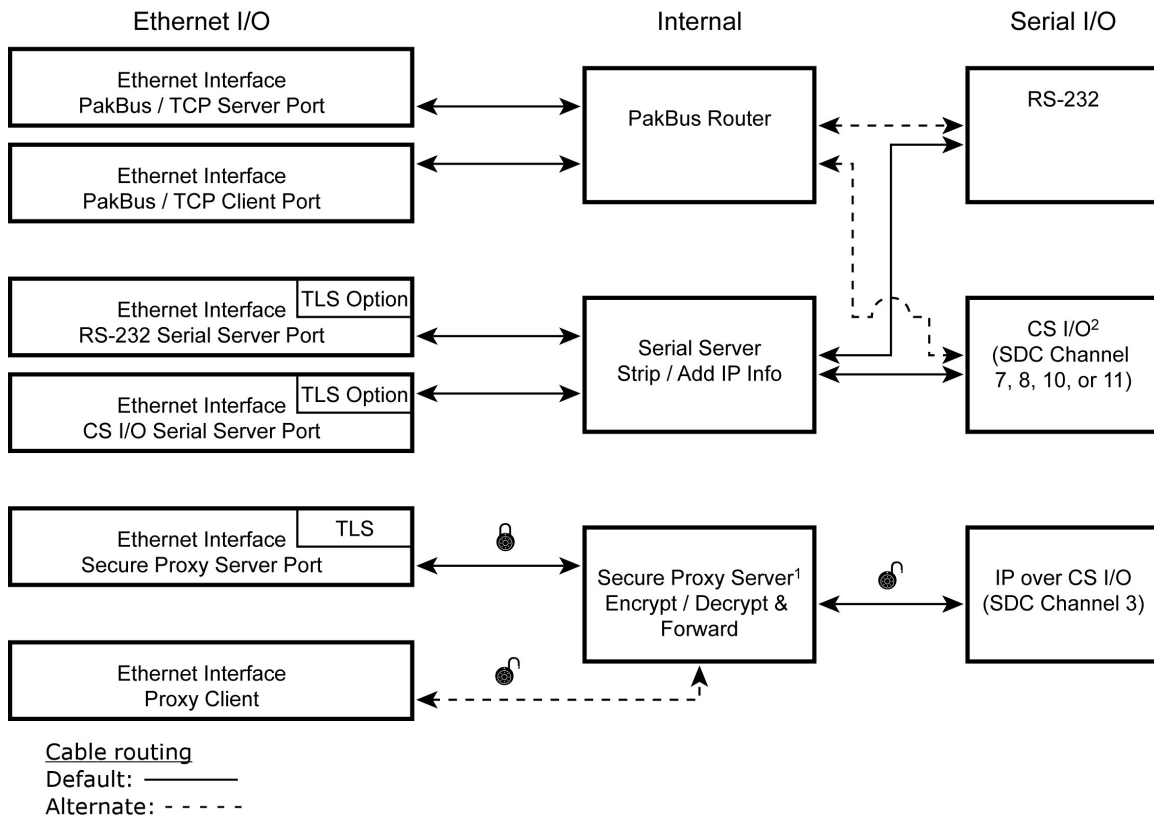


NOTE:

Devices connected to the CS I/O port must support IP over CS I/O. These include CR3000, CR1000, CR800, and newer data loggers.

4.2 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.



¹ The Secure Proxy Server can forward unsecured traffic to a single device. That device may be accessed via Ethernet or CS I/O. Any device connected to **CS I/O** wishing to use the Secure Proxy Service must support IP over CS I/O. Devices connected to the CS I/O port

must support IP over CS I/O. These include CR3000, CR1000, CR800, and newer data loggers.

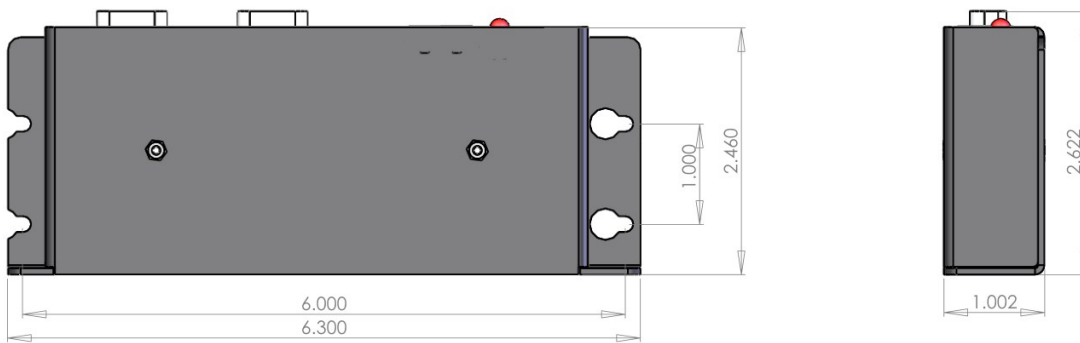
² Secure Proxy Server operation through the **CS I/O** port is independent of PakBus and Serial Server operations.

5. Specifications

General

177 g (6.3 oz)

16 x 6.73 x 2.54 cm (6.3 x 2.65 x 1 in)



Power input

NL201: **CS I/O** or DC Barrel connector (not USB)

NL200: DC Barrel connector (not USB)

7 to 20 VDC

600 mW active, 24 mW standby

NOTE:

To prevent the NL200/201 from being powered over the **CS I/O** port remove the internal jumper. See [Cables, pinouts, LED function, and jumper](#) (p. 45) for more information.

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 [IPNetPower\(\)](#). Note that the [IPNetPower\(\)](#) 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

Device Configuration Utility 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 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

Supported Protocols

10Base-T and 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 documents at: www.campbellsci.com/nl201 

6. Configuring the NL200/201

The NL200/201 is configured using *Device Configuration Utility* connected using either a network connection or USB.

6.1 Configuring the NL200/201 with Device Configuration Utility via USB	12
6.2 Configuring the NL200/201 with Device Configuration Utility via network connection	13
6.3 Configuring the NL200/201 with Telnet	13
6.4 Configuring the NL200/201 via RS-232	14

6.1 Configuring the NL200/201 with *Device Configuration Utility* via USB

NOTE:

Install the device driver before plugging the NL200/201 into your computer for the first time. The device driver must be properly installed before you can connect to the NL200/201 via USB.

To install the device driver, download the latest version of *Device Configuration Utility* from our website. Under **Device Type**, select **Network Peripheral > NL200 Series**. Click **Install USB Driver** and follow the prompts.

1. Apply power to the NL200/201.
2. Connect the supplied USB cable between a USB port on your computer and the **USB** port on the NL200/201.
3. Open *Device Configuration Utility*.
4. Under **Device Type**, select **Network Peripheral > NL200 Series**.
5. Click **Browse** next to **Communication Port**.
6. Select the port labeled **NL200/201**.
7. Click **OK**.
8. Click **Connect**.

9. Configure the NL200/201 as needed for your application.
10. Click **Apply** to save the changes.

6.2 Configuring the NL200/201 with *Device Configuration Utility* 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.

1. Apply power to the NL200/201.
2. Open *Device Configuration Utility*.
3. Under **Device Type**, select **Network Peripheral > NL200 Series**.
4. Select **Use IP Connection**.
5. Type the IP address of the device in the **Communication Port** field. If the address of the device is unknown and the device is connected to your local area network, **Browse** to discover the devices on the network.
6. Type **NL200/201** in the **Administrative Password** box. (nl200 is the default administrative password. It can be changed via the *Device Configuration Utility* **Deployment > NL200 Series** tab.)
7. Click **OK**.
8. Click **Connect**.
9. Configure the NL200/201 as needed for your application.
10. Click **Apply** to save the changes.

6.3 Configuring the NL200/201 with Telnet

NOTE:

For security reasons, Telnet is disabled by default. It must be enabled from the **Network Services** tab in *Device Configuration Utility*.

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

1. Apply power to the NL200/201.
2. Create a Telnet session with the NL200/201 over port 23.
3. Type **NL200/201** in the **Administrative Password** box. (**nl200** is the default administrative password. It can be changed via the *Device Configuration Utility Deployment > NL200 Series* tab.)
4. Type **help** to see a list of the functionality available when connected to the NL200/201.
5. Type **edit** and press **Enter** to edit the settings of the NL200/201.
6. 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.
7. After progressing through all of the NL200/201 settings, type **save** to accept the changes or **cancel** to discard the changes.
8. Type **bye** to exit the Telnet session.

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.

1. Using a null modem serial cable, connect your computer serial port to the **RS-232** port on the NL200/201.
2. Connect to the NL200/201 using a terminal emulator. The *Device Configuration Utility* “**Unknown**” device type is an example of a simple terminal emulator. The default settings for this interface are 115200 baud, 8 data bits, no parity, 1 stop bit, no flow control.
3. Power cycle the NL200/201 and repeatedly press **Enter** at the terminal.
4. Type **help** to see a list of the functionality available when connected to the NL200/201.
5. Type **edit** and press **Enter** to edit the settings of the NL200/201.
6. 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.
7. After progressing through all of the NL200/201 settings, type **save** to accept the changes or **cancel** to discard the changes.

8. Disconnect your computer and power cycle the NL200/201.

7. Operational mode

This section describes how to configure the operational mode of your NL200/201. See [Overview](#) (p. 6) for help in determining which operational mode to use.

7.1 PakBus router	15
7.2 Bridge mode	18
7.3 TCP serial server	21
7.4 TCP Serial Client	23
7.5 Modbus TCP/IP to RTU Gateway	24
7.6 TLS	24

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.

Use the following list of terms as a reference:

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 ensure that all devices in the network are aware of other viable devices 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 communications has taken place within the interval. If the **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. Generally, the **Verify Interval** should be set greater than or equal to the interval at which you will be talking to the attached PakBus devices. For example, if the NL200/201 is being used as a PakBus router to allow scheduled collection of a network of data loggers every 15 minutes, consider setting the **Verify Interval** to 30 minutes.

Neighbors Allowed (RS-232 port only) – Used to 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 **Neighbors Allowed** list except if the PakBus address is ≥ 4000 . Following a hello message, devices with PakBus addresses ≥ 4000 are automatically accepted as neighbors.

