



## NL241

### Wireless Network Link Interface





# Guarantee

---

This equipment is guaranteed against defects in materials and workmanship. We will repair or replace products which prove to be defective during the guarantee period as detailed on your invoice, provided they are returned to us prepaid. The guarantee will not apply to:

- Equipment which has been modified or altered in any way without the written permission of Campbell Scientific
- Batteries
- Any product which has been subjected to misuse, neglect, acts of God or damage in transit.

Campbell Scientific will return guaranteed equipment by surface carrier prepaid. Campbell Scientific will not reimburse the claimant for costs incurred in removing and/or reinstalling equipment. This guarantee and the Company's obligation thereunder is in lieu of all other guarantees, expressed or implied, including those of suitability and fitness for a particular purpose. Campbell Scientific is not liable for consequential damage.

Please inform us before returning equipment and obtain a Repair Reference Number whether the repair is under guarantee or not. Please state the faults as clearly as possible, and if the product is out of the guarantee period it should be accompanied by a purchase order. 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 a "Declaration of Hazardous Material and Decontamination" form will be issued for completion.

When returning equipment, the Repair Reference Number must be clearly marked on the outside of the package. Complete the "Declaration of Hazardous Material and Decontamination" form and ensure a completed copy is returned with your goods. Please note your Repair may not be processed if you do not include a copy of this form and Campbell Scientific Ltd reserves the right to return goods at the customers' expense.

Note that goods sent air freight are subject to Customs clearance fees which Campbell Scientific will charge to customers. In many cases, these charges are greater than the cost of the repair.



Campbell Scientific Ltd,  
80 Hathern Road,  
Shepshed, Loughborough, LE12 9GX, UK  
Tel: +44 (0) 1509 601141  
Fax: +44 (0) 1509 270924  
Email: [support@campbellsci.co.uk](mailto:support@campbellsci.co.uk)  
[www.campbellsci.co.uk](http://www.campbellsci.co.uk)



# PLEASE READ FIRST

---

## About this manual

Please note that this manual was originally produced by Campbell Scientific Inc. primarily for the North American market. Some spellings, weights and measures may reflect this origin.

Some useful conversion factors:

**Area:** 1 in<sup>2</sup> (square inch) = 645 mm<sup>2</sup>

**Length:** 1 in. (inch) = 25.4 mm  
1 ft (foot) = 304.8 mm  
1 yard = 0.914 m  
1 mile = 1.609 km

**Mass:** 1 oz. (ounce) = 28.35 g  
1 lb (pound weight) = 0.454 kg

**Pressure:** 1 psi (lb/in<sup>2</sup>) = 68.95 mb

**Volume:** 1 UK pint = 568.3 ml  
1 UK gallon = 4.546 litres  
1 US gallon = 3.785 litres

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 it will be suitable for use in your country.*

Reference to some radio transmitters, digital cell phones and aerials 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. Details of the alternatives will be covered in separate manuals.

Part numbers prefixed with a “#” symbol are special order parts for use with non-EU variants or for special installations. Please quote the full part number with the # when ordering.

## Recycling information



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.

Campbell Scientific Ltd 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 advice or support, please contact Campbell Scientific Ltd, or your local agent.



Campbell Scientific Ltd, 80 Hathern Road, Shepshed, Loughborough, LE12 9GX,  
UK Tel: +44 (0) 1509 601141 Fax: +44 (0) 1509 270924  
Email: [support@campbellsci.co.uk](mailto:support@campbellsci.co.uk)  
[www.campbellsci.co.uk](http://www.campbellsci.co.uk)



# 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.eu](http://www.campbellsci.eu) or by telephoning +44(0) 1509 828 888 (UK). You are responsible for conformance with governing codes and regulations, including safety regulations, and the integrity and location of structures or land to which towers, tripods, and any attachments are attached. Installation sites should be evaluated and approved by a qualified engineer. If questions or concerns arise regarding installation, use, or maintenance of tripods, towers, attachments, or electrical connections, consult with a licensed and qualified engineer or electrician.

