PRODUCT MANUAL

Communications Device

NL241

Wireless Network Link Interface

Revision: 04/2024

RELIABLE MONITORING SINCE 1974

Campbell SCIENTIFIC®

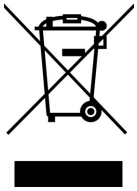
Please read first

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 European 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 British/European 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 European 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

The NL241 is a WLAN (wireless local area network) interface that allows Campbell Scientific data loggers and peripherals to communicate with a Wi-Fi network. The NL241 can either join an existing network or create a network. This WLAN interface can be connected to a data logger **CS I/O** port or **RS-232** port.

2. Precautions

- READ AND UNDERSTAND the Safety section at the back of this manual.
- The first time an NL241 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 NL241 is attached, it can take up to 10 seconds for the data logger to recognize it.
- This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. See Radio frequency emission (p. 72) for more information. Radio installations should be performed by a professional. It is very important that the transmit power level selected and the gain of the attached antenna do not exceed the maximum allowed ERP permitted by local regulations. Regulations vary by country and region. As the equipment owner, you are responsible for making sure that your installation and maintenance of the radio equipment ensure local regulations are met.
- Use the newest version of ***Device Configuration Utility*** to communicate with the NL241. It can be downloaded from our website at www.campbellsci.com/downloads.
- Install the device driver before plugging the NL241 into your computer for the first time. The device driver must be properly installed before you can connect to the NL241 via USB.

  To install the device driver, download the latest version of ***Device Configuration Utility*** from our website. Under **Device Type**, select **Network Peripheral** > **NL241**. Click **Install USB Driver** and follow the prompts.
- CR1000, CR3000, and CR800-series data loggers require operating system version 25 or newer in order to operate with the NL241 in bridge mode. (OS version 25 or newer is not

required to operate as a serial server or PakBus®[1] router.) The latest operating systems can be downloaded at www.campbellsci.com/downloads.

- Ensure maximum protection against surges. Use coaxial surge protection. Keep RS-232 and CS I/O cables short.
- When downloading a new operating system to the NL241, do not remove power until the LED stops rapidly flashing red and green.

3. QuickStart

Out of the box, the NL241 is configured for operation as a PakBus router and to create an open Wi-Fi network called "NL241_*SerialNumber*". In this mode, the NL241 can be used to communicate with Campbell Scientific PakBus devices using a Wi-Fi-enabled device such as a smart phone. The following instructions indicate how to use an NL241 to connect to a data logger using a smart phone with the Campbell Scientific ***LoggerLink*** Mobile App.

3.1 Physical setup

As shown in Figure 3-1 (p. 3), attach an antenna to the NL241 **Antenna** connector. Using the supplied serial cable, connect the NL241 CS I/O port to the data logger **CS I/O** port. This cable supplies communications and power from the data logger to the NL241. Ensure that the device is powered by inspecting the LED. The LED will be solid red when the device is connecting to or creating a Wi-Fi network. When the LED starts flashing green, it is ready for Wi-Fi communications. For more information see Link/Activity LED (p. 46).

[1]PakBus® is a registered trademark of Campbell Scientific, Inc.

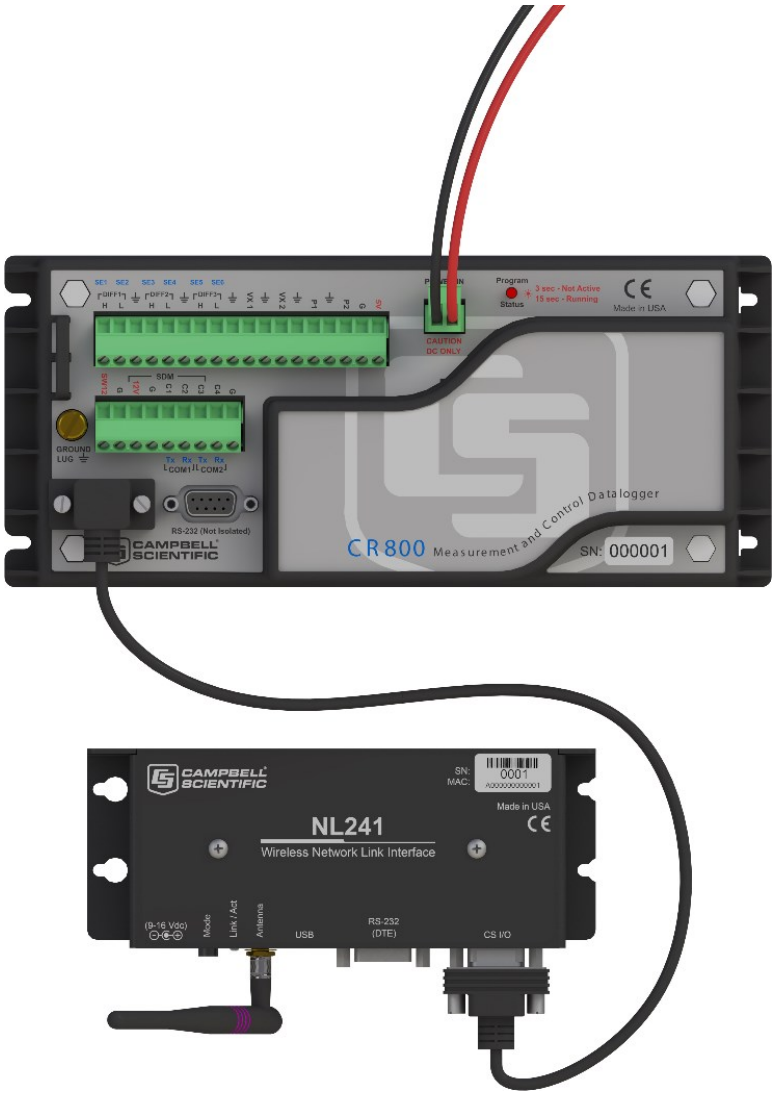


Figure 3-1. NL241 with CR800 (powered through CS I/O port)

3.2 Configuring the NL241

NOTE:
Install the device driver before plugging the NL241 into your computer for the first time. The device driver must be properly installed before you can connect to the NL241 via USB.

To install the device driver, download the latest version of ***Device Configuration Utility*** from our website. Under **Device Type**, select **Network Peripheral** > **NL241**. Click **Install USB Driver** and follow the prompts.

1. Apply power to the NL241.
2. Connect the supplied USB cable between a USB port on your computer and the **USB** port on the NL241.
3. Open ***Device Configuration Utility***.
4. Under **Device Type**, select **Network Peripheral** > **NL241**.
5. Click **Browse** ... next to **Communication Port**.
6. Select the virtual com port labeled **NL241**.
7. Click **OK**.
8. Click **Connect**.
9. Click the **Wi-Fi** tab.
10. By default, the NL241 will create an unsecured Wi-Fi network. The name of this network will be "NL241_*SerialNumber*." To change the name of this network, type a new name in the **Network Name (SSID)** field. Optionally, to enable encryption, type a password in the **Password** field. See NL241 settings (p. 49) for details on the password requirements.
11. Click the **NL241** tab.
12. The default IP address of the NL241 is shown in the **Status** field and will be **192.168.67.1**. To change the address, select **disable** in the **DHCP Enabled** field. Then type the **IP Address**, **Network Mask**, and **Default Gateway**.
13. Click **Apply** to save the changes.

3.3 *Loggerlink* setup

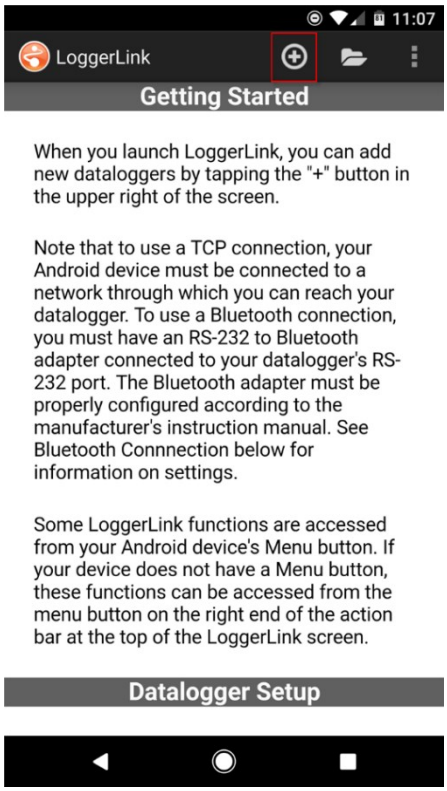
The next step is to download ***LoggerLink*** and configure it to connect to the data logger via the NL241.

1. ***LoggerLink*** is a free app downloadable from Google Play and the Apple App Store. Download and install the app.

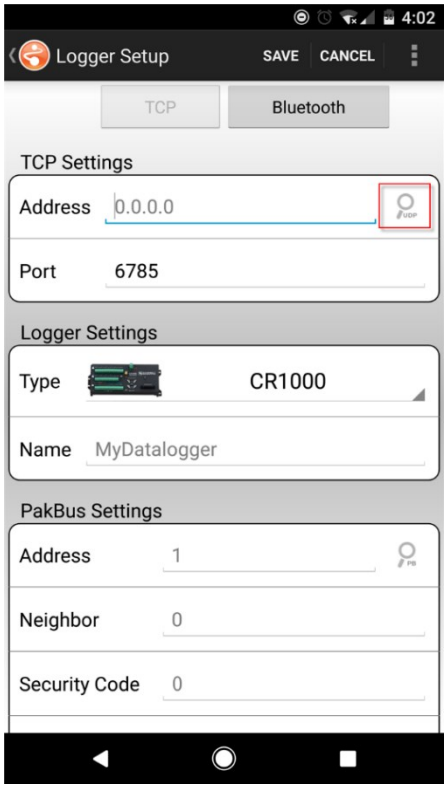
2. Connect your iOS or Android device to the Wi-Fi network created by the NL241 ("NL241_ *SerialNumber*," by default).

> NOTE:
> Android users may get a message saying there is no internet access and be asked if you want to stay connected. Select the **Don't ask again for this network** check box and click **YES**.

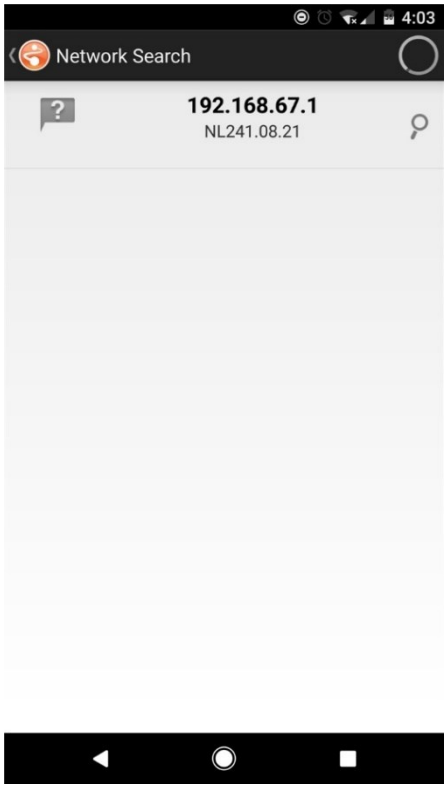
3. In the ***LoggerLink*** **Getting Started** screen, press the **+** key to add a data logger.