7.1.1 Physical setup

Using the supplied serial cable, connect the NL200/201 **CS I/O** port or **RS-232** port to the data logger **CS I/O** or **RS-232** port, respectively. The NL201 will be powered if connected via CS I/O. Alternatively, power either the NL201 or NL200 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 **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

7.1.2.1 RS-232 PakBus router

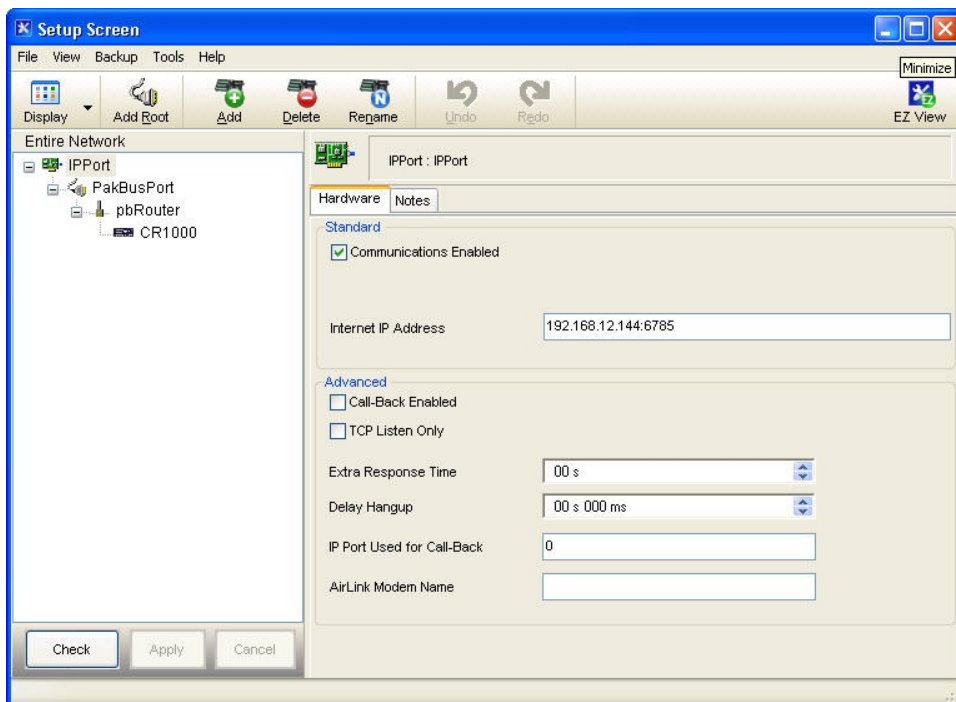
1. Connect to the NL200/201 in *Device Configuration Utility* (see [Configuring the NL200/201](#) [p. 12]).
2. On the **NL200 Series** tab, set **Bridge Mode** to **disable**.
3. On the **RS-232** tab:
 - a. Set **Configuration** to **PakBus**.
 - b. Set **Baud Rate** to baud rate of attached device, generally this is **115200** (default).
 - c. Set **Beacon Interval**, **Verify Interval**, and **PakBus Neighbors Allowed** as previously described. Often, the default values can be used. However, an allowed neighbors list can be useful in restricting communications paths.
4. On the **Network Services** tab, make note of the **PakBus/TCP Service Port**. The default **PakBus/TCP Service Port** is **6785**. Unless firewall issues exist, it is not necessary to change the port from its default value. This port number must match the port number entered in LoggerNet Setup after the IP address.

7.1.2.2 CS I/O PakBus Router

1. Connect to the NL200/201 in *Device Configuration Utility* (see [Configuring the NL200/201](#) [p. 12]).
2. On the **NL200 Series** tab, set **Bridge Mode** to **disable**.
3. On the **CS I/O** tab:
 - a. Set **Configuration** to **PakBus**.
 - b. Set **SDC address**. (Note that if multiple peripherals are connected to a data logger **CS I/O** port, each must have a unique SDC address.)
 - c. Set **Beacon Interval**, **Verify Interval**, and **PakBus Neighbors Allowed** as previously described. Often, the default values can be used. However, an allowed neighbors list can be useful in restricting communications paths.
4. On the **Network Services** tab, make note of the **PakBus/TCP Service Port**. The default **PakBus/TCP Service Port** is **6785**. Unless firewall issues exist, it is not necessary to change the port from its default value. This port number must match the port number entered in *LoggerNet Setup* after the IP address.

7.1.3 LoggerNet setup

1. In the *LoggerNet Setup* screen, click **Add Root** and select **IPPort**. Enter the NL200/201 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.
2. Add **PakBusPort (PakBus Loggers)**.
3. Add a PakBus Router (**pbRouter**). Enter the PakBus address of the NL200/201. The NL200/201 default PakBus address is **678**. Click **Close**.
4. Add the data logger and enter its PakBus address.
5. Click **Apply** to save the changes.



7.1.4 Connect

You are now ready to connect to your data logger using *LoggerNet*. Select **Main** and **Connect** on the *LoggerNet* toolbar, select the data logger from the **Stations** list, then **Connect**. From there, you can view and collect data, or manage data logger settings.

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 data logger over the **CS I/O** port. This enables the data logger to use its TCP/IP stack to interpret the packet and, therefore, all of the data logger TCP services are available. In bridge mode, none of the other device settings are valid. All other functionality is disabled. All settings (such as IP, netmask, gateway) are configured in the data logger. 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 *Device Configuration Utility*. 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 **CS I/O** port to the data logger **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 Ethernet port and the other end to your network. Ensure that the device is powered up by inspecting the Power LED.

NOTE:

The NL200 cannot be powered over **CS I/O** or **USB**. An external power adapter or power cable is required.

7.2.2 Configuring the NL200/201

Connect to the NL200/201 in *Device Configuration Utility* (see [Configuring the NL200/201](#) [p. 12]). On the **NL200/201** tab, set **Bridge Mode** to **enable**.

NOTE:

In bridge mode, the IP address, subnet mask, and IP gateway to be used by the NL200/201 are configured in the data logger.

7.2.3 Configuring the data logger

NOTE:

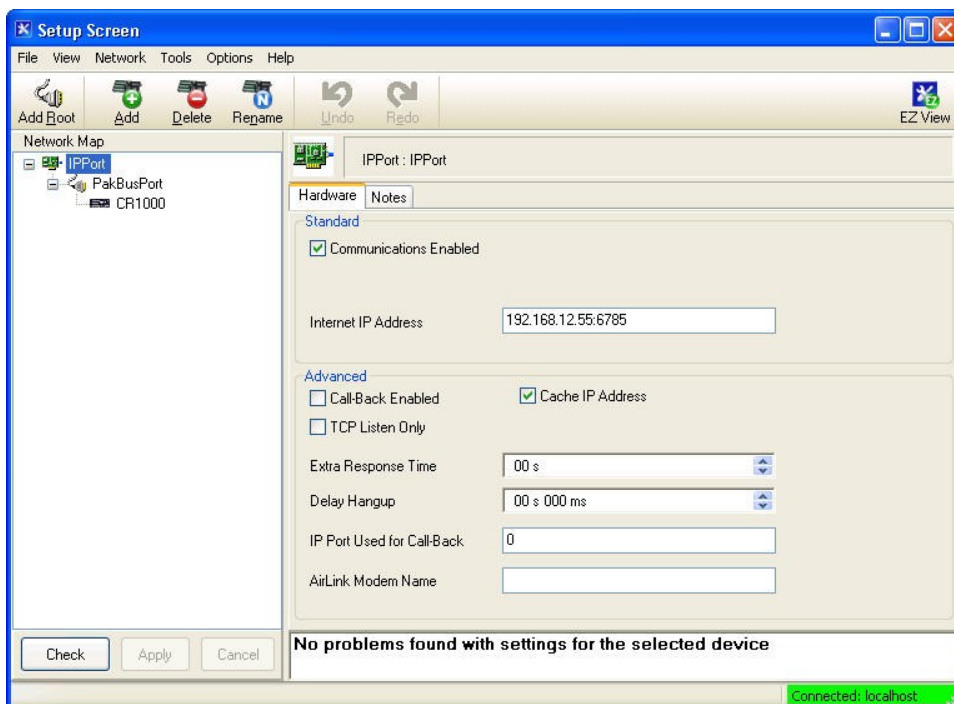
The NL200/201 must be connected to the data logger before configuring the data logger with *Device Configuration Utility*. If it is not connected, the Ethernet settings will not be displayed.

1. Connect a serial cable from the computer COM port to the data logger **RS-232** port.
2. Open *Device Configuration Utility*. Select the your data logger from the **Device Type** list, the appropriate **Communication Port**, and **Baud Rate**. Click **Connect** to connect to the data logger.
3. 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 **Ethernet** 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. Information acquired by DHCP is shown in the info box on the **Ethernet** and **CS I/O IP** tabs.
4. Click **Apply** to save the changes and then close *Device Configuration Utility*.

7.2.4 LoggerNet setup

The next step is to run *LoggerNet* and configure it to connect to the data logger via the **Ethernet** port. (See the following screen shot.)

1. In the *LoggerNet* Setup screen, click **Add Root** and select **IPPort**. Enter the data logger IP address and port number. The IP address and port number are input on the same line separated by a colon. The data logger default **Port** number is **6785**. Unless firewall issues exist, it is not necessary to change the port from its default value.
2. Add **PakBusPort (PakBus Loggers)**.
3. Add the data logger and enter its PakBus address.
4. Click **Apply** to save the changes and then close *Device Configuration Utility*.
5. Verify that the settings are correct by selecting the data logger in the **Network Map**, clicking the **Clock** tab, and clicking **Check Clocks**. If the settings are correct, the current clock of the server and data logger will update.



7.2.5 Connect

You are now ready to connect to your data logger using *LoggerNet*. Select **Main** and **Connect** on the *LoggerNet* toolbar, select the data logger from the **Stations** list, then **Connect**. From there, you can view and collect data, or manage data logger settings.

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 IP port will have the IP layer removed, the data is then directed to the serial connection.