## General

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

## Utility and Electrical

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

## Elevated Work and Weather

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

## Maintenance

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

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





# Table of Contents

---

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

<b>1. Introduction .....</b>	<b>1</b>
<b>2. Precautions .....</b>	<b>1</b>
<b>3. QuickStart.....</b>	<b>2</b>
3.1 Physical Setup .....	2
3.2 Configuring the NL241 .....	3
3.3 <i>LoggerLink</i> Setup .....	4
3.4 Connect .....	7
<b>4. Overview .....</b>	<b>7</b>
<b>5. Specifications.....</b>	<b>11</b>
<b>6. Wi-Fi .....</b>	<b>13</b>
6.1 Introduction to Wi-Fi for WLANs .....	13
6.2 Wireless Network Modes .....	13
6.3 RSSI .....	14
6.4 Antennas .....	15
6.5 Power .....	15
6.6 LED .....	15
6.7 Mode Button .....	16
<b>7. Configuring the NL241 .....</b>	<b>17</b>
7.1 Configuring the NL241 with <i>DevConfig</i> via USB .....	17
7.2 Configuring the NL241 with <i>DevConfig</i> via Wi-Fi WLAN .....	18
7.3 Configuring the NL241 with Telnet via Wi-Fi WLAN.....	19
7.4 Configuring the NL241 via RS-232 .....	19
<b>8. Operation .....</b>	<b>20</b>
8.1 Wi-Fi Connection.....	20
8.1.1 Join an Existing Network.....	20
8.1.2 Create a Network .....	21
8.2 Operational Mode .....	21
8.2.1 PakBus Router .....	21
8.2.1.1 Physical Setup .....	22
8.2.1.2 Configuring the NL241 .....	22
8.2.1.3 <i>LoggerNet</i> Setup.....	23
8.2.1.4 Connect .....	24
8.2.2 Bridge Mode .....	24
8.2.2.1 Physical Setup .....	24
8.2.2.2 Configuring the NL241 .....	24
8.2.2.3 Configuring the Datalogger.....	24

8.2.2.4	LoggerNet Setup .....	25
8.2.2.5	Connect.....	26
8.2.3	TCP Serial Server.....	26
8.2.3.1	Physical Setup .....	26
8.2.3.2	Configuring the NL241 .....	26
8.2.3.3	LoggerNet Setup .....	27
8.2.3.4	Connect.....	28
8.2.3.5	Serial Sensors .....	28
8.2.4	TCP Serial Client .....	28
8.2.5	Modbus TCP/IP to RTU Gateway.....	29
8.2.6	TLS .....	29
8.2.6.1	TLS Proxy Server .....	30
8.2.6.2	DevConfig TCP Encrypted Communication to the NL241 .....	32
<b>9.</b>	<b>Applications .....</b>	<b>33</b>
9.1	Working Around Firewalls.....	33
9.1.1	Configuring the NL241 .....	33
9.1.2	Configuring the Datalogger.....	34
<b>10.</b>	<b>Troubleshooting.....</b>	<b>34</b>
<b>11.</b>	<b>Attributions.....</b>	<b>37</b>
<b>Appendices</b>		
<b>A.</b>	<b>Glossary.....</b>	<b>A-1</b>
<b>B.</b>	<b>Cables, Pinouts, LED Function, and Jumper .....</b>	<b>B-1</b>
B.1	CS I/O.....	B-1
B.2	RS-232.....	B-1
B.3	USB .....	B-2
B.4	Power.....	B-2
B.5	LED .....	B-2
B.6	Power Jumper .....	B-3
<b>C.</b>	<b>NL241 Settings .....</b>	<b>C-1</b>
C.1	Main Tab .....	C-1
C.2	Wi-Fi Tab .....	C-4
C.3	RS-232 Tab .....	C-7
C.4	CS I/O Tab .....	C-11
C.5	Net Services Tab .....	C-12
C.6	TLS Proxy Server Tab.....	C-14
C.7	TLS Tab .....	C-16
<b>D.</b>	<b>Sending a New OS to the NL241 .....</b>	<b>D-1</b>
D.1	Sending an OS via USB .....	D-1
D.2	Sending an OS via Wi-Fi.....	D-1
<b>E.</b>	<b>Radio Frequency Emission .....</b>	<b>E-1</b>