4. With **TCP** selected, click the **UDP** icon next to the **Address** field to automatically discover IP devices on the network.

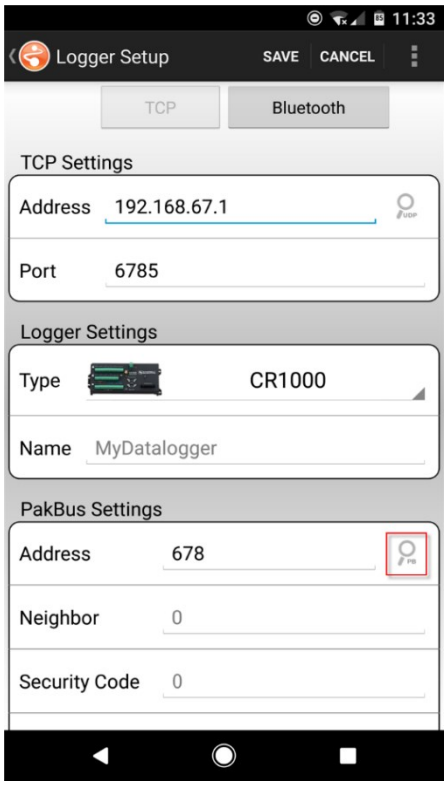


5. Select the NL241 (address 192.168.67.1 by default).

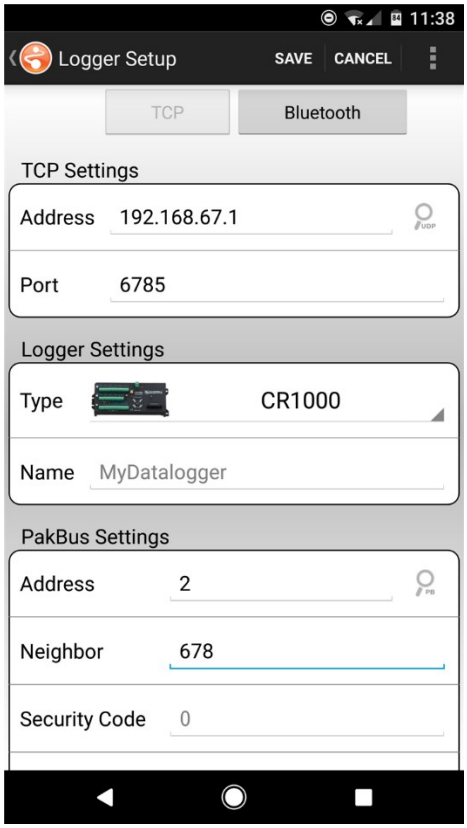


6. The following screen appears. Click the **PB** icon to cause ***LoggerLink*** to search for attached PakBus devices.

> NOTE:
> For the PakBus search to work with the NL241, you must have ***LoggerLink*** version 1.6 or later.



7. The data logger should be discovered automatically. Select the data logger, and all necessary fields in the Logger Setup screen will be filled in automatically. To enter the information by hand, manually type the IP address of the NL241 in the **Address** field under **TCP Settings**. Leave the **Port** at 6785. Select the data logger **Type**. Type the PakBus address of the data logger (default is 1) in the **Address** field under **PakBus Settings**. Type the NL241 PakBus address (default is 678) in the **Neighbor** field. The following screen shows the correct information filled in for a CR1000 with PakBus address of 2.



8. Type a name for your data logger in the **Name** field. If your data logger has a **Security Code**, **TCP Password**, or **Encryption Key**, type those in the corresponding field.
9. Click **SAVE** to save the changes.

3.4 Connect

You are now ready to connect to your data logger using ***LoggerLink***. Select the data logger from the ***LoggerLink*** home screen and ***LoggerLink*** will connect to the data logger. From there, you can view and collect data, or manage data logger settings.

4. Overview

The NL241 Wireless Network Link Interface is designed for communications with Campbell Scientific data loggers and peripherals over a Wi-Fi network.

The NL241 includes a **CS I/O** port and an **RS-232** port for communications. A **USB** port is used for configuring the NL241 device.

Some reasons to use each of these modes are described below. Refer to Configuring the NL241 (p. 22) and Operation (p. 25) for information on setting up your NL241 for each mode.

Campbell Scientific ***LoggerNet*** software is used to communicate with the data loggers once the NL241 is configured properly and connected to a network.

Bridge Mode

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

> 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.

Bridge Mode disabled

- With Bridge Mode disabled, the NL241 can provide multiple services simultaneously including TCP Serial Server, TCP Serial Client, Modbus TCP/IP Gateway, and PakBus router. The NL241 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 NL241 can act as TLS proxy server. The TLS proxy server is independent of other modes.

Serial Server

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

PakBus Router

- Allows access to a CR10X-PB over a Wi-Fi network.
- Allows access to a CR200X over a Wi-Fi 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 WLAN.
- Allows multiple computers to concurrently talk to PakBus devices connected to the **RS-232** and **CS I/O** ports.

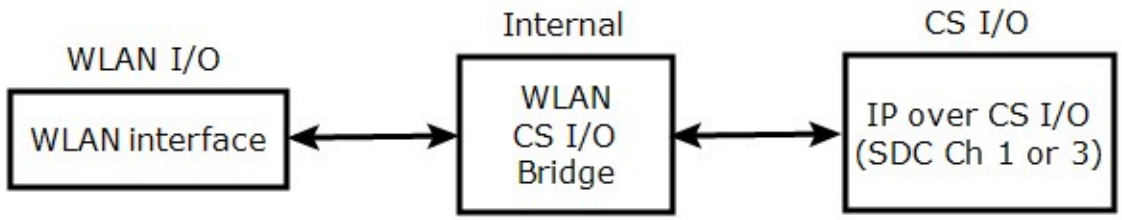
TLS Proxy Server

- Adds an encrypted WLAN interface to a data logger that supports CS I/O IP (bridge mode) communications.

4.1 Bridge mode enabled

The NL241 can be configured to bridge WLAN 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

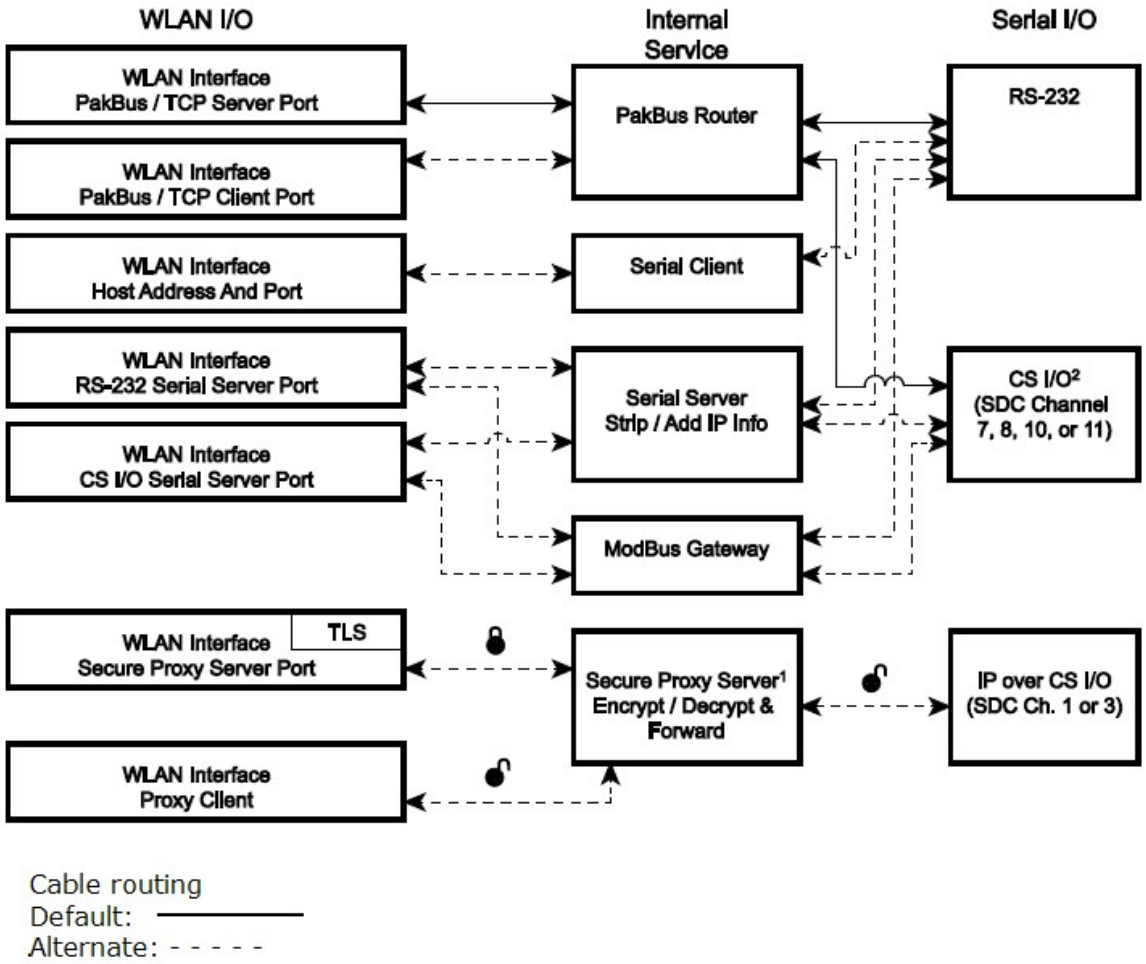
does not use PPP. Instead, raw IP packets are transferred between the WLAN and CS I/O connections.



> 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 NL241 can provide multiple services simultaneously including TCP Serial Server, TCP Serial Client, Modbus TCP/IP Gateway, and PakBus router. The NL241 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 NL241 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 WLAN 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.