7.3.1 Physical setup

Using the supplied serial cable, connect the NL200/201 **CS I/O** port or **RS-232** port to the data logger **CS I/O** or **RS-232** port, respectively. The NL201 will be powered if connected via CS I/O. Alternatively, power either the NL201 or NL200 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 **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

7.3.2.1 RS-232 Serial server

1. Connect to the NL200/201 in *Device Configuration Utility* (see [Configuring the NL200/201](#) [p. 12]).
2. On the **NL200 Series** tab, set **Bridge Mode** to **disable**.
3. On the **RS-232** tab:
 - a. Set **Configuration** to **TCP Serial Server**.
 - b. Set **Baud Rate** to baud rate of attached device, generally this is **115200** (default).
 - c. Make a note of the **Serial Service Port**. The default RS-232 **Serial Service Port** is **6784**. Typically, it is not necessary to change this entry from its default.

7.3.2.2 CS I/O serial server

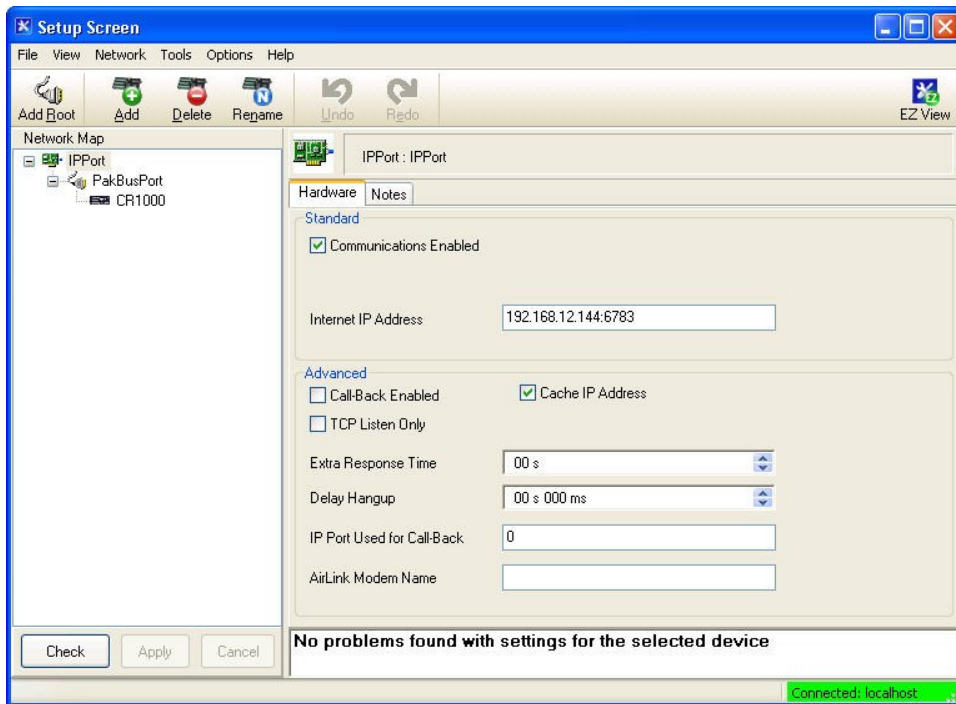
1. Connect to the NL200/201 in *Device Configuration Utility* (see [Configuring the NL200/201](#) [p. 12]).
2. On the **NL200 Series** tab, set **Bridge Mode** to **disable**.

3. On the **CS I/O** tab:
 - a. Set **Configuration** to **TCP Serial Server**.
 - b. Set **SDC address**. (Note that if multiple peripherals are connected to a data logger **CS I/O** port, each must have a unique SDC address.)
 - c. Make a note of the **Serial Service Port**. The default **CS I/O Serial Service 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 data logger via the **Ethernet** port. (See the following screen shot.)

1. In the *LoggerNet* Setup screen, click **Add Root** and select **IPPort**. Enter the NL200/201 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. The NL200/201 default **Port** number is **6783**. Unless firewall issues exist, it is not necessary to change the port from its default value.
2. Add **PakBusPort (PakBus Loggers)**.
3. Add the data logger and enter its PakBus address.
4. Click **Apply** to save the changes and then close *Device Configuration Utility*.
5. Verify that the settings are correct by selecting the data logger in the **Network Map**, clicking the **Clock** tab, and clicking **Check Clocks**. If the settings are correct, the current clock of the server and data logger will update.



7.3.4 Connect

You are now ready to connect to your data logger using *LoggerNet*. Select **Main** and **Connect** on the *LoggerNet* toolbar, select the data logger from the **Stations** list, then **Connect**. From there, you can view and collect data, or manage data logger settings.

7.3.5 Serial sensors

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

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 client (formerly called master). The port number of the listening connection is specified in the RS-232 (or CS I/O) **Service Port** 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 (or CS I/O) 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 client over the established TCP connection. The Modbus RTU device is generally a data logger connected to the RS-232 (or CS I/O) port or a data logger located remotely over a transparent radio (for example, RF452/RF451/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 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. Certificates should be PEM (privacy-enhanced mail) 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 data logger. The NL200/201 TLS proxy server maintains a secure TLS connection with a remote TLS client and forwards data onto a data logger using a standard TCP connection thus enabling communications with TLS clients. The TLS client can be a web browser using HTTPS or another user-supplied TLS client. This offloads from the data logger 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 *Device Configuration Utility*.

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 *Device Configuration Utility*.

1. Connect to the NL200/201 in *Device Configuration Utility* (see [Configuring the NL200/201](#) [p. 12]).
2. Navigate to the **Settings Editor** tab and then to the **TLS** tab.
3. 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**.
4. 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**.
5. Enter the **TLS Private Key Password** if the TLS private key is encrypted. Otherwise, leave the setting blank.
6. After loading the key and certificate, click **Apply**. The NL200/201 will reboot. Connect with *Device Configuration Utility* 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 *Device Configuration Utility* link. The **TLS Private Key**, **TLS Private Key Password**, and **TLS Certificate** can only be edited/transmitted over a secure *Device Configuration Utility* 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 *Device Configuration Utility* as long as the **Use IP Connection** option is selected.

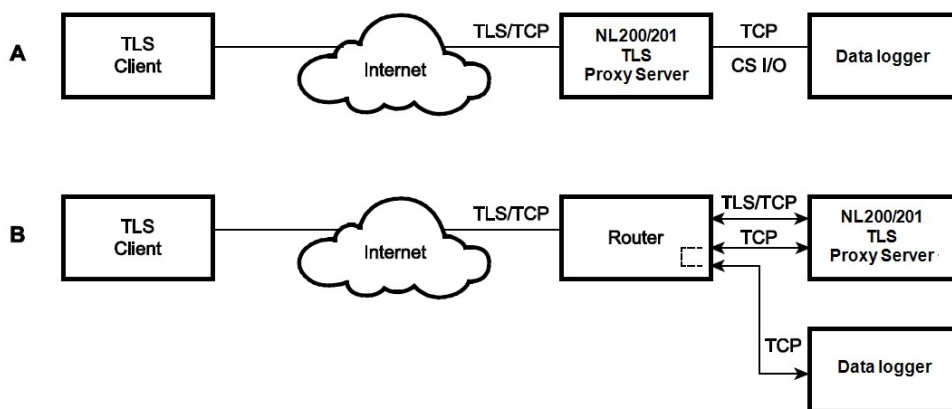
7.6.1 TLS proxy server

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, webpage, 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 TLS proxy server maintains a secure TLS connection with a remote TLS client and forwards data to a data logger using a standard TCP connection thus enabling communications with TLS clients. The TLS client can be a web browser using HTTPS or another 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 data logger. In this way, a remote TLS client can establish a TLS connection with a data logger.

The settings found in the **TLS Proxy Server** and **TLS** tab in *Device Configuration Utility* 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.



To configure the NL200/201 TLS proxy server to communicate with a data logger attached to the **CS I/O** port or with a data logger over a Ethernet connection, open *Device Configuration Utility* and configure the following settings.

Settings Editor > TLS Proxy Server tab

Configuration A

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

1. Connect to the NL200/201 in *Device Configuration Utility* (see [Configuring the NL200/201](#) [p. 12]).
2. Select the **CS I/O IP** tab.
3. Set the **CS I/O Interface IP Address** to a static IP address. Use the data logger CS I/O Interface that corresponds to the **NL200/201CS I/O IP Interface Identifier** setting.

Configuration B

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

1. Connect to the NL200/201 in *Device Configuration Utility* (see [Configuring the NL200/201](#) [p. 12]).
2. Select the **TCP/IP** tab.
3. Set the Ethernet Interface **IP Address** to a static IP address.
4. Set the **TLS Proxy Server** setting to **enable**.
5. Enter the **TLS Proxy Service Port**. 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 data logger 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.
6. Set the **TLS Proxy Forward Physical Port** to **CS I/O Port** for Configuration A or to **Ethernet Port** for Configuration B.
7. For Configuration A, leave the **TLS Proxy Forward IP Address** set to **0.0.0.0**. For Configuration B, enter the data logger IP address in the **TLS Proxy Forward IP Address** setting. This address must be configured in the data logger. 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 data logger would be 192.168.5.2 provided there are no other devices on the subnet with that address.
8. Set the **TLS Proxy Forward Port**. This is the TCP port number that the proxy server will use when it opens a TCP connection to the data logger to forward unencrypted data. The data logger TCP server must be set to communicate on this port number. The default value for the data logger PakBus/TCP service port is 6785, so this setting can likely be left at the default. The data logger 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.
9. 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.

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 data logger address could be set as 192.168.5.2 provided there are no other devices on the subnet with that address. Also, set the data logger subnet mask to match that of the NL200/201.

The data logger 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**). The data logger always listens on port 80 for HTTP, therefore, no TCP port configuration is necessary for using HTTP.

7.6.2 *Device Configuration Utility* TCP encrypted communications to the NL200/201

In order to use *Device Configuration Utility* TCP encrypted communications with the NL200/201, you will need to load the TLS private key and TLS certificate into the NL200/201. This is done from the **Settings Editor** > **TLS** tab in *Device Configuration Utility*. Once the private key and certificate are loaded successfully, the **TLS Status** field should read **Initialized**.

To use TCP encrypted communications, select the **Use IP Connection** check box in *Device Configuration Utility*. Input the NL200/201 IP address (or click **Browse** to select it from a list of NL200/201s connected to the network) and click **Connect**.