## **Figures**

3-1.	NL241 with CR800 (powered through CS I/O port).....	2
4-1.	NL241 .....	8
4-2.	Bridge mode enabled .....	8
4-3.	Bridge mode disabled.....	9
5-1.	NL241 dimensions .....	11
6-1.	Infrastructure network.....	14
8-1.	PakBus router LoggerNet setup .....	23
8-2.	Bridge mode LoggerNet setup .....	26
8-3.	CS I/O serial server LoggerNet setup .....	28
8-4.	TLS proxy server configurations .....	31
9-1.	Working around firewalls .....	33

## **Tables**

B-1.	CS I/O Pinout .....	B-1
B-2.	RS-232 Pinout.....	B-1
B-3.	USB Micro-B.....	B-2
B-4.	Power In .....	B-2
B-5.	LED.....	B-2



# NL241 Wireless Network Link Interface

---

## 1. Introduction

The NL241 is a WLAN (wireless local area network) interface that allows Campbell Scientific dataloggers 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 datalogger CS I/O port or RS-232 port.

## 2. Precautions

- READ AND UNDERSTAND the [Safety](#) section at the front of this manual.
- The first time an NL241 is attached to a datalogger and bridge mode is enabled, the datalogger 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 datalogger 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 Appendix E, *Radio Frequency Emission (p. E-1)*, 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.
- *Device Configuration Utility (DevConfig)* 2.15 or higher is required to communicate with the NL241. The latest version of *DevConfig* can be downloaded from our website at [www.campbellsci.eu/downloads](http://www.campbellsci.eu/downloads).
- The device driver for the NL241 must be installed on your computer before you can connect to the NL241 via USB. To install the device driver, verify you have the latest version of *DevConfig* (see previous bullet). Under **Device Type**, select **Network Peripheral | NL241**. Click **Install USB Driver** and follow the prompts.
- CR1000, CR3000, and CR800-series dataloggers require operating system version 25 or higher in order to operate with the NL241 in bridge mode. (OS version 25 or higher is not required to operate as a serial server or PakBus router.) The latest operating systems can be downloaded at [www.campbellsci.eu/downloads](http://www.campbellsci.eu/downloads).
- Ensure maximum protection against surges. Use coaxial surge protection. Keep RS-232 and CS I/O connections short.
- When downloading a new operating system to the NL241, do not remove power until the LED stops rapidly blinking 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 datalogger using a smart phone with Campbell Scientific’s *LoggerLink* Mobile App.

#### 3.1 Physical Setup

As shown in FIGURE 3-1, attach an antenna to the NL241 **Antenna** connector. Using the supplied serial cable, connect the NL241 **CS I/O** port to the datalogger **CS I/O** port. This cable supplies communications and power from the datalogger 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 communication.