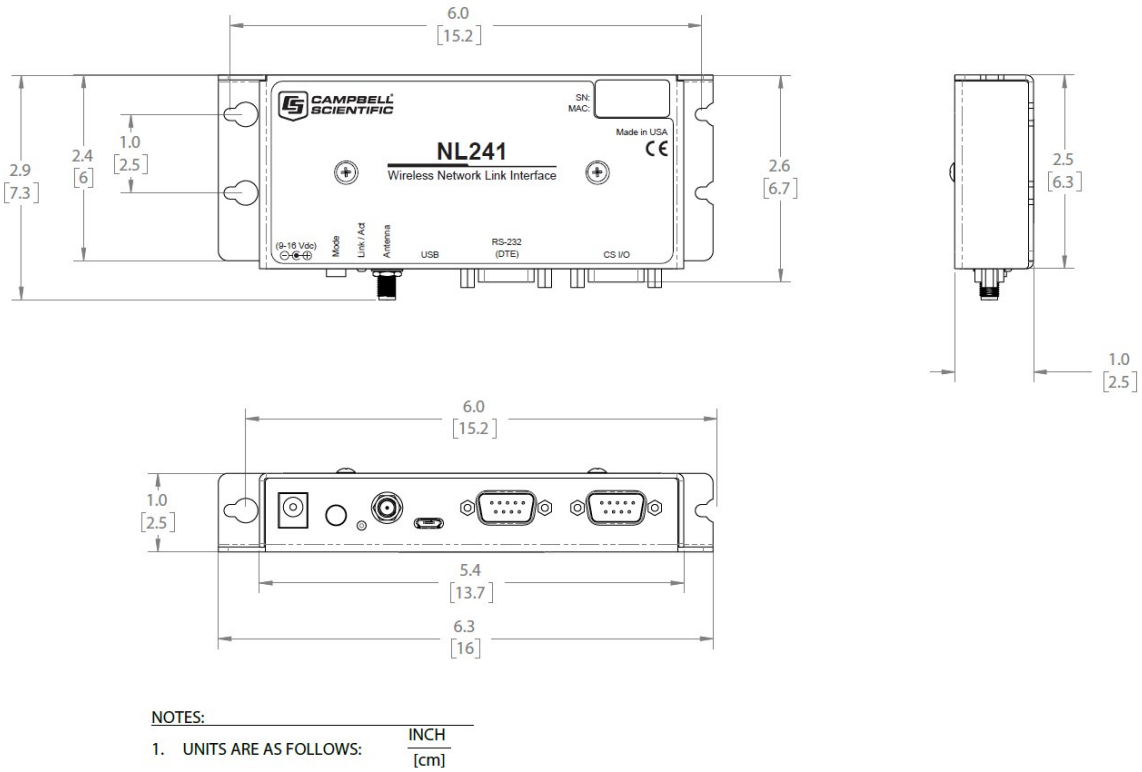
[2] Secure Proxy Server operation through the **CS I/O** port is independent of PakBus and Serial Server operations.

5. Specifications

General

180.35 g (6.36 oz)

16 x 7.3 x 2.54 cm (6.3 x 2.9 x 1 in)



Power input

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

9 to 16 VDC

> **NOTE:**
> To prevent the NL241 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.

Typical Power Consumption (@ 12VDC)

Client Mode: 7.5 to 8 mA idle, 65 to 75 mA communicating

Access Point Mode: 67 mA idle, 70 mA communicating

Standby: less than 1.5 mA

> **NOTE:**
> Standby power is when the NL241 Wi-Fi power has been turned off. This state can be enabled by configuration of the **Mode** button or by using the `IPNetPower()` data logger instruction. See the CRBasic help for an example of using the `IPNetPower()` instruction.

> Note that the `IPNetPower()` instruction is only applicable when the NL241 is configured with bridge mode enabled. See Mode button (p. 20) for information on the **Mode** button configuration.

Operating Temperature

Standard: –40 to 70 °C

Configuration

Device Configuration Utility over USB or Wi-Fi

Telnet console over Wi-Fi

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

WLAN

Antenna Connector: RP-SMA

Supported Technologies: 802.11b/g/n, WPA/WPA2-Personal, WPA/WPA2-Enterprise Security, WEP

Client Mode: WPA/WPA2-Personal and Enterprise, WEP

Access Point Mode: WPA2-Personal

Communications Rate:

- 802.11b: up to 11Mbps
- 802.11g: up to 54 Mbps
- 802.11n: up to 72 Mbps

Frequency: 2.4 GHz

Transmit Power: 7 to 18 dBm (5 to 63 mW)

Rx Sensitivity: –97 dBm

Supported Protocols

IPv4, IPv6, ICMP/Ping, ICMPv6/Ping, TCP/IP, DHCP Client, DHCP Server (in Access Point Mode only), SLAAC, DNS Client, HTTPS Proxy, TLS, Telnet Server, PakBus, Modbus

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

CE Compliant

Complies with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules.

Contains an embedded radio transmitter with the following approvals:

FCC Identifier: XF6-RS9113SB

Industry Canada: 8407A-RS9113SB

View documents at: www.campbellsci.com/nl241

6. Wi-Fi

Wi-Fi is a technology that allows data transfer among electronic devices using specific radio frequencies over a wireless local area network (WLAN). A wireless network is like a wired network, except it uses radio waves just like cell phones, televisions, and other radios. Over-the-air speeds vary depending on protocol, distance, and network activity. When using the NL241, please note that your total throughput to the data logger will generally be governed by the speed of serial communications.

Wi-Fi transmits at frequencies around 2.4 and 5 GHz (the NL241 only uses 2.4 GHz). The high frequency allows fast rates but reduced communications distance. These frequencies can be used by anyone and do not require a license from the FCC to use or transmit (unlike most UHF and VHF frequencies) as long as certain power levels are maintained.

The NL241 supports the 802.11b, 802.11g, and 802.11n wireless network standards.

The NL241 also supports several wireless security protocols. These include WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) (personal), WPA2 (Wi-Fi Protected Access II) (personal),

and WPA/WPA2-Enterprise. These security protocols allow network traffic to be encrypted and help protect data transmitted over the Wi-Fi network.

> TIP:
> WEP is an old technology and is not secure. We recommend that you configure your networks to use WPA2 technology.

6.1 Wireless network modes

6.1.1 Join a network

The NL241 can be configured to join an already established infrastructure wireless network (WLAN) (see Figure 6-1 [p. 17]). An infrastructure wireless network is one in which all devices or stations (STA) communicate through an access point (AP). This AP will typically connect the wireless network (and the NL241) to a larger wired company or home network and/or the internet. The AP device also controls and routes all the traffic on the wireless network. Once the NL241 has successfully joined the existing wireless network, it can communicate with other devices on the network.

The AP, furthermore, controls security for network access, the wireless frequency (channel) to use, and has the pre-established Service Set Identifier (SSID) for the wireless network. The SSID (or network name) and password/key (if required) can be obtained from your network administrator.

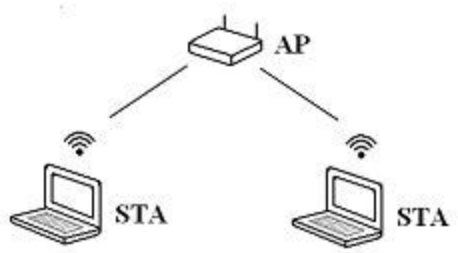


Figure 6-1. Infrastructure network

6.1.2 Create a network

The NL241 can be configured to create a network. In this mode, it acts as the access point which other Wi-Fi enabled devices can join. If this configuration is enabled, the user may set an SSID (network name) and password. If a password is supplied, the network created will be secured by

WPA2 encryption. If no password is supplied, the network created will be an open network with no encryption.

If this mode is selected, the channel may be specified manually using the **Channel** setting in the **Settings Editor**. If the **Channel** setting is left at the default setting **Auto**, the device will only use channels 1, 6, and 11 on which to operate to minimize interference from other networks detected in the area.

When manually selecting a channel, it should be noted that two Wi-Fi networks operating on the same channel will interfere with each other and will have to compete for bandwidth. The center frequencies of adjacent channels are 5 MHz apart and the bandwidth of each channel is 20 MHz which means that adjacent channels overlap. To completely avoid interference there must be a spacing of at least 5 channels between each Wi-Fi network. It is therefore recommended to use channels 1, 6, and 11. For a list of all the wireless networks in the area and the associated channels on which they operate, see the **Settings Editor** > **Wi-Fi Wireless Networks in Area** box.

A network created by the NL241 supports up to 8 joinees.

6.1.3 DHCP server in a created network

When configured to create a network, the device will run a DHCP server to assign addresses to joinees of the network. The beginning address of the DHCP server pool is the address of the device plus 100. In the case that the device address ends in 135 or above, the beginning address of the DHCP server pool is the address of the device minus 100. There are 20 entries in the DHCP server pool, thus the ending address in the pool is the beginning address plus 20. By default, the device uses a server address of 192.168.67.1. In this case, the pool of addresses is 192.168.67.101 – 192.168.67.120. If the device address is 192.168.67.135, the pool of addresses would be 192.168.67.35 – 192.168.67.55. Any connecting devices running a DHCP client will be assigned an address in this range. If static IP addressing is desired, assign addresses outside of the range of the DHCP address pool (while observing the network mask).

If an IP address is supplied in the **IP Address** user setting, that address will be used as the DHCP server address. The beginning address in the DHCP server pool will still be the address of the server plus or minus 100. The ending address in the pool will be the beginning address plus 20.

6.2 RSSI

RSSI is received signal strength indication. It is a generic radio receiver technology metric used to determine the strength of the link between a receiver and a transmitter. In the case of the NL241, RSSI is the measurement between the NL241 and a wireless access point. The strength of this link is recorded in dBm (power ratio in decibels) and can be found on the **Wi-Fi** tab in the **Settings Editor** of *Device Configuration Utility*.

RSSI in the NL241 is measured in a scale between –100 dBm and 0 dBm. The higher the number (for example, –12 dBm as compared to –72 dBm), the better the connection between Wi-Fi devices. A reliable connection will be maintained if the RSSI reading in the NL241 stays between –85 dBm and –15 dBm. A weak, and thus intermittent, connection will have readings between –85 dBm and –95 dBm. For every 3 dBm increase, the NL241 is receiving twice as much signal (radiated power). For every 3 dBm lost, the NL241 is receiving 50% less signal.

To improve your RSSI readings, shorten antenna cable lengths and use frequency-matched antennas with higher gain. An NL241 with a 0 db gain antenna can achieve ranges of up to 32 meters (120 feet) indoors and 95 meters (300 feet) outdoors. Ranges can be improved by installing higher gain antennas on both the NL241 and/or the wireless access point. Remember that RSSI can also be affected by weather, vegetation, terrain, interference, and antenna cable length and type.

6.3 Antennas

Antenna selection and placement can greatly affect the strength of the signal transmitted and received and therefore can impact the quality of communications. The NL241 should be paired with an antenna designed for Wi-Fi communications at 2.4 GHz (2.401 to 2.483 GHz). Ideally the antenna will be connected directly to the NL241 or positioned in such a way as to minimize coaxial cable length. Note that coaxial cables attenuate signals more as frequency increases; take care when selecting the type and length of coaxial cable used with the NL241. The NL241 antenna connector is RP-SMA male. When connecting directly to the NL241, select a coaxial cable or antenna with a mating RP-SMA female connector.