NOTE:

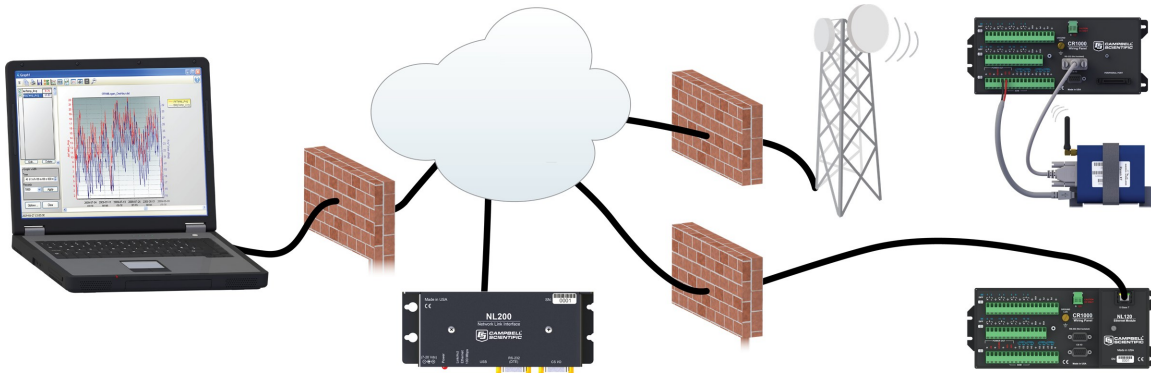
If the status of the TLS stack is **Initialized**, the NL200/201 will automatically negotiate a secure TLS connection with *Device Configuration Utility* as long as the **Use IP Connection** option is selected.

Encrypted communications 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. Working around firewalls

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



8.1 Configuring the NL200/201

Connect to the NL200/201 in *Device Configuration Utility* (see [Configuring the NL200/201](#) [p. 12]).

1. On the NL200/201 tab:
 - a. Set **Bridge Mode** to **disable**.
 - b. Set **DHCP Enabled** to **disable**.
 - c. Enter the **IP Address**, **Network Mask**, and **Default Gateway**. These values can be provided by your network administrator.
2. On the **Network Services** tab, make note of the **PakBus/TCP Service Port**.

8.2 Configure the data logger

NOTE:

The data logger must first be configured for internet communications.

1. Connect a serial cable from the computer COM port to the data logger **RS-232** port.
2. Open *Device Configuration Utility*. Select the your data logger from the **Device Type** list, the appropriate **Communication Port**, and **Baud Rate**. Click **Connect** to connect to the data logger.
3. On the **Network Services** tab input the **NL200/201IP address** and **PakBus TCP Service Port** in the **PakBus TCP Clients** area.
4. Click **Apply** to save the changes and then close *Device Configuration Utility*.

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 guidance to correct simple errors yourself.

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


1. Check all the 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 cables.
Verify that your Ethernet cable is securely plugged in between your NL200/201 and your hub, router, or computer. The yellow Link/Act light on the NL200/201 should start flashing when it is connected to the Ethernet.
If an Ethernet cable is connected but the Link/Act light is not flashing, 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/computer.
Turn off or unplug your hub/router/computer 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.
 - a. Make sure the assigned NL200/201 IP address (DHCP or static) and the IP address of the computer you are trying to connect from are able to communicate with each other. (Your network administrator can help 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
Computer: IP address: 192.168.0.3, Network Mask: 255.255.255.0
 - b. If using DHCP to assign an IP address to the NL200/201, use **Device Configuration Utility** to read the IP address assigned to the NL200/201. This is done through a USB connection to the NL200/201 while the NL200/201 is connected to your network (if bridge mode is not being used).
 - c. The IP address assigned to the NL200/201 must be unique on your network.
 - d. When bridge mode is enabled, the data logger controls how the IP address is assigned. Make sure your data logger is connected correctly to the NL200/201 via the **CS I/O** port and SC12 cable.
5. Try to ping the NL200/201 from your computer. (From the Windows Start Menu, type **command**, and click **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.
6. Make sure the IP address and port number entered in **LoggerNet/RTDAQ/PC400** match the settings in the NL200/201.

NOTE:

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 (for example, 192.168.0.3:6783).

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

8. If the NL200/201 is configured as a CS I/O serial server, verify that any other SDC device attached to the data logger is using a different SDC address. For example, if the NL200/201 is configured for SDC7, any other device attached to the data logger cannot use SDC7.
9. If communicating over a slow or intermittent connection, it may be necessary to lower the **Maximum Packet Size** of the data logger in *LoggerNet* Setup and/or add **Extra Response Time** to the **PakBus Port** in *LoggerNet* Setup.
10. Reset the NL200/201 to its default settings.

If none of the above steps correct your communications problems, reset the NL200/201 to its default settings. This can be done using the **Factory Defaults** button in *Device Configuration Utility* or by using the **Defaults** command in a Telnet session with the NL200/201.

11. Verify that the latest revision of firmware (operating system) is running. It is possible that an issue affecting your ability to communicate via the NL200/201 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 [Sending a new OS to the NL200/201](#) (p. 65) for instructions on downloading the firmware revision to the NL200/201.
12. 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:
 - a. 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 NL200/201 communications network.
 - b. Save a copy of the NL200/201 settings (in XML format) using *Device Configuration Utility*.
 - c. Save a copy of the NL200/201 event log. This is low-level code that can be used by Campbell Scientific technical support to help troubleshoot the NL200/201. To obtain the event log, the NL200/201 must not be in bridge mode. Telnet into the NL200/201 using your favorite Telnet program. Once 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.
 - d. Once the eventlogs have been copied, type "eventlog erase" at the prompt to clear the log. To add a date to indicate when the logs were last cleared 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

Copyright (c) 2001-2004 Swedish Institute of Computer Science. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT 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.

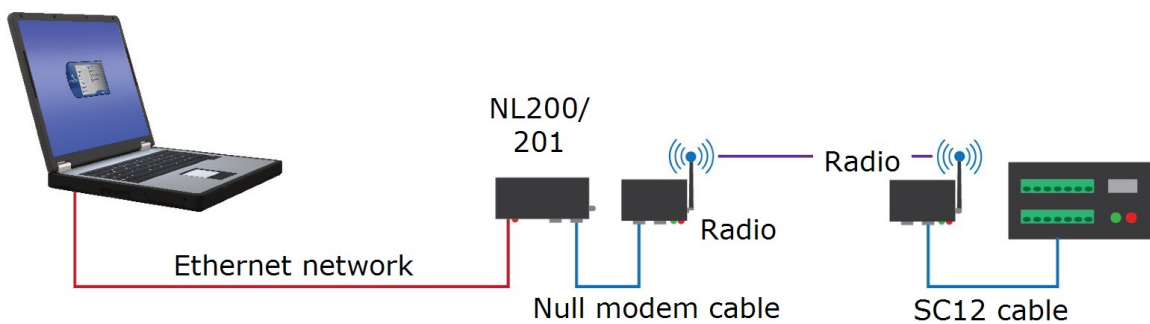
Appendix A. Network examples

The following sections describe frequently used configurations with the NL200/201.

A.1 NL200/201 with radio network	34
A.2 NL200/201 with cellular network	38
A.3 CR300 over IP to Konect	41

A.1 NL200/201 with radio network

This type of network is useful when the data logger is not located close enough to an Ethernet network to be plugged in. To overcome this distance, use spread-spectrum radios to establish connectivity with the Ethernet network.



A.1.1 Configure the NL200/201 as a PakBus router

Out of the box, the NL200/201 is configured for operation as a PakBus router. You may not need to make any changes. The following steps provide information about these default settings.

1. Connect to the NL200/201 in *Device Configuration Utility* (see [Configuring the NL200/201](#) [p. 12]).
2. On the **NL200 Series** tab, set **Bridge Mode** to **disable**.
3. If a dynamic address is to be used, the network information acquired via DHCP can be seen on the NL200 Series tab under **Status**. The **Status** box also displays the MAC address of the NL200/201.
4. 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. For the purposes of this example assume that both the NL200/201 and data logger are directly connected with an Ethernet cable. Use the following IP info: 192.168.1.2 with a subnet mask of 255.255.255.0.

5. On the **RS-232** tab:
 - a. Set **Configuration** to **PakBus**.
 - b. Set **Baud Rate** to baud rate of attached radio. Generally this is **115200** (default).
 - c. Set **Beacon Interval** to **60** (seconds) and **Verify Interval** to **0**. If you want to restrict communications paths, use the **PakBus Neighbors Allowed** setting to specify allowed neighbor addresses.
6. On the **Network Services** tab, make note of the **PakBus/TCP Service Port**. The default **PakBus/TCP Service Port** is **6785**. Unless firewall issues exist, it is not necessary to change the port from its default value. This port number must match the port number entered in LoggerNet Setup after the IP address. See [Setup LoggerNet](#) (p. 37).

A.1.2 Configure radio connected to the NL200/201

Using a USB cable, connect to the radio that will be connected to the NL200/201. Either an RF407-series or RF451/452 can be used. See those product manuals for additional details.

A.1.2.1 RF407-series

1. Connect to the radio in *Device Configuration Utility*.
2. Click the **Factory Defaults** button at the bottom of the Deployment window.
3. On the **Main** tab set **Active Interface** to **RS-232**.
4. Click **Apply** to save the changes.

A.1.2.2 RF451/452

1. Connect to the radio in *Device Configuration Utility*.
2. Click the **Factory Defaults** button at the bottom of the Deployment window.
3. On the **Deployment** tab set:
 - a. **Active Interface** to **RS-232**
 - b. **Radio Operation Mode** to **Gateway** (previously called Master)

NOTE:

There can only be one Gateway in an RF451/452 network.

4. Click **Apply** to save the changes.

A.1.3 Configure radio connected to the data logger

1. Using an SC12 cable, connect the data logger **CS I/O** port to the radio **CS I/O** port.
2. Connect a USB cable between a USB port on your computer and the radio **USB** port.

A.1.3.1 RF407-series

1. Connect to the radio in *Device Configuration Utility*.
2. Click the **Factory Defaults** button at the bottom of the Deployment window.
3. Click **Apply** to save the changes.