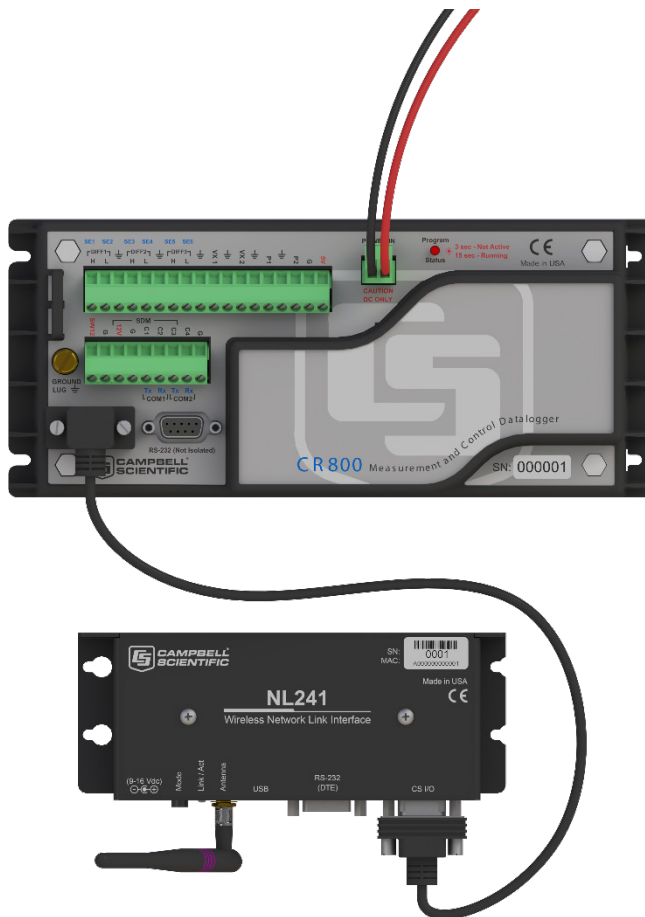


FIGURE 3-1. NL241 with CR800 (powered through CS I/O port)

## 3.2 Configuring the NL241

**NOTE**

INSTALL THE DEVICE DRIVER BEFORE plugging the NL241 into your computer for the first time. You will need the device driver properly installed before you can connect to the NL241 via USB. To install the device driver, download the latest version of *DevConfig* from our website. Under **Device Type**, select **Network Peripheral | NL241**. Click **Install USB Driver** and follow the prompts.

1. Ensure the NL241 is powered.
2. Connect the supplied USB cable between a USB port on your computer and the **USB** port on the NL241.
3. Open *DevConfig*.
4. Under **Device Type**, select **Network Peripheral | NL241**.
5. Click the **Browse** button next to **Communication Port**.
6. Select the virtual com port labelled **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*." If you wish to change the name of this network, type a new name in the **Network Name (SSID)** field. If you wish to enable encryption, type a password in the **Password** field.
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**. If you desire 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 your changes.

### 3.3 LoggerLink Setup

The next step is to download *LoggerLink* and configure it to connect to the datalogger 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

For Android users, you may get a message saying there is no internet access and asking if you want to stay connected. Select the **Don't ask again for this network** check box and press **YES**.

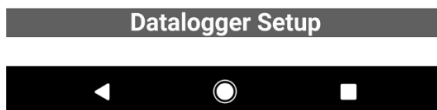
3. In the *LoggerLink* **Getting Started** screen, press the + key to add a datalogger.



When you launch LoggerLink, you can add new dataloggers by tapping the "+" button in the upper right of the screen.

Note that to use a TCP connection, your Android device must be connected to a network through which you can reach your datalogger. To use a Bluetooth connection, you must have an RS-232 to Bluetooth adapter connected to your datalogger's RS-232 port. The Bluetooth adapter must be properly configured according to the manufacturer's instruction manual. See Bluetooth Connection below for information on settings.

Some LoggerLink functions are accessed from your Android device's Menu button. If your device does not have a Menu button, these functions can be accessed from the menu button on the right end of the action bar at the top of the LoggerLink screen.





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

The screenshot shows the 'Logger Setup' interface. At the top, there are 'TCP' and 'Bluetooth' buttons. Below them is the 'TCP Settings' section with an 'Address' field containing '0.0.0.0' and a 'Port' field containing '6785'. A red box highlights a magnifying glass icon next to the 'Address' field. Below this is the 'Logger Settings' section with a 'Type' dropdown set to 'CR1000' and a 'Name' field containing 'MyDatalogger'. At the bottom is the 'PakBus Settings' section with an 'Address' field containing '1', a 'Neighbor' field containing '0', and a 'Security Code' field containing '0'. The status bar at the top shows the time as 4:02.