6.4 Power

One advantage of using the NL241 in your application is its low power consumption capabilities. With careful planning, you can reduce your station power needs while still meeting critical communications needs. See Specifications (p. 13) (Typical Power Consumption) and Wi-Fi tab (p. 53) for more details.

6.5 LED

There is a bi-color LED on the NL241 that serves as an indicator as described below.

> NOTE:
> This manual describes LED behavior for NL241s with operating system 10.05 or newer. It is recommended that the latest operating system be used. See Sending a new OS to the NL241 (p. 69).

6.5.1 Normal operation

After power-up, the LED turns solid green while the NL241 is searching for and trying to join a Wi-Fi network. The LED turns solid amber when creating a network.

After successfully joining or creating a network, the LED will flash with network activity. Note that the LED may only flash once every few seconds on the created network or networks that are not very busy. For more information see Link/Activity LED (p. 46).

If the device is unsuccessful at joining or creating a network, the LED will periodically double-flash red. The device will attempt to connect to the network again after approximately one minute.

If the Wi-Fi has been disabled via the **Mode** button configuration, or via an `IPNetPower()` instruction from the data logger, the LED will be off. See Mode button (p. 20) for information on the **Mode** button configuration.

6.5.2 Operating system upgrade

When a new operating system is sent to the NL241, the LED will flash repeatedly while the NL241 copies the operating system into its internal flash memory. This process takes about 10 seconds. While the LED is flashing, the NL241 is in a vulnerable state where removal of power could leave the NL241 without a valid operating system. Do not remove power until the LED resumes normal operation.

If an operating system upgrade includes an upgrade to the internal Wi-Fi module firmware, after the typical re-flashing of the LED, the device will power up and start copying the new firmware to the Wi-Fi module. The LED will also flash during this process. It will start out as a slow flash and get faster and faster as the process nears completion. This process can take up to two minutes. Again, do not remove power until the LED resumes normal operation. For more information see Link/Activity LED (p. 46).

6.6 Mode button

The behavior of the **Mode** button is determined by the **Mode Button Configuration** setting on the *Device Configuration Utility* **Wi-Fi** tab.

The following graphic illustrates the possible Wi-Fi and **Mode** button configurations.

Configuration:

1. Wi-Fi Config: Join a Network
   Button Config: Temporarily Enable Wi-Fi
2. Wi-Fi Config: Join a Network
   Button Config: Temporarily Create a Network
3. Wi-Fi Config: Create a Network
   Button Config: Temporarily Enable Wi-Fi
4. Wi-Fi Config: Create a Network
   Button Config: Temporarily Create a Network

	Boot Up	Button Pressed	Timeout (or button pressed again)
1.	Wi-Fi disabled	join configured network	Wi-Fi disabled again
2.	join configured network	create NL241_nnnn network	join the original network again
3.	Wi-Fi disabled	create configured network	Wi-Fi disabled again
4.	Wi-Fi disabled	create configured network	Wi-Fi disabled again

6.6.1 Disable button

If this configuration is selected, pressing the button will have no effect on the operation of the device. The Wi-Fi network will continue to work as configured.

6.6.2 Temporarily enable Wi-Fi

If this configuration is selected, the configured Wi-Fi network will normally be disabled, and it will be activated temporarily when the button is pressed.

6.6.3 Temporarily create a network

If this configuration is selected, the device will temporarily create a network when the button is pressed. If the Wi-Fi **Configuration** is set to **Join a Network**, the temporarily created network will be an open network with the name "NL241_*SerialNumber*." If the Wi-Fi **Configuration** is set to **Create a Network**, the configured Wi-Fi network will normally be disabled and it will be temporarily activated when the button is pressed.

Note that when the Wi-Fi **Configuration** is set to **Create a Network**, the device behavior is the same for both button configurations.

6.6.4 Temporary network duration

When the **Mode** button is used to temporarily enable or create the Wi-Fi network, it will stay powered for at least 5 minutes. There is a 2-minute timeout that is refreshed every time communications are detected. Once the timeout has expired, the device will power off the network.

If the **Mode** button is pressed again while the temporary network is active, the device will power off the network.

7. Configuring the NL241

The NL241 is configured using ***Device Configuration Utility*** 2.15 or greater connected using either a Wi-Fi connection or USB.

7.1 Configuring the NL241 with *Device Configuration Utility* via USB

> NOTE:
> Install the device driver before plugging the NL241 into your computer for the first time. The device driver must be properly installed before you can connect to the NL241 via USB.
>
> To install the device driver, download the latest version of ***Device Configuration Utility*** from our website. Under **Device Type**, select **Network Peripheral** > **NL241**. Click **Install USB Driver** and follow the prompts.

1. Apply power to the NL241.
2. Connect the supplied USB cable between a USB port on your computer and the **USB** port on the NL241.
3. Open ***Device Configuration Utility***.
4. Under **Device Type**, select **Network Peripheral** > **NL241**.

5. Click **Browse** ... next to **Communication Port**.
6. Select the port labeled **NL241**.
7. Click **OK**.
8. Click **Connect**.
9. Configure the NL241 as needed for your application.
10. Click **Apply** to save the changes.

7.2 Configuring the NL241 with *Device Configuration Utility* via Wi-Fi WLAN

> **NOTE:**
> The NL241 is configured by default to host an open Wi-Fi network and have an IP address of 192.168.67.1. The network name will follow the pattern "NL241_*SerialNumber*."

1. Apply power to the NL241.
2. The NL241 will power up and either create or join a Wi-Fi network. After successfully joining or creating a network, the LED will flash with network activity. Note that the LED may only flash once every few seconds on the created network or an idle network.
3. If the device is configured to create a network, the computer must join the NL241-created network. If the NL241 has been previously configured to join a network, join the same network with your computer.
4. Open ***Device Configuration Utility***.
5. Under **Device Type**, select **Network Peripheral** > **NL241**.
6. Select **Use IP Connection**.
7. 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.) The IP address must be followed by **:6786** (for example, 192.168.10.55:6786) in order to connect the device configuration service.
8. Type **NL241** in the **Administrative Password** box. (**nl241** is the default administrative password. It can be changed via the ***Device Configuration Utility*** **Deployment** > **NL241** tab.)
9. Click **OK**.
10. Click **Connect**.

11. Configure the NL241 as needed for your application.
12. Click **Apply** to save the changes.

7.3 Configuring the NL241 with Telnet via Wi-Fi WLAN

> NOTE:
> For security reasons, Telnet is disabled by default. It must be enabled from the **Network Services** tab in *Device Configuration Utility*.
>
> The NL241 must have an IP address before connecting via Telnet. Configuration via Telnet is not available in bridge mode.

1. Apply power to the NL241.
2. The NL241 will power up and either create or join a Wi-Fi network. After successfully joining or creating a network, the LED will flash with network activity. Note that the LED may only flash once every few seconds on the created network or an idle network.
3. If the device is configured to create a network, the computer must join the NL241-created network. If the NL241 has been previously configured to join a network, join the same network with your computer.
4. Create a Telnet session with the NL241 over port 23.
5. Type **NL241** in the **Administrative Password** box. (**nl241** is the default administrative password. It can be changed via the *Device Configuration Utility* **Deployment** > **NL241** tab.)
6. Type **help** to see a list of the functionality available when connected to the NL241.
7. Type **edit** and press **Enter** to edit the settings of the NL241.
8. As each NL241 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.
9. After progressing through all of the NL241 settings, type **save** to accept the changes or **cancel** to discard the changes.
10. Type **bye** to exit the Telnet session.

7.4 Configuring the NL241 via RS-232

> NOTE:
> Accessing the configuration terminal menu via RS-232 requires the NL241 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 NL241.

1. Using a null modem serial cable, connect your computer serial port to the **RS-232** port on the NL241.
2. Connect to the NL241 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 NL241 and repeatedly press **Enter** at the terminal.
4. Type **help** to see a list of the functionality available when connected to the NL241.
5. Type **edit** and press **Enter** to edit the settings of the NL241.
6. As each NL241 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 NL241 settings, type **save** to accept the changes or **cancel** to discard the changes.
8. Disconnect your computer and power cycle the NL241.

8. Operation

This section describes how to configure the Wi-Fi connection and operational mode of your NL241. See Wi-Fi (p. 16) for more information about the types of Wi-Fi connections available. See Overview (p. 10) for help in determining which operational mode to use.

8.1 Wi-Fi connection

8.1.1 Join an existing network

In this configuration, the device will scan for available infrastructure networks and attempt to join the network specified by the SSID setting.

1. Connect to the NL241 in ***Device Configuration Utility*** (see Configuring the NL241 [p. 22]).
2. Click the **Wi-Fi** tab.
3. Set **Configuration** to **Join a Network**.
4. Click **Browse** ... next to the **Network Name (SSID)** field to see a list of the available networks in the area. To join a hidden network, manually enter its SSID. Select the network you wish to connect to and click **OK**.
5. If this is a secured network, enter the password in the **Password** field.
6. Click **Apply** to save the changes.

> NOTE:
> If for some reason the device cannot join the desired network (for example, out of range or incorrect parameters), it will go to a low-power state and periodically retry to join the network approximately once every minute. If the device has successfully joined a network and then detects a loss of connectivity with the network, it will begin periodically searching for the network at approximately the one-minute interval.

8.1.2 Create a network

In this configuration, the device will be the creator of a network. A network created by the module supports up to 8 joinees.

> NOTE:
> Please remember when joining a network with Windows or iOS, it can take some time to successfully join the network.

1. Connect to the NL241 in ***Device Configuration Utility*** (see Configuring the NL241 [p. 22]).
2. Click the **Wi-Fi** tab.
3. Set **Configuration** to **Create a Network**.
4. By default, the NL241 will create an unsecured Wi-Fi network. The name of this network will be "NL241_*SerialNumber*." To change the name of this network, type a new name in the **Network Name (SSID)** field. Optionally, to enable encryption, type a password in the **Password** field. See NL241 settings (p. 49) for details on the password requirements.
5. Other Wi-Fi settings are available from the **Settings Editor**, but can often be left at their default values. See Wi-Fi tab (p. 53) for more information on these settings.
6. Click **Apply** to save the changes.

8.2 Operational mode

8.2.1 PakBus router

When the **RS-232** or **CS I/O** port is configured as a PakBus router, the NL241 can route packets to other devices in the network that it has in its routing table. These are devices that the NL241 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 NL241 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 NL241 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 NL241 expects to hear from within set intervals (the Verify Interval). If the NL241 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.

8.2.1.1 Physical setup

Using the supplied serial cable, connect the NL241 **CS I/O** port or **RS-232** port to the data logger **CS I/O** or **RS-232** port, respectively. The NL241 will be powered if connected via CS I/O. Alternatively, power the NL241 through the barrel-connector jack located on the edge of the device. Connect the NL241 to your local wireless network by attaching an antenna to the NL241 **Antenna** connector. Ensure that the device is powered up by inspecting the LED.