A.1.3.2 RF451/452

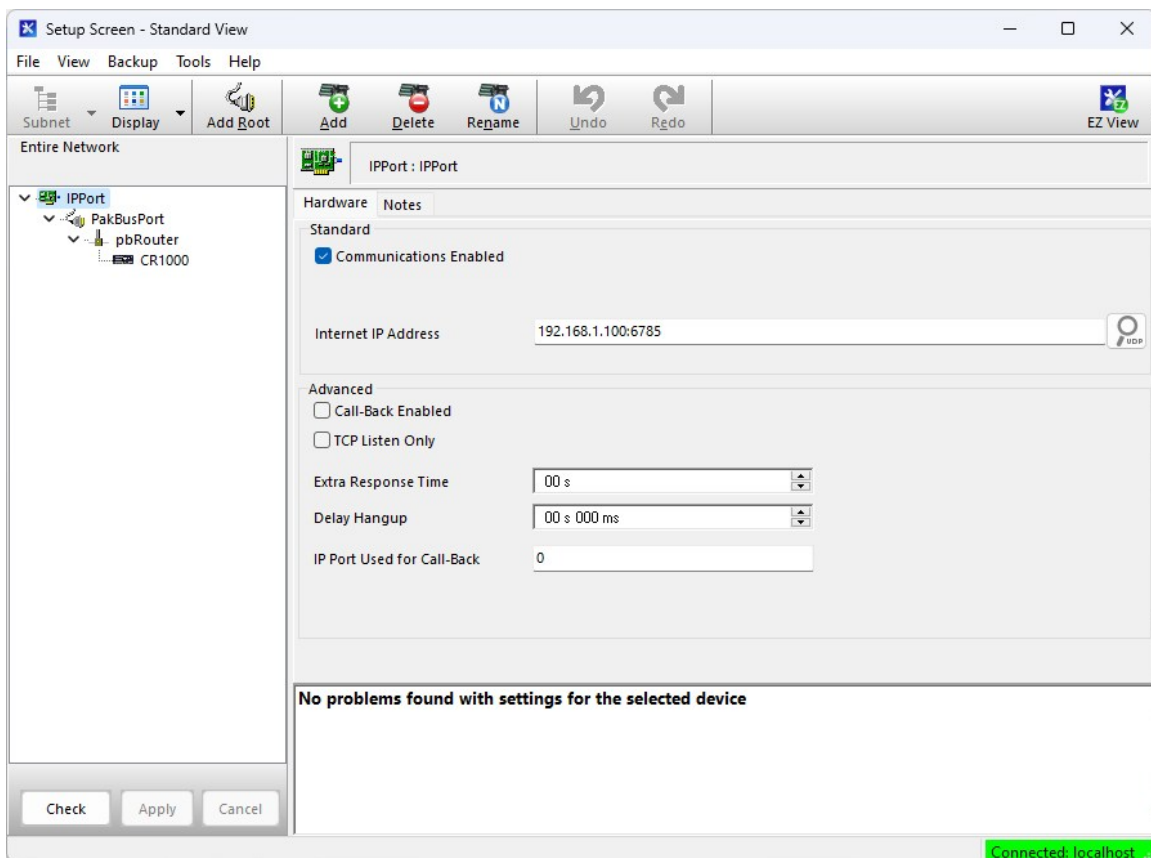
1. Connect to the radio in *Device Configuration Utility*.
2. Click the **Factory Defaults** button at the bottom of the Deployment window.
3. On the **Deployment** tab, keep the defaults and confirm:
 - a. **Active Interface** is **CS I/O SDC**
 - b. **SDC Address** is **7**
 - c. **Radio Operation Mode** is **Endpoint** (previously called Slave)
4. Click **Apply** to save the changes.

A.1.4 Configure the data logger

1. Connect to the data logger in *Device Configuration Utility*.
2. Click the **Factory Defaults** button at the bottom of the Deployment window.
3. On the **Com Ports Settings** tab set:
 - a. **ComPort** to **CS I/O SDC7**
 - b. **Beacon Interval** to **60** (seconds)
4. Click **Apply** to save the changes and then close *Device Configuration Utility*.

A.1.5 Setup *LoggerNet*

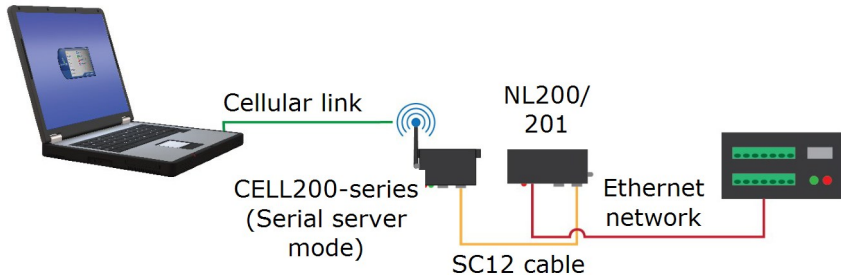
1. In the *LoggerNet* Setup screen, click **Add Root** and select **IPPort**. Enter the NL200/201 IP address and port number. The IP address and port number are input on the same line separated by a colon. IPv6 addresses will need to be enclosed in square brackets when specifying a port number. An IPv4 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.
2. Add **PakBusPort (PakBus Loggers)**.
3. Add a PakBus Router (**pbRouter**). Enter the PakBus address of the NL200/201. The NL200/201 default PakBus address is **678**. Click **Close**.
4. Add the data logger and enter its PakBus address.
5. Click **Apply** to save the changes.



6. You are now ready to connect to your data logger using *LoggerNet*. Select **Main** and **Connect** on the *LoggerNet* toolbar, select the data logger from the **Stations** list, then **Connect**. From there, you can view and collect data, or manage data logger settings.

A.2 NL200/201 with cellular network

This type of network is useful when there is no cellular signal at the data logger but a cellular signal can be reached using a run of Ethernet cable.



A.2.1 CELL200-series physical setup

1. Connect the CELL200-series and NL200/201 RS-232 ports using a straight-through RS-232 pin to socket cable such as an SC12.
2. Connect the cellular antenna, if it is not already connected.
3. Apply DC power to the CELL200-series and NL200/201.

A.2.2 Configure the CELL200-series as a serial server

1. Connect a USB cable between a USB port on your computer and the USB port on the CELL200-series.
2. Starting with the default settings, open a web browser and go to: cell.linktodevice.com.

NOTE:

Cellular service must be setup before configuring the CELL200-series. See the CELL200-series manual for more information.

3. If the data logger has been assigned a **public static IP address**, on the **Settings > General** tab:
 - a. Enter the **APN** as assigned by your service provider.
 - b. Change **Mode** from PPP to **Serial Server**.
 - c. Click **Apply** to save the changes and then close the web browser.

4. If the data logger has been assigned a **private dynamic IP address** and you are using the *Konect PakBus Router* service, on the **Settings** tab:
 - a. **General** tab > Enter the **APN** as assigned by your service provider.
 - b. **General** tab > Change **Mode** from PPP to **Serial Server/Client**.
 - c. **Serial Mode Setup** > **URL** > Enter the Konect PakBus Router address.
 - d. **Serial Mode Setup** > **Port Number** > Enter the Konect PakBus Router port number.

NOTE:

Konect PakBus Router connections through a CELL200-series modem do not support a TCP Password. Contact Campbell Scientific support for more information.

A.2.3 NL200/201 physical setup

1. Connect the data logger to the NL200/201 using an Ethernet cable.
2. Apply 12 VDC power to the data logger and NL200/201..

A.2.4 Configure the NL200/201

1. Connect to the NL200/201 in *Device Configuration Utility* (see [Configuring the NL200/201](#) [p. 12]).
2. Click the **Factory Defaults** button at the bottom of the Deployment window.
3. On the **NL200 Series** tab, set **Bridge Mode** to **disable**.
4. If a dynamic address is to be used, the network information acquired via DHCP can be seen on the NL200 Series tab under **Status**. The **Status** box also displays the MAC address of the NL200/201.
5. 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. For the purposes of this example assume that both the NL200/201 and data logger are directly connected with an Ethernet cable. Use the following IP info: 192.168.1.2 with a subnet mask of 255.255.255.0.

6. On the **RS-232** tab:
 - a. Set **Configuration** to **PakBus**.
 - b. Set **Baud Rate** to baud rate of attached cellular modem. Generally this is **115200** (default).
 - c. Set **Beacon Interval** to **60** (seconds) and **Verify Interval** to **0**. If you want to restrict communications paths, use the **PakBus Neighbors Allowed** setting to specify allowed neighbor addresses.
7. On the **Network Services** tab, make note of the **PakBus/TCP Service Port**. The default **PakBus/TCP Service Port** is **6785**. Unless firewall issues exist, it is not necessary to change the port from its default value. This port number must match the port number entered in LoggerNet Setup after the IP address. See [Setup LoggerNet](#) (p. 40).

A.2.5 Configure the data logger

1. Connect to the data logger in *Device Configuration Utility*.
2. Click the **Factory Defaults** button at the bottom of the Deployment window.
3. On the **Datalogger** tab verify the **PakBus Address**.
4. On the **Ethernet** tab set:
 - a. **Ethernet Power** to **Always On**
 - b. **IP Address** to **192.168.1.1**
 - c. **Subnet Mask** to **255.255.255.0**

NOTE:

The **IP Gateway** does not need to be set.