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

The screenshot shows the 'Network Search' interface. At the top, there is a search bar with a magnifying glass icon. Below the search bar, a search result is displayed: '192.168.67.1' with 'NL241.08.21' below it. A question mark icon is visible on the left side of the search result. The status bar at the top shows the time as 4:03.

6. The following screen appears. Press 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.

The screenshot shows the 'Logger Setup' screen on a mobile device. At the top, there are 'SAVE' and 'CANCEL' buttons. Below them are two tabs: 'TCP' and 'Bluetooth'. The 'TCP' tab is selected, showing 'TCP Settings' with fields for 'Address' (192.168.67.1) and 'Port' (6785). Below this is the 'Logger Settings' section with a 'Type' dropdown set to 'CR1000' and a 'Name' field set to 'MyDatalogger'. The 'PakBus Settings' section at the bottom has fields for 'Address' (678), 'Neighbor' (0), and 'Security Code' (0). A red square highlights the search icon (PB) next to the 'Address' field in the PakBus Settings.

7. The datalogger should be discovered automatically. Select the datalogger, 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 datalogger **Type**. Type the PakBus address of the datalogger (default is 1) in the **Address** field under **PakBus Settings**. Type the NL241 PakBus address (default is 678) in the **Neighbour** field. The following screen shows the correct information filled in for a CR1000 with PakBus address of 2.

The screenshot shows the 'Logger Setup' interface. At the top, there are buttons for 'TCP' and 'Bluetooth', and 'SAVE' and 'CANCEL' buttons. Below these are three sections of settings:

- TCP Settings:**
  - Address: 192.168.67.1
  - Port: 6785
- Logger Settings:**
  - Type: CR1000 (with a small icon of a datalogger)
  - Name: MyDatalogger
- PakBus Settings:**
  - Address: 2
  - Neighbor: 678
  - Security Code: 0

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

### 3.4 Connect

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

## 4. Overview

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

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



FIGURE 4-1. NL241

### Bridge Mode Enabled

The NL241 can be configured to bridge WLAN and CS I/O communications (see FIGURE 4-2). 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.

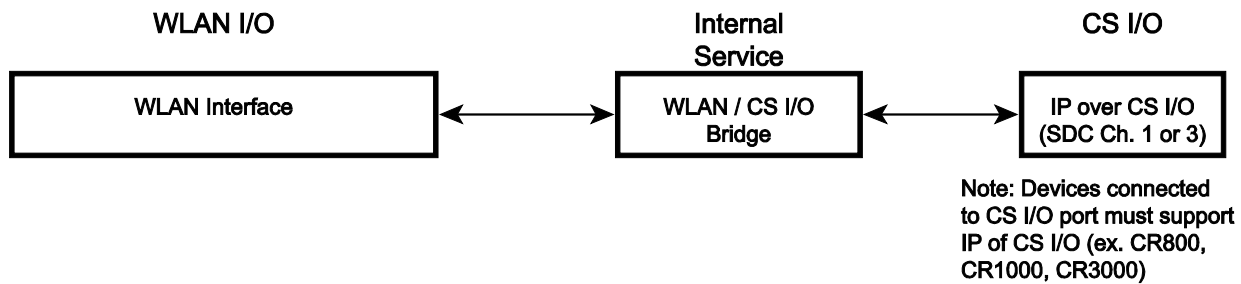


FIGURE 4-2. Bridge mode enabled

### Bridge Mode Disabled

With bridge mode disabled (see FIGURE 4-3), 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.