8.2.1.2 Configuring the NL241

RS-232 PakBus router

1. Connect to the NL241 in ***Device Configuration Utility*** (see Configuring the NL241 [p. 22]).
2. On the **NL241** 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.
    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.)

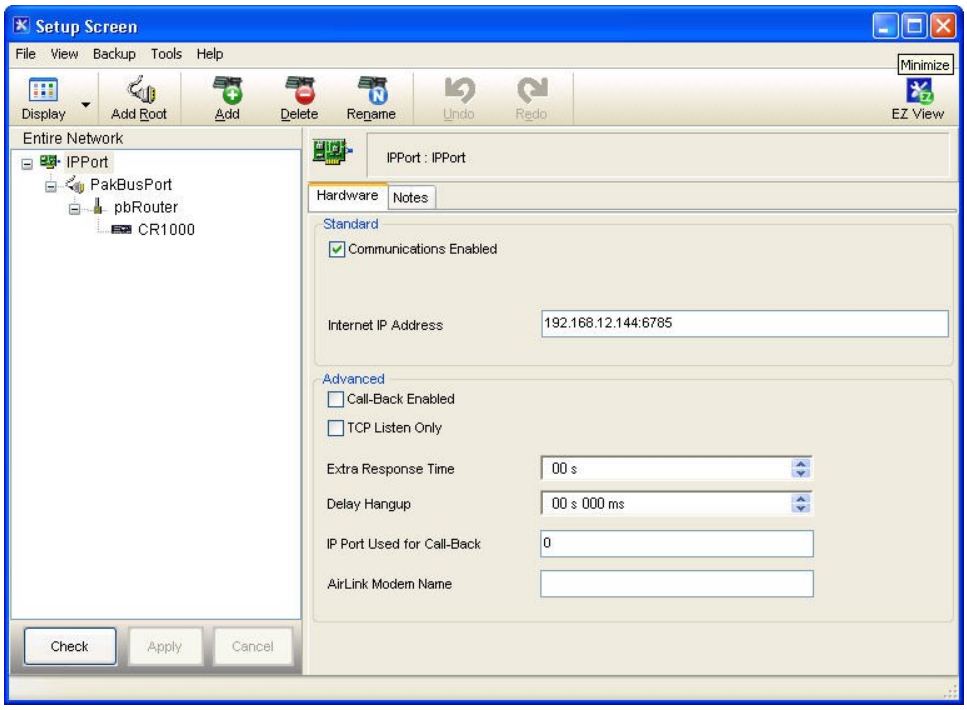
CS I/O PakBus Router

1. Connect to the NL241 in ***Device Configuration Utility*** (see Configuring the NL241 [p. 22]).
2. On the **NL241** 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.)

8.2.1.3 *LoggerNet* setup

1. In the ***LoggerNet*** Setup screen, click **Add Root** and select **IPPort**. Enter the NL241 IP address and port number. The IP address and port number are input on the same line separated by a colon.
2. Add a PakBus Port (**PakBusPort**).
3. Add a PakBus Router (**pbRouter**). Type the PakBus address of the NL241. The NL241 default PakBus address is **678**.
4. Add the data logger and type the PakBus address of the data logger.
5. Click **Apply** to save the changes.



8.2.1.4 Connect

You are now ready to connect to your data logger using ***LoggerLink***. Select the data logger from the ***LoggerLink*** home screen and ***LoggerLink*** will connect to the data logger. From there, you can view and collect data, or manage data logger settings.

8.2.2 Bridge mode

With bridge mode enabled, the device will act as a bridge from WLAN to CS I/O. All IP packets that come into the device via WLAN 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, only the Wi-Fi 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**.

8.2.2.1 Physical setup

As shown in 8.2.2.1 (p. 30), attach an antenna to the NL241 **Antenna** connector. Using the supplied serial cable, connect the NL241 CS I/O port to the data logger **CS I/O** port. This cable supplies communications and power from the data logger to the NL241. Ensure that the device is

powered by inspecting the LED. The LED will be solid red when the device is connecting to or creating a Wi-Fi network. When the LED starts flashing green, it is ready for Wi-Fi communications.

8.2.2.2 Configuring the NL241

Connect to the NL241 in ***Device Configuration Utility*** (see Configuring the NL241 [p. 22]). On the **NL241** tab, set **Bridge Mode** to **enable**.

> NOTE:
> In bridge mode, the IP address, subnet mask, and IP gateway to be used by the NL241 are configured in the data logger.

8.2.2.3 Configuring the data logger

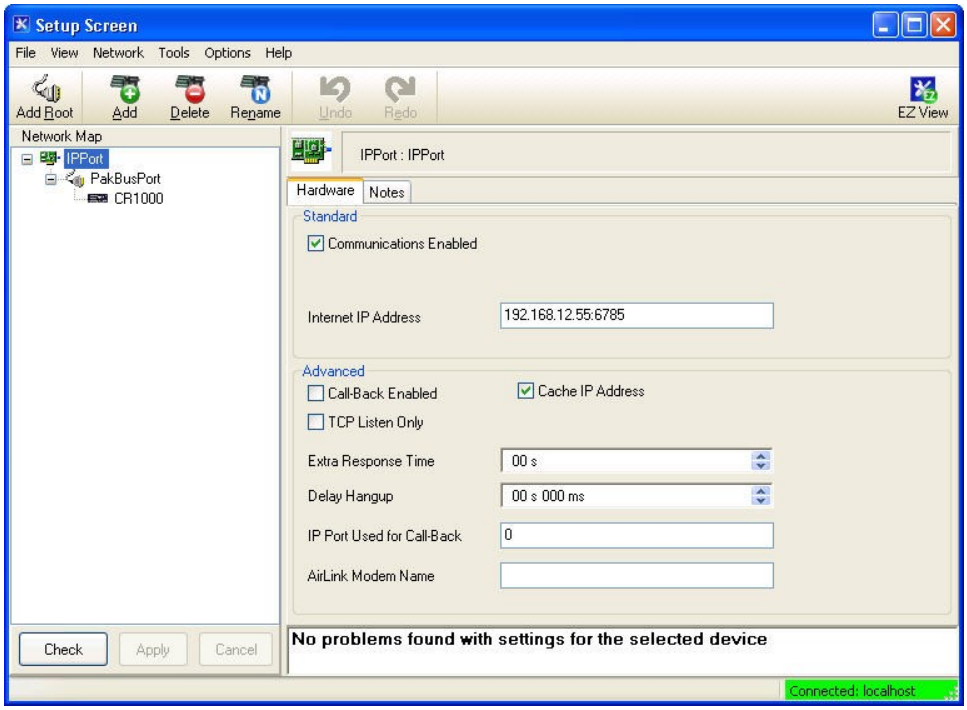
> NOTE:
> The NL241 must be connected to the data logger before configuring the data logger with ***Device Configuration Utility***. If it is not connected, the Ethernet settings will not be displayed.
>
> By default, the NL241 uses the data logger CS I/O Interface #2. If connecting more than one NL241 to a data logger, one NL241 can be configured to use CS I/O Interface #1. This is done by connecting to the NL241 in ***Device Configuration Utility***, going to the **Settings Editor** > **CS I/O IP** tab, and changing the **CS I/O IP Interface Identifier** from **2** to **1**. If this setting is changed, the IP address, subnet mask, and IP gateway should be input under CS I/O IP #1 on the data logger **CS I/O IP** tab. CS I/O Interface #2 communicates over SDC address 1. CS I/O Interface #1 communicates over SDC address 3.

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 NL241 is CS I/O IP Interface #2 (SDC1). 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***.

8.2.2.4 *LoggerNet* setup

The next step is to run ***LoggerNet*** and configure it to connect to the data logger via the **Wi-Fi** port. (See the following screen shot.) Note that the ***LoggerNet*** computer must be part of the same network that the NL241 has joined or created.

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 a PakBus Port (**PakBusPort**).
3. Add the data logger and type the PakBus address of the data logger.
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.



8.2.2.5 Connect

You are now ready to connect to your data logger using ***LoggerLink***. Select the data logger from the ***LoggerLink*** home screen and ***LoggerLink*** will connect to the data logger. From there, you can view and collect data, or manage data logger settings.

8.2.3 TCP serial server

The NL241 can tunnel RS-232 and CS I/O serial communications over Wi-Fi. Any packet sent to the configured IP port will have the IP layer removed, the data is then directed to the serial connection.

8.2.3.1 Physical setup

Using the supplied serial cable, connect the NL241 **CS I/O** port or **RS-232** port to the data logger **CS I/O** or **RS-232** port, respectively. The NL241 will be powered if connected via CS I/O. Alternatively, power the NL241 through the barrel-connector jack located on the edge of the device. Connect the NL241 to your local wireless network by attaching an antenna to the NL241 **Antenna** connector. Ensure that the device is powered up by inspecting the LED.

8.2.3.2 Configuring the NL241

RS-232 Serial server

1. Connect to the NL241 in ***Device Configuration Utility*** (see Configuring the NL241 [p. 22]).
2. On the **NL241** 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.
    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.

CS I/O serial server

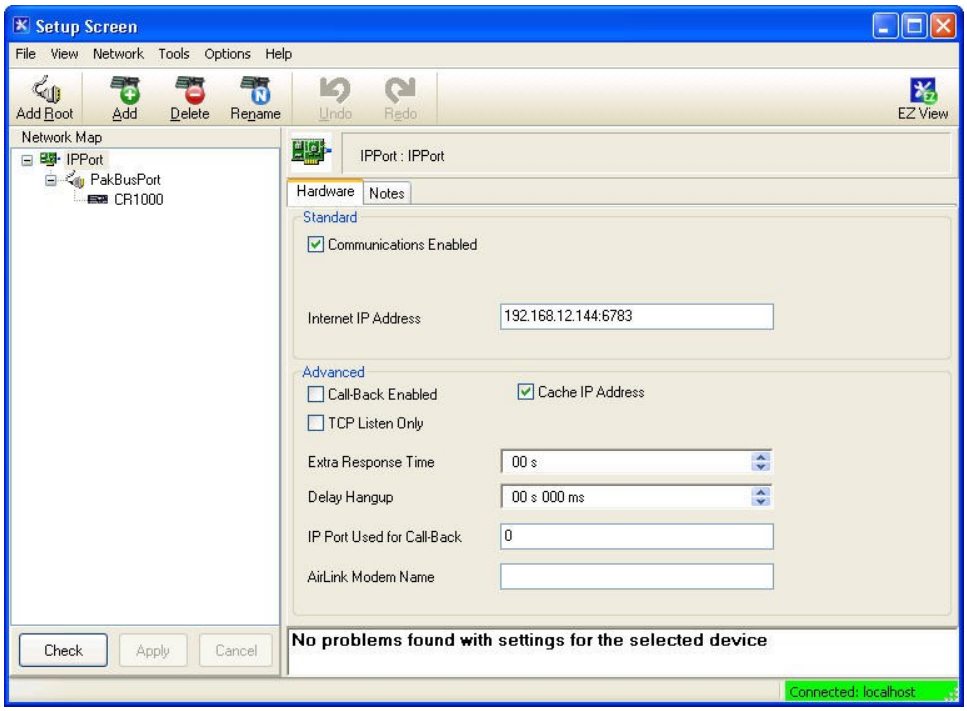
1. Connect to the NL241 in ***Device Configuration Utility*** (see Configuring the NL241 [p. 22]).
2. On the **NL241** tab, set **Bridge Mode** to **disable**.