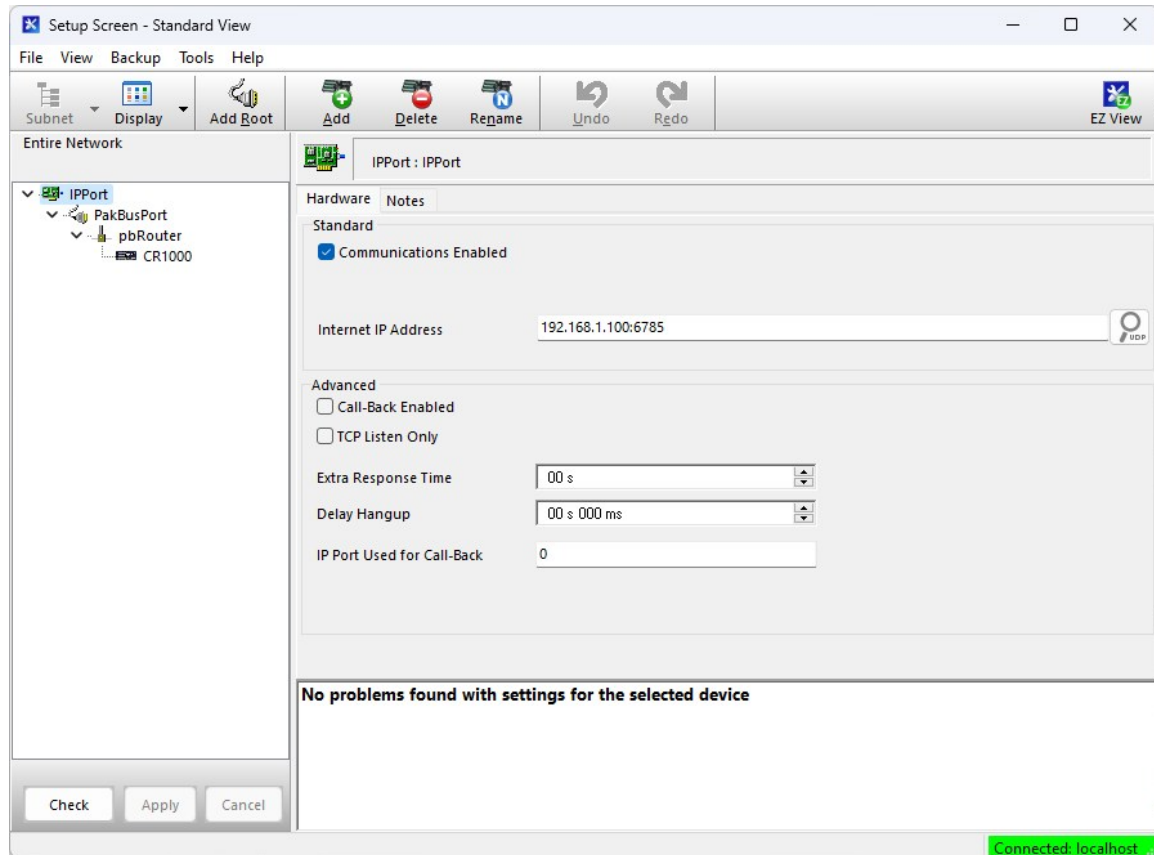
5. On the **Network Services** tab set the **PakBus/TCP Clients Address** to that of the NL200/201: **192.168.1.2**. This will cause the data logger to communicate with the NL200/201 over PakBus.
6. Click **Apply** to save the changes and then close *Device Configuration Utility*.

A.2.6 Setup LoggerNet

1. In the *LoggerNet* Setup screen, click **Add Root** and select **IPPort**. Enter the CELL200-series 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.

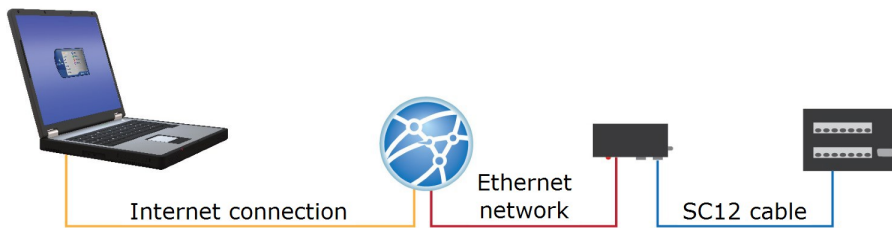
2. Add **PakBusPort (PakBus Loggers)**.
3. Add a PakBus Router (**pbRouter**). Enter the PakBus address of the NL200/201. The NL200/201 default PakBus address is **678**. Click **Close**.
4. Add the data logger and enter its PakBus address.
5. Click **Apply** to save the changes.



6. Ensure that your computer has a connection to the internet.
7. You are now ready to connect to your data logger using **LoggerNet**. Select **Main** and **Connect** on the **LoggerNet** toolbar, select the data logger from the **Stations** list, then **Connect**. From there, you can view and collect data, or manage data logger settings.

A.3 CR300 over IP to Konect

This type of network is useful for accessing a data logger remotely through a firewall, especially when the data logger, such as a CR300, lacks a CS I/O or Ethernet port.



A.3.1 NL200/201 physical setup

1. Connect the data logger and NL200/201 RS-232 ports using a straight-through RS-232 pin to socket cable such as an SC12.
2. Apply 12 VDC power to the data logger and NL200/201.

A.3.2 Configure the NL200/201

1. Connect to the NL200/201 in *Device Configuration Utility* (see [Configuring the NL200/201](#) [p. 12]).
2. Click the **Factory Defaults** button at the bottom of the Deployment window.
3. On the **NL200 Series** tab, set **Bridge Mode** to **disable**.
4. If a dynamic address is to be used, the network information acquired via DHCP can be seen on the NL200 Series tab under **Status**. The **Status** box also displays the MAC address of the NL200/201.
5. 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. For the purposes of this example assume that both the NL200/201 and data logger are directly connected with an Ethernet cable. Use the following IP info: 192.168.1.2 with a subnet mask of 255.255.255.0.
6. On the **RS-232** tab:
 - a. Set **Configuration** to **PakBus**.
 - b. Set **Baud Rate** to baud rate of attached device, generally this is **115200** (default).
 - c. Set **Beacon Interval** to **60** (seconds) and **Verify Interval** to **0**. If you want to restrict communications paths, use the **PakBus Neighbors Allowed** setting to specify allowed neighbor addresses.

7. On the **Network Services** tab set:
 - a. The **PakBus Address** of your Konect PakBus Router. The default is **678**.
 - b. The **PakBus/TCP Client Connection Address** to the Konect PakBus Router address.
 - c. The **PakBus/TCP Client Connection Port** to the Konect PakBus Router port.
 - d. The **PakBus/TCP Password** to the TCP Password configured on your Konect PakBus Router.
 - e. **ICMP Ping** to **enable**. For diagnostic purposes.
8. Click **Apply** to save the changes.

A.3.3 Configure the data logger (CR300)

1. Connect to the data logger in *Device Configuration Utility*.
2. Click the **Factory Defaults** button at the bottom of the Deployment window.
3. On the **Datalogger** tab verify that the **PakBus Address** is different than that set in the NL200/201.
4. On the **Com Ports Settings** tab set:
 - a. **ComPort** to **RS-232**
 - b. **Beacon Interval** to **60** (seconds)
5. Click **Apply** to save the changes and then close *Device Configuration Utility*.

A.3.4 Setup *LoggerNet*

1. In the *LoggerNet* Setup screen, click **Add Root** and select **IPPort**. Enter the Konect PakBus Router IP address and port number of the NL200/201. The Konect address was assigned when your account was setup. The IP address and port number are input on the same line separated by a colon. The fully qualified host name entry will look like **xxx.konectgds.com:6785**.
2. Add **PakBusPort (PakBus Loggers)**.
3. Enter the Konect PakBus Router **TCP Password**.
4. Add a PakBus Router (**pbRouter**). Enter **4070**, the PakBus address associated with Konect PakBus Routers. Click **Close**.
5. Add another PakBus Router (**pbRouter**). Enter the PakBus address of the NL200/201. The NL200/201 default PakBus address is **678**. Click **Close**.

6. Add the data logger and enter its PakBus address.

NOTE:

The CR300 and NL200/201 must have different PakBus addresses.

7. Click **Apply** to save the changes.
8. Ensure that your computer is connected to the same network as the NL200/201.
9. You are now ready to connect to your data logger using *LoggerNet*. Select **Main** and **Connect** on the *LoggerNet* toolbar, select the data logger from the **Stations** list, then **Connect**. From there, you can view and collect data, or manage data logger settings.

Appendix B. Cables, pinouts, LED function, and jumper

The following sections provide specific information about the hardware:

B.1 CS I/O	45
B.2 RS-232	46
B.3 Ethernet	46
B.4 USB	47
B.5 Power	48
B.6 LEDs	48
B.7 Power jumper (NL201 only)	48

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 is recommended. Pin configuration for the CS I/O port and connected peripheral device is shown in the following Table.

Pin	Data logger (DB9 socket) function	Peripheral (DB9 pin) 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

Pin	Data logger (DB9 socket) function	Peripheral (DB9 pin) function
8	12 VDC (output)	NL200: Not connected NL201: 12 VDC (input)
9	TXD	RXD

B.2 RS-232

A DB9 pin and socket cable is used to connect the NL200/201 RS-232 port to the data logger RS-232 port. A Campbell Scientific SC12 cable can also be used. A DB9 socket null modem cable is used to connect the NL200/201 RS-232 port to a computer RS-232 port. The RS-232 cable should be kept short when using high baud rates. Pin configurations for the RS-232 port of a data logger and peripheral device are shown in the following Table.

Pin	Data Logger (DCE, DB9 socket) function	Peripheral (DTE, DB9 pin) 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

Use a Category 5 or better Ethernet 10Base-T/100Base-TX twisted pair cable. 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 NL200/201 and the Ethernet repeater, hub, switch, or router it is connected to.

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

Use a USB A to micro B style cable for configuring the NL200/201.