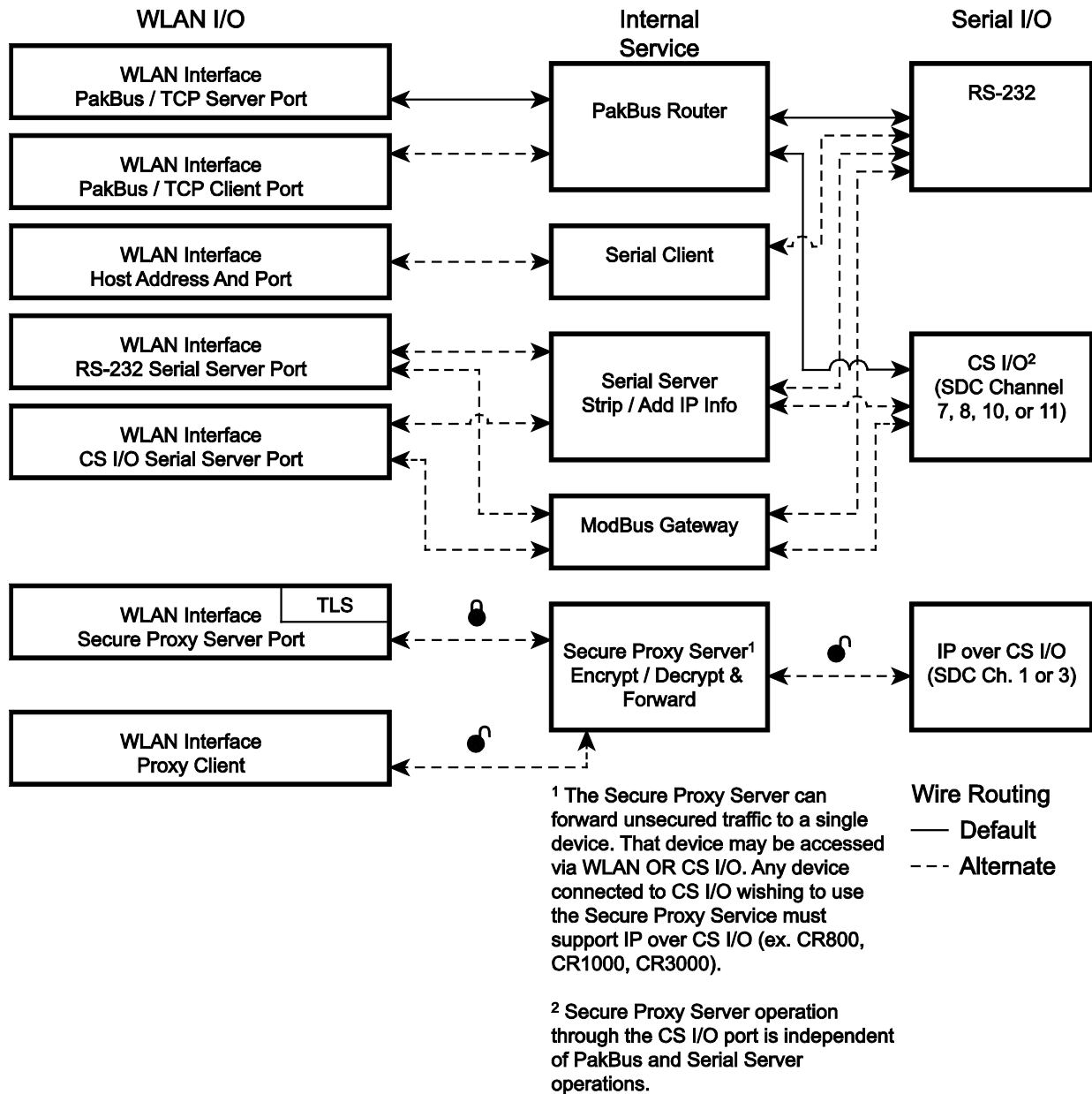


FIGURE 4-3. Bridge mode disabled

Some reasons you might want to use each of these modes are described below. Refer to Section 7, *Configuring the NL241* (p. 17), and Section 8, *Operation* (p. 20), for information on setting up your NL241 for each mode.