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.

8.2.3.3 *LoggerNet* setup

The next step is to run ***LoggerNet*** and configure it to connect to the data logger via the **Wi-Fi** port. (See the following screen shot.) Note that the ***LoggerNet*** computer must be part of the same network that the NL241 has joined or created.

1. In the ***LoggerNet*** Setup screen, click **Add Root** and select **IPPort**. Enter the NL241 IP address and port number. The IP address and port number are input on the same line separated by a colon. The NL241 default **Port** number is **6783**. Unless firewall issues exist, it is not necessary to change the port from its default value.
2. Add a PakBus Port (**PakBusPort**).
3. Add the data logger and type the PakBus address of the data logger.
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.



8.2.3.4 Connect

You are now ready to connect to your data logger using ***LoggerLink***. Select the data logger from the ***LoggerLink*** home screen and ***LoggerLink*** will connect to the data logger. From there, you can view and collect data, or manage data logger settings.

8.2.3.5 Serial sensors

The NL241 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 NL241.

8.2.4 TCP Serial Client

When the RS-232 port is configured as **TCP Serial Client**, the NL241 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 NL241 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 NL241 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.

8.2.5 Modbus TCP/IP to RTU Gateway

The NL241 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 NL241 will convert incoming Modbus TCP/IP frames to Modbus RTU and forward them to the RS-232 (or CS I/O) port. The NL241 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 NL241 is connected directly to a CR800 series, CR1000, or CR3000 being polled by a Modbus TCP/IP client, the NL241 is most commonly configured with bridge mode enabled instead of as a Modbus TCP/IP to RTU Gateway.

8.2.6 TLS

The NL241 supports transport layer security (TLS) for proxy functions including HTTPS. TLS versions 1.0, 1.1, and 1.2 are supported. The TLS implementation supports symmetric algorithms AES-256, AES-128, and RC4 and RSA keys up to 4096 bits. For any TLS connection, the unit will preferentially use AES-256, then AES-128, and finally RC4. X.509 certificates are supported, with the exception of v3 extensions. Certificates should be PEM (privacy-enhanced mail) format. Up to 10 certificates can be chained. 10 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 NL241 is provided so that secure, encrypted communications can be established between a TLS client and the NL241. With the TLS proxy server enabled, the NL241 can act as a TLS proxy server for a data logger. The NL241TLS 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 NL241 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 NL241 with a user-supplied TLS private key and TLS certificate. The key and certificate are loaded using *Device Configuration Utility*.

1. Connect to the NL241 in *Device Configuration Utility* (see Configuring the NL241 [p. 22]).
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 NL241 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 NL241 will automatically negotiate a secure TLS connection with *Device Configuration Utility* as long as the **Use IP Connection** option is selected.

8.2.6.1 TLS proxy server

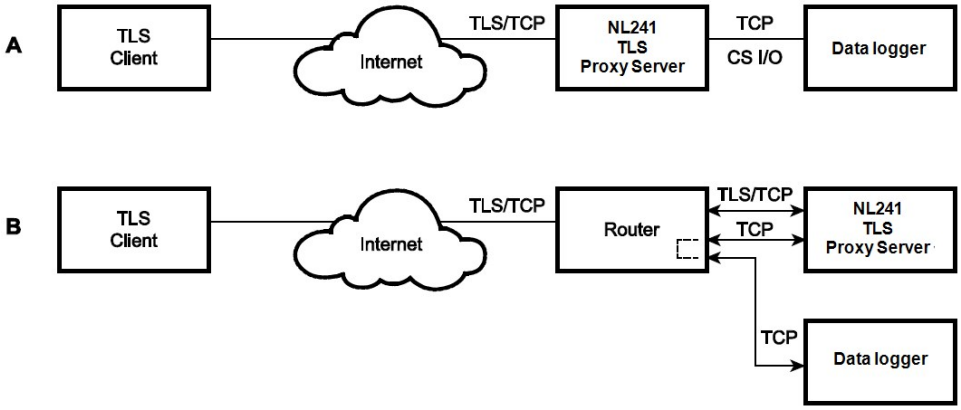
A TLS proxy server is a device that acts as a secure intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting some service, such as a file, connection, webpage, or other resource, available from a different server. The proxy server 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 NL241 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 NL241 TLS proxy server, and the NL241 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 NL241 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 NL241 TLS proxy server to communicate with a data logger attached to the **CS I/O** port or with a data logger over a Wi-Fi connection, open ***Device Configuration Utility*** and configure the following settings.

Settings Editor > **TLS Proxy Server** tab

Configuration A

In Configuration A, the NL241 decrypts TLS traffic and forwards the unencrypted TCP traffic to the data logger over the **CS I/O** port. The NL241 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 NL241 in ***Device Configuration Utility*** (see Configuring the NL241 [p. 22]).
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 NL241**CS I/O IP Interface Identifier** setting.

Configuration B

In Configuration B, the NL241 decrypts TLS traffic and forwards the unencrypted TCP traffic to the data logger back out on the Wi-Fi port. The user must specify an IP address and TCP port number for the forwarding TCP connection.

1. Connect to the NL241 in ***Device Configuration Utility*** (see Configuring the NL241 [p. 22]).
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 NL241 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 NL241 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 **Wi-Fi** 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 NL241 IP address. For example, if the NL241 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 NL241 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 NL241 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 NL241 IP address. For example, if the NL241 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 NL241.

The data logger must be listening on the same TCP port that the NL241 is configured to forward TCP traffic on (NL241 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.

8.2.6.2 *Device Configuration Utility* TCP encrypted communications to the NL241

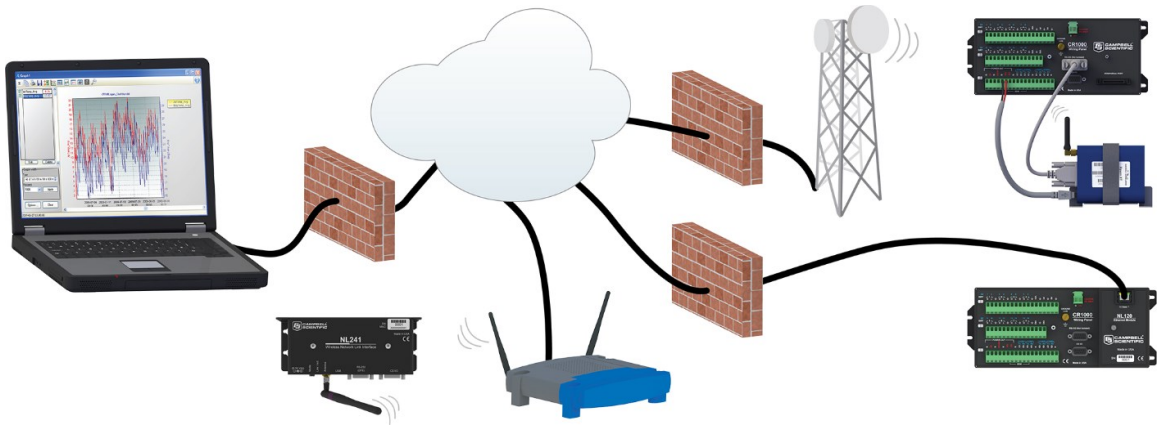
In order to use ***Device Configuration Utility*** TCP encrypted communications with the NL241, you will need to load the TLS private key and TLS certificate into the NL241. This is done from the **Settings Editor** > **TLS** tab in ***Device Configuration Utility***. Once the private key and certificate 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 NL241 IP address (or click **Browse** ... to select it from a list of NL241s connected to the network) and click **Connect**.

> NOTE:
> If the status of the TLS stack is **Initialized**, the NL241 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 NL241.
>
> When the NL241 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.

9. Working around firewalls

The NL241 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 NL241 must be on a public IP address and will act as a common meeting place for all PakBus communications.



9.1 Configuring the NL241

Connect to the NL241 in *Device Configuration Utility* (see Configuring the NL241 [p. 22]).

1. On the **NL241** 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**.

9.2 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 NL241**IP 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*.

10. Troubleshooting

This section covers some common problems that might be encountered when using the NL241. 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 NL241, do the following:

1. Check all the power connections.

   Your NL241 and any wireless access point (WAP) and/or wireless router being used must be connected to power. Check power indicator lights to make sure your devices are powered.

2. Check all cables and antenna.

   Verify that the antenna is securely attached to the NL241 and oriented in the same direction as the antenna of your WAP. The **Link/Act** LED on the NL241 should start flashing when it is connected to a network. Also, the WLAN activity light on your WAP (if it has one) should flash with activity as well.

3. Power cycle the NL241 and your WAP/hub/router/computer.

   Turn off or unplug your WAP/hub/router/computer and NL241. 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 NL241.

   a. Make sure the correct SSID and password (if needed) have been entered for your network.

   b. Make sure the NL241 is connected to the right WLAN (**Wi-Fi Status** in *Device Configuration Utility* or show > Wi-Fi settings > Wi-Fi in a Telnet session).

   c. Make sure the wireless network you are connecting to has a RSSI level of greater than (>) –90dBm (in *Device Configuration Utility*, **Settings Editor** > **Wi-Fi** > **Wireless Networks in Area**).

d. Make sure the assigned NL241 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:

   NL241: 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

e. If using DHCP to assign an IP address to the NL241, use ***Device Configuration Utility*** to read the IP address assigned to the NL241. This is done through a USB connection to the NL241 while the NL241 is connected to your network (if bridge mode is not being used).

f. The IP address assigned to the NL241 must be unique on your network.

g. 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 NL241 via the **CS I/O** port and SC12 cable.

5. Try to ping the NL241 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 NL241.) 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 NL241.

   > 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 NL241 in ***LoggerNet*** Setup in order for ***LoggerNet*** to communicate through the NL241. For example, if the NL241 is configured as a CS I/O serial server, in ***LoggerNet*** Setup, enter the correct IP address of your NL241 followed by :6783 (for example, 192.168.0.3:6783).

7. If you are unable to communicate with the NL241 via the USB cable, verify that the latest drivers for the NL241 have been installed. These can be downloaded from our website at www.campbellsci.com/downloads.

8. If the NL241 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 NL241 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 NL241 to its default settings.