Pin	Function
1	VBUS (not used)
2	Data -
3	Data +
4	Not connected
5	Ground

B.5 Power

Pin	Function
Center	7 to 20 VDC
Sleeve	Power ground-

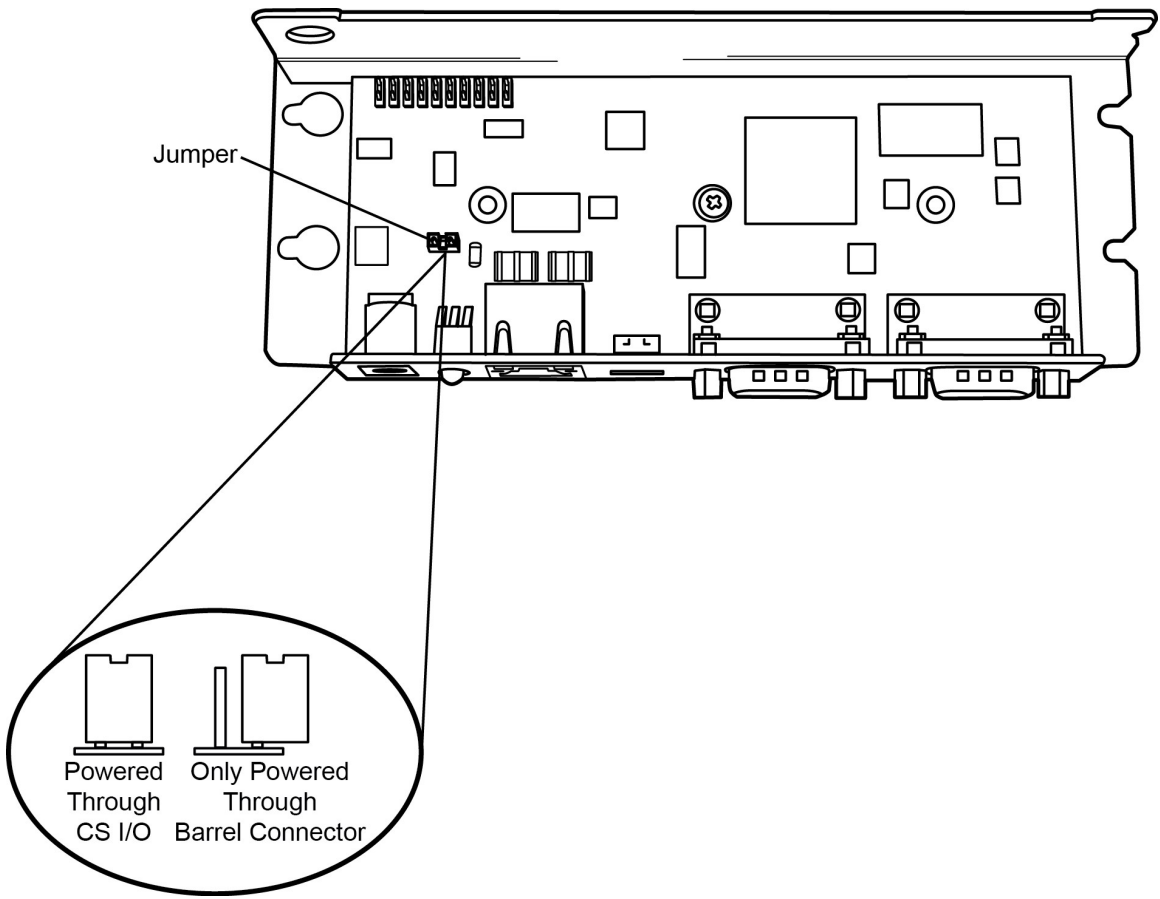
B.6 LEDs

State	Description
Off	Device powered off
On	Device powered on and ready
Flash	OS Download in progress – CAUTION: Do not disconnect power

State	Description
Yellow on	Valid Ethernet link
Yellow off	Ethernet link not valid
Yellow flash	Activity on Ethernet port
Green on	100Mbit/s link
Green off	10Mbit/s link

B.7 Power jumper (NL201 only)

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 top cover, remove the jumper above the mode button 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

The NL200/201 settings available from the **Settings Editor** in *Device Configuration Utility* are described as follows.

C.1 Main tab	50
C.2 RS-232 tab	54
C.3 CS I/O tab	57
C.4 Net Services tab	59
C.5 TLS Proxy Server tab	61
C.6 TLS tab	63

C.1 Main tab

C.1.1 Model (read only)

Model name.

C.1.2 Serial Number (read only)

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

C.1.3 OS Version (read only)

Operating system version currently in the NL200/201.

C.1.4 Compile Date (read only)

Operating system compile date.

C.1.5 Bridge Mode

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

Bridge Mode Disabled

With **Bridge Mode** set to **disable**, 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** set to **enable**, 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 data logger 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 data logger is sent intact as a complete Ethernet/TCP packet. This enables the data logger to use its TCP/IP stack to interpret the packet, and, therefore, all of the data logger 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 address, subnet mask, and default gateway) are configured in the data logger. 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 Device Configuration Utility. 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.

C.1.6 CS I/O IP Interface Identifier

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

C.1.7 Bridge Mode Forward Code

When the device is configured for bridge mode, it forwards Ethernet packets to the data logger. Because the device is aware of the MAC address and IP address being used by the data logger, 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 data logger 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 data logger IP communications. If desired, other codes may be entered to filter out certain packet types.

A packet is forwarded to the data logger 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 (0xFFFFB): Clear bit 2 to forward all relevant packets except UDP Broadcast packets. Filtering UDP broadcasts will disable the data logger ability to respond to Device Configuration Utility 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 data logger is on an IPv6-enabled network but not required to respond to any IPv6-related traffic.

C.1.8 DHCP

When **DHCP** (Dynamic Host Configuration Protocol) is set to **enable**, the device will 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, refresh by pressing F5.

C.1.9 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** box on the **Deployment > NL200 Series** tab. (It is recommended to configure a static IP address.)

NOTE:

In bridge mode, this setting is obtained from the data logger and cannot be edited here. It must be edited in the data logger settings. The setting obtained from the data logger will be displayed in the **Status** box on the **Deployment > NL200 Series** tab.

C.1.10 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** box on the **Deployment > NL200 Series** tab.

NOTE:

In bridge mode, this setting is obtained from the data logger and cannot be edited here. It must be edited in the data logger settings. The setting obtained from the data logger will be displayed in the **Status** box on the **Deployment > NL200 Series** tab.

C.1.11 Default Gateway

Packets 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** box on the **Deployment > NL200 Series** tab.

NOTE:

In bridge mode, this setting is obtained from the data logger and cannot be edited here. It must be edited in the data logger settings. The setting obtained from the data logger will be displayed in the **Status** box on the **Deployment > NL200 Series** tab.

C.1.12 DNS 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.

C.1.13 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.

C.1.14 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.

C.1.15 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 **Device Configuration Utility** over TCP and Telnet. 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.

C.1.16 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. Typically, it is not necessary to change this entry from its default (range 1 to 65535).

C.2 RS-232 tab

C.2.1 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** 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 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** 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.

C.2.2 RS-232 Service Port

This setting is used when the **RS-232 Configuration** is set to **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 to 65535).

C.2.3 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.

C.2.4 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 (**enable**).

C.2.5 RS-232 TCP Timeout (seconds)

This setting determines how fast the device will time out on the open TCP connection. For Serial Server and **MODBUS/TCP 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 to 999 seconds).

C.2.6 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 RS-232 port in order to discover any new PakBus neighboring nodes. It will also govern the default verification interval if the value of the **RS -232 PakBus Verify Interval** setting for the associated port is 0.

C.2.7 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 communications has taken place within the interval.