    If none of the above steps correct your communications problems, reset the NL241 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 NL241.
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 NL241 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 NL241 (p. 69) for instructions on downloading the firmware revision to the NL241.
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 NL241 communications network.
    b. Save a copy of the NL241 settings (in XML format) using ***Device Configuration Utility***.
    c. Save a copy of the NL241 event log. This is low-level code that can be used by Campbell Scientific technical support to help troubleshoot the NL241. To obtain the event log, the NL241 must not be in bridge mode. Telnet into the NL241 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.

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

The following sections provide specific information about the hardware:

A.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.

Table A-1: CS I/O pinout

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
8	12 VDC (output)	12 VDC (input)
9	TXD	RXD

A.2 RS-232

A DB9 pin and socket cable is used to connect the NL241 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 NL241 **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.

Table A-2: RS-232 pinout

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

A.3 Link/Activity LED

The color and light pattern of the **Link/Act** (Activity) LED indicate the state of the device as described in the following Table.

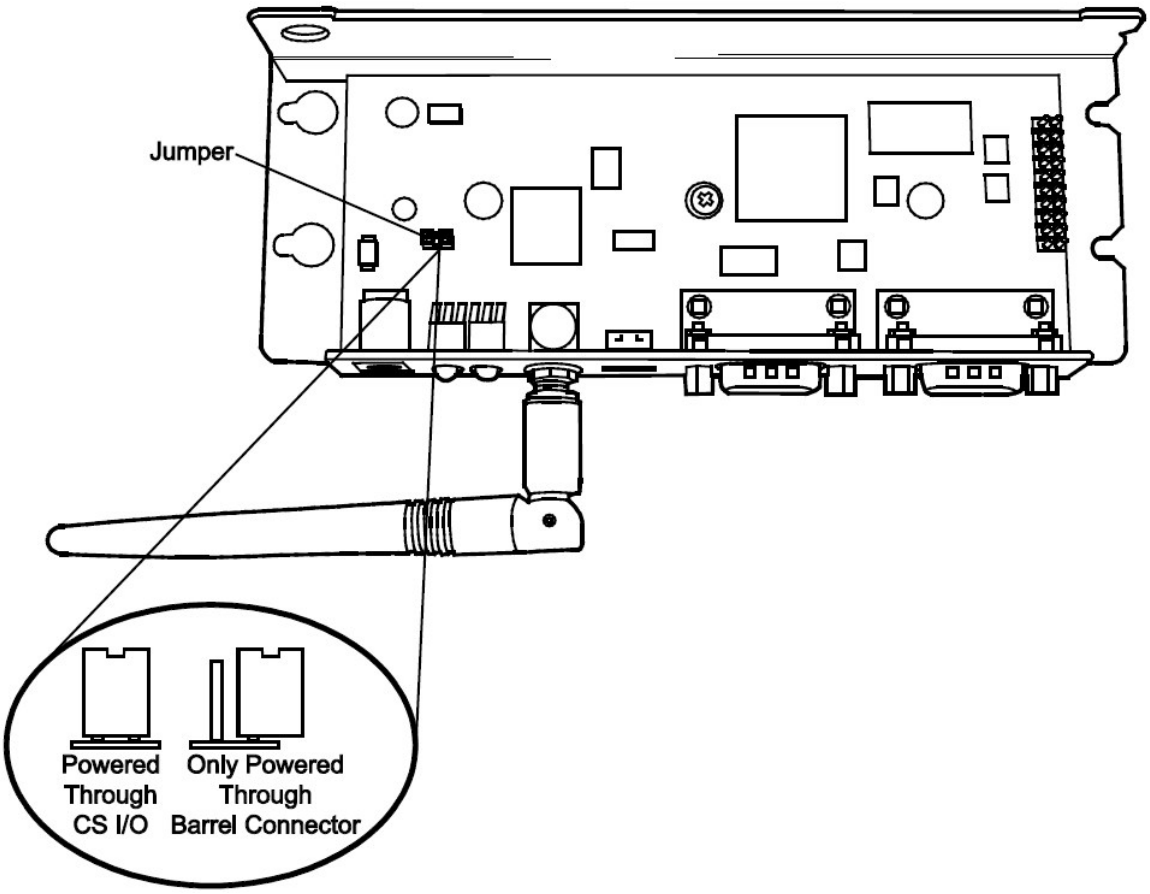
Table A-3: LED

State	Description
Off	The device is powered off or the Wi-Fi has been disabled via the **Mode** button configuration or via an `IPNetPower()` instruction from the data logger. See Mode button (p. 20) for information on the **Mode** button configuration.
On solid	After power-up: scanning nearby networks and trying to join or create a Wi-Fi network. The LED turns solid green when joining a network and solid amber when creating a network.

Table A-3: LED	
State	Description
Flashing	After successfully joining or creating a network, the LED will flash with network activity. Note that the LED may only flash once every few seconds on the created network or networks that are not very busy.
Red double-flash	If the device is unsuccessful at joining or creating a network, the LED will periodically double-flash red. The device will attempt to connect to the network again after approximately one minute.
Fast red and green flash	OS Download in progress – DO NOT DISCONNECT POWER

A.4 Power jumper

To prevent the NL241 from being powered over the **CS I/O** port, remove the two screws on the top of the NL241, remove the NL241 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 NL241 can only be powered from the barrel connector. With the jumper connected to both posts, the NL241 can be powered from the **CS I/O** port or from the barrel connector.


Jumper
Powered Through CS I/O
Only Powered Through Barrel Connector

Appendix B. NL241 settings

The NL241 settings available from the **Settings Editor** in *Device Configuration Utility* are described as follows.

B.1 Main tab

B.1.1 Model (read only)

Model name.

B.1.2 Serial Number (read only)

Specifies the NL241 serial number assigned by the factory.

B.1.3 OS Version (read only)

Operating system version currently in the NL241.

B.1.4 Compile Date (read only)

Operating system compile date.

B.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.

B.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.

B.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 (0xFFFB): 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.

B.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 presssing F5.

B.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** > **NL241** 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** > **NL241** tab.

B.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** > **NL241** 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** > **NL241** tab.

B.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** > **NL241** 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** > **NL241** tab.

B.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.

B.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.

B.1.14 Admin Password

To help guard against unauthorized access to the NL241, it is password-protected by the admin password. This password will be required to gain access to the NL241 via ***Device Configuration***

Utility over TCP and Telnet. If the password setting is left blank, no password is required to access the NL241. After settings are saved, the new password will be in effect.

B.1.15 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).

B.2 Wi-Fi tab

B.2.1 Wi-Fi Status

Status of the Wi-Fi Module.

B.2.2 Configuration

This setting controls whether the device is configured to join an existing network or create a network.

Join a Network

If this mode is selected, the device will scan for available networks and attempt to join the network specified by the SSID setting. If for some reason the device cannot join the desired SSID (that is, network out of range or incorrect parameters), it will go to a low power state and periodically (approximately every 1 minute) retry.

Create a Network

The NL241 can be configured to create a network. In this mode, it acts as the access point which other Wi-Fi enabled devices can join. If this configuration is enabled, the user may set an SSID (network name) and password. If a password is supplied, the network created will be secured by WPA2 encryption. If no password is supplied, the network created will be an open network with no encryption.

If this mode is selected, the channel may be specified manually using the **Channel** setting in the **Settings Editor**. If the **Channel** setting is left at the default setting **Auto**, the device will only use channels 1, 6, and 11 on which to operate to minimize interference from other networks detected in the area.

When manually selecting a channel, it should be noted that two Wi-Fi networks operating on the same channel will interfere with each other and will have to compete for bandwidth. The center frequencies of adjacent channels are 5 MHz apart and the bandwidth of each channel is

20 MHz which means that adjacent channels overlap. To completely avoid interference there must be a spacing of at least 5 channels between each Wi-Fi network. It is therefore recommended to use channels 1, 6, and 11. For a list of all the wireless networks in the area and the associated channels on which they operate, see the **Settings Editor** > **Wi-Fi Wireless Networks in Area** box.

A network created by the NL241 supports up to 8 joinees.

B.2.3 Network Name (SSID)

The **Network Name (SSID)** setting is the name that identifies a wireless network (31- character maximum). The SSID differentiates one wireless network from another, so all devices attempting to connect to the same network must use the same SSID. If the device is configured to **Join a Network**, enter the SSID of the network to join here. To join a hidden network, manually enter its SSID. If the device is configured to **Create a Network**, the SSID entered here will be the SSID of the network created.

To see a list of the available networks detected in the area click **Browse** ... or view the **Wireless Networks in Area** list.

> NOTE:
> When **Browse** ... is clicked or the **Refresh** button inside the resulting dialog is clicked, if the device is currently connected to a network, the connection will be temporarily interrupted. The device will disconnect, scan for available networks, then reconnect.

B.2.4 Password

If joining a WPA or WPA2 security enabled network, this is where the password is entered. If joining a WEP security enabled network, this is where the WEP key is entered.

If creating a network and a password is supplied, the network will be created using WPA2 encryption. The password must be at least 8 characters. If a password is not supplied, an open (unencrypted) network will be created.

When joining a network, the device supports 64-bit WEP and 128-bit WEP. For 64-bit WEP, enter a 40-bit key in the form of 5 ASCII characters or 10 hexadecimal digits (0-9, A-F). For 128-bit WEP, enter a 104-bit key in the form of 13 ASCII characters or 26 hexadecimal digits (0-9, A-F).

B.2.5 EAP User

If joining an Enterprise Security enabled network, enter the user name here.

B.2.6 EAP Password

If joining an Enterprise Security enabled network, enter the password here.

B.2.7 EAP Method

The **EAP Method** must be set to match the EAP method being used by the Enterprise Security Network. The inner EAP Methods supported are TTLS, MSCHAPv2, MSCHAP, CHAP, and PAP.

B.2.8 Button Configuration

This setting controls how the device acts when the **Mode** button is pressed.

Disable Button

If this configuration is selected, pressing the button will have no effect on the operation of the device. The Wi-Fi network will continue to work as configured.

Temporarily Enable Wi-Fi

If this configuration is selected, the configured Wi-Fi network will normally be disabled and it will be activated temporarily when the button is pressed.

Temporarily Create a Network

If this configuration is selected, the device will temporarily create a network when the button is pressed. If the Wi-Fi **Configuration** is set to **Join a Network**, the temporarily created network will be an open network with the name "NL241_SerialNumber." If the Wi-Fi **Configuration** is set to **Create a Network**, the configured Wi-Fi network will normally be disabled and it will be temporarily activated when the button is pressed.

Note that when the Wi-Fi **Configuration** is set to **Create a Network**, the device behavior is the same for both button configurations.

B.2.9 Channel

Applicable only when the device is configured to create a network. This setting specifies on which channel the network should be created. If **Auto** is selected, the device will only use channels 1, 6, and 11 on which to operate to minimize interference from other networks detected in the area.