C.2.8 Neighbors Allowed RS-232

This setting specifies the explicit list of PakBus node addresses that the NL200/201 will accept as neighbors on the RS-232 port. 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 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
```

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

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

C.2.9 RS-232 Modbus Timeout

This setting determines how long, in milliseconds, the MODBUS/TCP to MODBUS/RTU gateway will wait for an answer from the MODBUS server (formerly called 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).

C.2.10 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.

C.2.11 RS-232 TCP Serial Client Port

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

C.3 CS I/O tab

C.3.1 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** 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** 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.

C.3.2 CS I/O Service Port

This setting is used when the **CS I/O Configuration** is set to **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 serial server is set. Typically, it is not necessary to change this entry from its default (range 1 to 65535).

C.3.3 SDC Address

Communications with the data logger via the **CS I/O** port is done using SDC (Synchronous Device Communications). The data logger 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.

C.3.4 CS I/O TCP Timeout

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

C.3.5 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 **CS I/O** port in order to discover any new PakBus neighboring nodes. It will also govern the default verification interval if the value of the **CS I/O Verify Interval** setting is set to 0.

C.3.6 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 communications has taken place within the interval.

C.3.7 CS I/O Modbus Timeout

This setting determines how long, in milliseconds, the MODBUS/TCP to MODBUS/RTU gateway will wait for an answer from the MODBUS server (formerly called 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).

C.4 Net Services tab

C.4.1 Telnet

Enables/Disables the Telnet service.

C.4.2 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 to 65535).

C.4.3 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 to 999).

C.4.4 Ping (ICMP)

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

C.4.5 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 data logger 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 neighbors allowed list 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 neighbors allowed list.

C.4.6 PakBus/TCP Service Port

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

C.4.7 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 service port. If the client fails to respond appropriately, the connection will be terminated. If this password is blank (the default value), no authentication will take place.

C.4.8 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 that connection periodically until a connection is made. No entry or a setting of 0.0.0.0 specifies that no client connection will be made.

C.4.9 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 to 65535).

C.4.10 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.

C.4.11 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

C.5.1 TLS Proxy Server

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

NOTE:

If the TLS Proxy Server is enabled and a data logger is connected to the **CS I/O** port, the data logger will load its TCP stack in case it is required to do TCP communications. Running the TCP stack causes the data logger 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.

C.5.2 TLS Proxy Service 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 set to **CS I/O Port**, the

NL200/201 will open a TCP connection with the data logger over the CS I/O port and do unencrypted data transfer with the data logger. If the **TLS Proxy Forward Physical Port** is set to **Ethernet**, 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 **TLS Proxy Service Port**, the NL200/201 will attempt to open a TCP connection to the data logger on the **TLS Proxy Forward Port**. 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 data logger on the HTTP port 80 (range 1 to 65535).

C.5.3 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 open a TCP connection with the data logger over the CS I/O port and do unencrypted data transfer with the data logger. If the **TLS Proxy Forward Physical Port** is specified to be **Ethernet**, the NL200/201 will open the TCP connection over Ethernet on the **TLS Proxy Forward IP Address**.

C.5.4 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 does not need to be set by the user since the NL200/201 will obtain the IP address of the data logger automatically. The data logger must be configured with a static IP address that is unique and that exists on the same subnet as the NL200/201 IP address. If the **TLS Proxy Forward Physical Port** is specified to be **Ethernet**, the forward IP address must be specified. Enter the IP address of the destination data logger here.

C.5.5 TLS Proxy Forward 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 open a TCP connection with the data logger over the CS I/O port

and do unencrypted data transfer with the data logger. If the **TLS Proxy Forward Physical Port** is specified to be **Ethernet**, the NL200/201 will open the TCP connection over Ethernet on the **TLS Proxy Forward IP Address**.

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

If secure communications come in on the **TLS Proxy Service Port**, the NL200/201 will attempt to open a TCP connection to the data logger on the **TLS Proxy Forward Port**. 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 data logger on the HTTP port 80.

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

C.5.6 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 to 999).

C.6 TLS tab

C.6.1 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 *Device Configuration Utility* 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 *Device Configuration Utility* link (USB or TLS). These settings cannot be edited over a standard TCP *Device Configuration Utility* link.

C.6.2 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 *Device Configuration Utility* link is considered secure (USB or TLS). If the TLS stack has been initialized, the device will automatically negotiate a secure TLS connection with *Device Configuration Utility* if the **Use TCP** option is selected.

C.6.3 TLS Private Key

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

NOTE:

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

C.6.4 TLS Certificate

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

NOTE:

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

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

Whenever a new operating system (OS) 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. Plug the wall charger into an AC outlet and the barrel connector into the NL200/201 power jack.
2. Connect a USB cable between one of your computer USB ports and the **USB** port on the NL200/201.
3. Open *Device Configuration Utility*.
4. Under **Device Type**, select **Network Peripheral > NL200 Series**.
5. Select the appropriate **Communication Port**.
6. Go to the **Send OS** tab.
7. Click **Start**.
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 click **OK**.
9. The operating system will be sent to the NL200/201.
10. After the file has been sent, the power LED on the NL200/201 will flash repeatedly while the NL200/201 copies the OS into its internal flash. Depending upon the operating system that was previously installed, it may take up to 2 minutes for the NL200/201 to finish updating the operating system. While the LED is flashing, the NL200/201 is in a vulnerable state where a removal of power could leave the NL200/201 without a valid operating system to run. Do not remove power until the LED stops flashing.

D.2 Sending an OS via IP

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

1. Using the supplied serial cable, connect the NL200/201 **CS I/O** port to the data logger **CS I/O** port. Alternatively, power the NL200/201 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 *Device Configuration Utility*.
4. Select the NL200 Series under **Device Type**.
5. Ensure that the **Use IP Connection** box is checked on the left-hand panel.
6. If the Admin Password of the device has been set, 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 Communications 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 **Browse** to the right of Communications 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. Click **Start**.
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 click **OK**.
11. The operating system will be sent to the NL200/201.
12. After the file has been sent, the power LED on the NL200/201 will flash repeatedly while the NL200/201 copies the OS into its internal flash. Depending upon the operating system that was previously installed, it may take up to 2 minutes for the NL200/201 to finish updating the operating system. While the LED is flashing, the NL200/201 is in a vulnerable state where a removal of power could leave the NL200/201 without a valid operating system to run. Do not remove power until the LED stops flashing.

Appendix E. Glossary

A

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.

B

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.

D

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.

H

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.

M

MIMO

Multiple-input, multiple-output antenna

N

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.

P

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 or service to which a network message is to be forwarded when it arrives at the NL200/201. For example, FTP often uses port 21 while HTTP uses port 80.

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 as 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.

S

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.

T

TLS (Transport Layer Security)

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

V

Verify Interval

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


Limited warranty

Covered equipment is warranted/guaranteed against defects in materials and workmanship under normal use and service for the period listed on your sales invoice or the product order information web page. The covered period begins on the date of shipment unless otherwise specified. For a repair to be covered under warranty, the following criteria must be met:

1. There must be a defect in materials or workmanship that affects form, fit, or function of the device.
2. The defect cannot be the result of misuse.
3. The defect must have occurred within a specified period of time; and
4. The determination must be made by a qualified technician at a Campbell Scientific Service Center/ repair facility.

The following is not covered:

1. Equipment which has been modified or altered in any way without the written permission of Campbell Scientific.
2. Batteries; and
3. Any equipment which has been subjected to misuse, neglect, acts of God or damage in transit.


Campbell Scientific regional offices handle repairs for customers within their territories. Please see the back page of the manual for a list of [regional offices](#) or visit www.campbellsci.com/contact  to determine which Campbell Scientific office serves your country. For directions on how to return equipment, see [Assistance](#).

Other manufacturer's products, that are resold by Campbell Scientific, are warranted only to the limits extended by the original manufacturer.

CAMPBELL SCIENTIFIC EXPRESSLY DISCLAIMS AND EXCLUDES ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Campbell Scientific 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.


Campbell Scientific will, as a default, return warranted equipment by surface carrier prepaid. However, the method of return shipment is at Campbell Scientific's sole discretion. Campbell Scientific will not reimburse the claimant for costs incurred in removing and/or reinstalling equipment. This warranty and the Company's obligation thereunder is in lieu of all other

warranties, expressed or implied, including those of suitability and fitness for a particular purpose. Campbell Scientific is not liable for consequential damage.

In the event of any conflict or inconsistency between the provisions of this Warranty and the provisions of Campbell Scientific's Terms, the provisions of Campbell Scientific's Terms shall prevail. Furthermore, Campbell Scientific's Terms are hereby incorporated by reference into this Warranty. To view Terms and conditions that apply to Campbell Scientific, Logan, UT, USA, see [Terms and Conditions](#) . To view terms and conditions that apply to Campbell Scientific offices outside of the United States, contact the [regional office](#) that serves your country.

Assistance

Products may not be returned without prior authorization. Please inform us before returning equipment and obtain a **return material authorization (RMA) number** whether the repair is under warranty/guarantee or not. See [Limited warranty](#) for information on covered equipment.

Campbell Scientific regional offices handle repairs for customers within their territories. Please see the back page of the manual for a list of [regional offices](#) or visit www.campbellsci.com/contact  to determine which Campbell Scientific office serves your country.

When returning equipment, a RMA number must be clearly marked on the outside of the package. Please state the faults as clearly as possible. Quotations for repairs can be given on request.

It is the policy of Campbell Scientific to protect the health of its employees and provide a safe working environment. In support of this policy, when equipment is returned to Campbell Scientific, Logan, UT, USA, it is mandatory that a "[Declaration of Hazardous Material and Decontamination](#)" form be received before the return can be processed. If the form is not received within 5 working days of product receipt or is incomplete, the product will be returned to the customer at the customer's expense. For details on decontamination standards specific to your country, please reach out to your [regional Campbell Scientific](#) office.

NOTE:

All goods that cross trade boundaries may be subject to some form of fee (customs clearance, duties or import tax). Also, some regional offices require a purchase order upfront if a product is out of the warranty period. Please contact your [regional Campbell Scientific](#) office for details.

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 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

- Protect from over-voltage.
- Protect electrical equipment from water.
- Protect from electrostatic discharge (ESD).
- Protect from lightning.
- 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, 6 meters (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.
- Only use power sources approved for use in the country of installation to power Campbell Scientific devices.

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.

Internal Battery

- Be aware of fire, explosion, and severe-burn hazards.
- Misuse or improper installation of the internal lithium battery can cause severe injury.

- Do not recharge, disassemble, heat above 100 °C (212 °F), solder directly to the cell, incinerate, or expose contents to water. Dispose of spent batteries properly.

Use and disposal of batteries

- Where batteries need to be transported to the installation site, ensure they are packed to prevent the battery terminals shorting which could cause a fire or explosion. Especially in the case of lithium batteries, ensure they are packed and transported in a way that complies with local shipping regulations and the safety requirements of the carriers involved.
- When installing the batteries follow the installation instructions very carefully. This is to avoid risk of damage to the equipment caused by installing the wrong type of battery or reverse connections.
- When disposing of used batteries, it is still important to avoid the risk of shorting. Do not dispose of the batteries in a fire as there is risk of explosion and leakage of harmful chemicals into the environment. Batteries should be disposed of at registered recycling facilities.

Avoiding unnecessary exposure to radio transmitter radiation

- Where the equipment includes a radio transmitter, precautions should be taken to avoid unnecessary exposure to radiation from the antenna. The degree of caution required varies with the power of the transmitter, but as a rule it is best to avoid getting closer to the antenna than 20 cm (8 inches) when the antenna is active. In particular keep your head away from the antenna. For higher power radios (in excess of 1 W ERP) turn the radio off when servicing the system, unless the antenna is installed away from the station, e.g. it is mounted above the system on an arm or pole.

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.

Global Sales and Support Network

A worldwide network to help meet your needs



Campbell Scientific Regional Offices

Australia

Location: Garbutt, QLD Australia
Phone: 61.7.4401.7700
Email: info@campbellsci.com.au
Website: www.campbellsci.com.au

Brazil

Location: São Paulo, SP Brazil
Phone: 11.3732.3399
Email: vendas@campbellsci.com.br
Website: www.campbellsci.com.br

Canada

Location: Edmonton, AB Canada
Phone: 780.454.2505
Email: dataloggers@campbellsci.ca
Website: www.campbellsci.ca

China

Location: Beijing, P. R. China
Phone: 86.10.6561.0080
Email: info@campbellsci.com.cn
Website: www.campbellsci.com.cn

Costa Rica

Location: San Pedro, Costa Rica
Phone: 506.2280.1564
Email: info@campbellsci.com
Website: www.campbellsci.com

France

Location: Montrouge, France
Phone: 0033.0.1.56.45.15.20
Email: info@campbellsci.fr
Website: www.campbellsci.fr

Germany

Location: Bremen, Germany
Phone: 49.0.421.460974.0
Email: info@campbellsci.de
Website: www.campbellsci.de

India

Location: New Delhi, DL India
Phone: 91.11.46500481.482
Email: info@campbellsci.in
Website: www.campbellsci.in

Japan

Location: Kawagishi, Toda City, Japan
Phone: 048.400.5001
Email: jp-info@campbellsci.com
Website: www.campbellsci.co.jp

South Africa

Location: Stellenbosch, South Africa
Phone: 27.21.8809960
Email: sales@campbellsci.co.za
Website: www.campbellsci.co.za

Spain

Location: Barcelona, Spain
Phone: 34.93.2323938
Email: info@campbellsci.es
Website: www.campbellsci.es

Thailand

Location: Bangkok, Thailand
Phone: 66.2.719.3399
Email: info@campbellsci.asia
Website: www.campbellsci.asia

UK

Location: Shephed, Loughborough, UK
Phone: 44.0.1509.601141
Email: sales@campbellsci.co.uk
Website: www.campbellsci.co.uk

USA

Location: Logan, UT USA
Phone: 435.227.9120
Email: info@campbellsci.com
Website: www.campbellsci.com