When manually selecting a channel, it should be noted that two Wi-Fi networks operating on the same channel will interfere with each other and will have to compete for bandwidth. The center frequencies of adjacent channels are 5 MHz apart and the bandwidth of each channel is 20 MHz which means that adjacent channels overlap. To completely avoid interference there must be a spacing of at least 5 channels between each Wi-Fi network. It is therefore recommended to use

channels 1, 6, and 11. For a list of all the wireless networks in the area and the associated channels on which they operate, see the **Settings Editor** > **Wi-Fi Wireless Networks in Area** box.

B.2.10 Tx Power Level

This fixes the Transmit Power level of the module. This value can be set as follows: Low (7 +/– 1 dBm), Medium (10 +/– 1 dBm), High (15 +/– 2 dBm).

> NOTE:
> This setting affects the transmission power level of the NL241, which may affect the transmission range of the device. This setting does not affect the overall power consumption of the device.

B.2.11 Power Mode

This setting controls the power saving mode of the device. Regardless of the Power Mode, the device enables the power-save mode when communications are not active. The Power Mode determines how the device acts when communications are ongoing.

This setting only applies when the Wi-Fi **Configuration** is set to **Join a Network**.

Mode 0

If this mode is selected, the device will attempt to determine automatically when high throughput communications are desired and temporarily disable the Wi-Fi module power-save mode while the high throughput communications are ongoing. The power-save mode will be re-enabled when the high throughput communications are finished. Use this mode for a good balance between communications speed and low power consumption.

Mode 1

If this mode is selected, the device will disable the Wi-Fi module power-save mode at the first sign of any type of communications and re-enable the power-save when communications are finished. Use this mode when throughput is of more concern than power consumption and communications seem too slow using **Mode 0**.

Mode 2

If this mode is selected, the device will leave the Wi-Fi module power-save mode enabled at all times even during communications. This lessens throughput a great deal but saves more power overall. Use this mode if power consumption is of greater concern than throughput.

B.2.12 WLAN Domain Name

This setting is only relevant when the Wi-Fi **Configuration** is set to **Create a Network**. When attempting to communicate with the device, attached Wi-Fi client devices can use the domain name specified here which will be resolved to the device IP address. For example, the data logger webpage can be accessed by entering the domain name specified here into a web browser.

B.2.13 Wireless Networks in Area

This is a read-only field that lists the networks available in the area. Information listed for each network is: SSID, RSSI / Signal Strength, Channel, and Security. Sometimes areas are covered by multiple access points configured with the same network name (SSID). In that case, multiple unique access points possessing the same network name (SSID) may be listed here.

B.3 RS-232 tab

B.3.1 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.

B.3.2 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).

B.3.3 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.

B.3.4 RS-232 RTS

The NL241 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**).

B.3.5 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).

B.3.6 RS-232 Always On

This setting controls whether the device is allowed to shut down the RS-232 port when it is not in use in order to conserve power. Typically, it is not necessary to change this setting from its default (**Auto**).

Auto

Based on the RS-232 port configuration, the device will decide which of the following two modes is more likely to be desired and will operate in the according manner. If the port is configured to **TCP Serial Client**, the device will choose RS-232 **Always On**. Otherwise, the device will choose **Power Down Port When Inactive**, and it will allow the RS-232 port to power down when not in use in order to conserve power.

Always On

The device will not power down the RS-232 port. The port will remain active always. As a result, the processor cannot enter its lowest power state. Keeping the port **Always On** may be necessary because when the RS-232 port is powered down, there is a wake-up latency and the first few bytes that come in on the port will be missed. If this behavior is unacceptable, set this setting to **Always On** to keep the RS-232 port always on.

Power Down Port when Inactive

The device will power down RS-232 when the port is inactive. If the device is configured for **Serial Server** mode, the inactivity timeout is 40 seconds. If configured for **PakBus**, the device can use the PakBus protocol link-state to do a more intelligent and effective inactivity timeout. If communications are received on the port after it has been powered down, there is a wake-up latency and the first few bytes will be missed. PakBus has a built-in mechanism to deal with this, but if the device is not configured for PakBus communications, the user must decide if the application can accept this behavior. If this behavior is unacceptable, set this setting to **Always On**. The power savings that the device is able to achieve by powering down the RS-232 port are significant as the processor is also able to go to a deeper sleep mode. In an idle state with **Low Power Mode** enabled, an additional ~0.12W savings are observed by setting **RS-232 Always On** to **Power Down Port when Inactive**.

B.3.7 RS-232 PakBus Beacon Interval

This setting, in units of seconds, governs the rate at which the NL241 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.

B.3.8 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 NL241 will attempt to start a hello transaction with a neighbor if no other communications has taken place within the interval.

B.3.9 Neighbors Allowed RS-232

This setting specifies the explicit list of PakBus node addresses that the NL241 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 NL241.

B.3.10 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).

B.3.11 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.

B.3.12 RS-232 TCP Serial Client Port

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

B.4 CS I/O tab

B.4.1 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.

B.4.2 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).

B.4.3 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.

B.4.4 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).

B.4.5 CS I/O PakBus Beacon Interval

This setting, in units of seconds, governs the rate at which the NL241 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**.

B.4.6 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 NL241 will attempt to start a hello transaction with a neighbor if no other communications has taken place within the interval.

B.4.7 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).

B.5 Net Services tab

B.5.1 Telnet

Enables/Disables the Telnet service.

B.5.2 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).

B.5.3 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).

B.5.4 Ping (ICMP)

The NL241 will not respond to Ping requests if this setting is disabled.

B.5.5 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.

B.5.6 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.

B.5.7 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.

B.5.8 PakBus/TCP Client Address (1-4)

This setting specifies the IP address of an outgoing PakBus/TCP client connection that the NL241 should maintain. If the connection fails, the NL241 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.

B.5.9 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).

B.5.10 PakBus Routes (read only)

This setting lists the routes that are known to the NL241. Each route known to the NL241 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.

B.5.11 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.

B.6 TLS Proxy Server tab

B.6.1 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.

B.6.2 TLS Proxy Service Port

When doing TLS Proxy communications, the NL241 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 NL241 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 **Wi-Fi**, the NL241 will open the TCP connection over Wi-Fi on the **TLS Proxy Forward IP Address**.

In order to communicate with the NL241 TLS server, the client application must open a socket to that server. The socket of the NL241 TLS server is uniquely identified by the IP address and a port number. This entry is where the port number of the NL241 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 NL241 will attempt to open a TCP connection to the data logger on the **TLS Proxy Forward Port**. Also, regardless of this setting, the NL241 Secure Proxy Server will always listen on the secure HTTP (HTTPS) port number 443. If a secure connection is established on this port, the NL241 will attempt to communicate to the data logger on the HTTP port 80 (range 1 to 65535).

B.6.3 TLS Proxy Forward Physical Port

When doing TLS Proxy communications, the NL241 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 NL241 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 **Wi-Fi**, the NL241 will open the TCP connection over Wi-Fi on the **TLS Proxy Forward IP Address**.

B.6.4 TLS Proxy Forward IP Address

Secure communications received on the NL241 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 NL241 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 NL241 IP address. If the **TLS Proxy Forward Physical Port** is specified to be **Wi-Fi**, the forward IP address must be specified. Enter the IP address of the destination data logger here.

B.6.5 TLS Proxy Forward Port

When doing TLS Proxy communications, the NL241 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 NL241 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 **Wi-Fi**, the NL241 will open the TCP connection over Wi-Fi on the **TLS Proxy Forward IP Address**.

In order to communicate with the connected data logger TCP server, the NL241 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 NL241 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 NL241 will attempt to open a TCP connection to the data logger on the **TLS Proxy Forward Port**. Also, regardless of this setting, the NL241 TLS Proxy Server will always listen on the secure HTTP (HTTPS) port number 443. If a secure connection is established on this port, the NL241 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).

B.6.6 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).

B.7 TLS tab

B.7.1 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.

B.7.2 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.

B.7.3 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.

B.7.4 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 C. Sending a new OS to the NL241

Whenever a new operating system (OS) is released for the NL241, it will be available from our website, www.campbellsci.com/downloads.

C.1 Sending an OS via USB

Follow these steps to send the new OS to the NL241 via USB:

1. Plug the wall charger into an AC outlet and the barrel connector into the NL241 power jack.
2. Connect a USB cable between one of your computer USB ports and the **USB** port on the NL241.
3. Open *Device Configuration Utility*.
4. Under **Device Type**, select **Network Peripheral** > **NL241**.
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 NL241.
10. After the file has been sent, the LED on the NL241 will flash repeatedly while the NL241 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 NL241 to finish updating the operating system. While the LED is flashing, the NL241 is in a vulnerable state where a removal of power could leave the NL241 without a valid operating system to run. Do not remove power until the LED stops flashing.

C.2 Sending an OS via Wi-Fi

Follow these steps to send the new OS to the NL241 via Wi-Fi:

1. Using the supplied serial cable, connect the NL241 **CS I/O** port to the data logger **CS I/O** port. Alternatively, power the NL241 through the barrel-connector jack located on the edge of the device.
2. The NL241 will power up and either create or join a Wi-Fi network. After successfully joining or creating a network, the LED will flash with network activity. Note that the LED may only flash once every few seconds on the created network or an idle network. See Link/Activity LED (p. 46).
3. If the device is configured to create a network, the computer must join the NL241 created network. If the NL241 has been previously configured to join a network, join the same network with your computer.
4. Open ***Device Configuration Utility***.
5. Select the NL241 under **Device Type**.
6. Ensure that the **Use IP Connection** box is checked on the left-hand panel.
7. 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.
8. 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.
9. Go to the **Send OS** tab.
10. Click **Start**.
11. 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**.
12. The operating system will be sent to the NL241.
13. After the file has been sent, the LED on the NL241 will flash repeatedly while the NL241 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 NL241 to finish updating the operating system. While the LED is flashing, the NL241 is in a vulnerable state where a

removal of power could leave the NL241 without a valid operating system to run. Do not remove power until the LED stops flashing.

Appendix D. Radio frequency emission

Changes or modifications to the NL241 not expressly approved by Campbell Scientific, Inc. could void the user's authority to operate this product.

> NOTE:
> This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

The embedded radio transmitter approval:

FCC Identifier: XF6-RS9113SB

Industry Canada: 8407A-RS9113SB

View the EU Declaration of Conformity at www.campbellsci.com/nl241

View the Supplier Declaration of Conformity at www.campbellsci.com/nl241

Appendix E. Glossary

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 NL241 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 NL241 is powered down. If DHCP is enabled but the NL241 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.

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 to which a network message is to be forwarded when it arrives at the NL241.

Proxy (Proxy Server)

A device that acts as an intermediary for IP communications between two clients. In the context of this manual, the NL241 acts an intermediary between two or more clients requiring a secure connection (TLS) and one client requiring an unsecured connection. Communications are encrypted and decrypted as necessary for the two clients to communicate via the proxy.

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 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.cc
Website: www.campbellsci.cc

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: Shepshed, 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