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

### **Bridge Mode**

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

### **Serial Server**

- Allows access to a CR10X over 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**

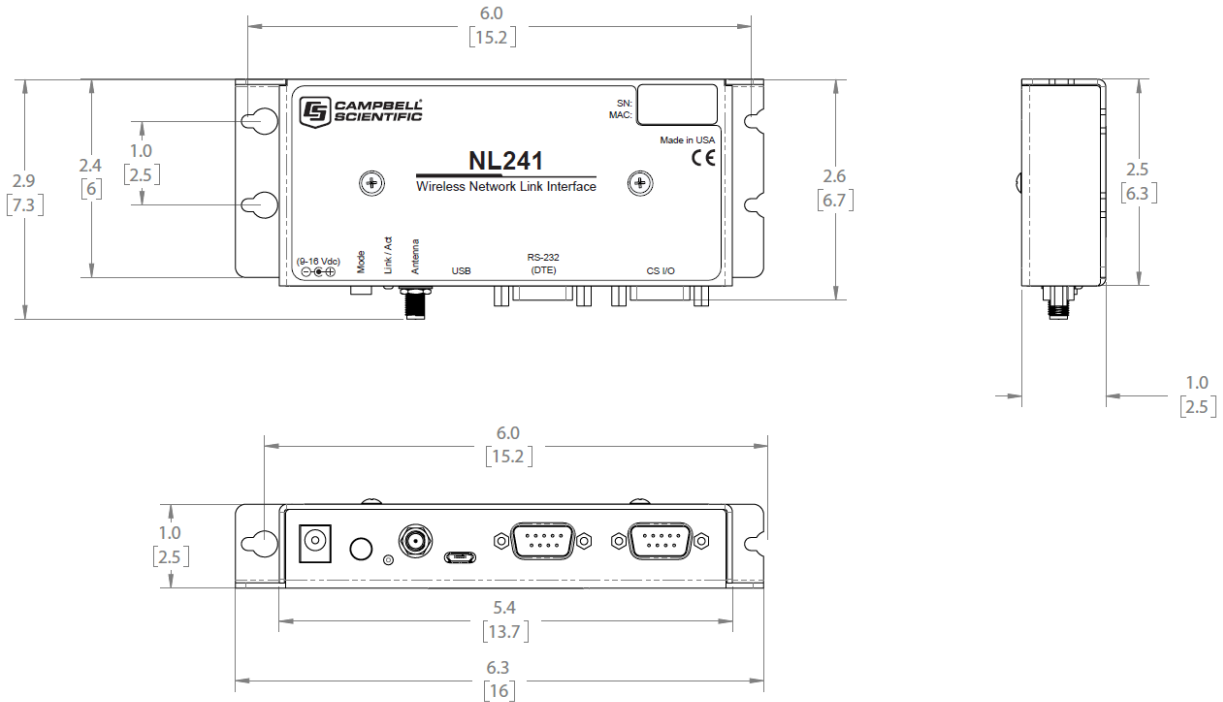
- Adds an encrypted WLAN interface to a datalogger that supports CS I/O IP (bridge mode) communications.

## 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)



#### NOTES:

1. UNITS ARE AS FOLLOWS:

INCH
[cm]

FIGURE 5-1. NL241 dimensions

### Power

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

9 to 16 Vdc

#### NOTE

If you wish to prevent the NL241 from being powered over the CS I/O port, you can do so by removing a jumper. See Appendix B, *Cables, Pinouts, LED Function, and Jumper (p. B-1)*, 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()** datalogger 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 Section 6.7, *Mode Button (p. 16)*, for information on the **Mode** button configuration.

---

**Operating Temperature**

Standard: -40 to 70 °C

**Configuration**

DevConfig 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  
Communication 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 B 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 the EU Declaration of Conformity at [www.campbellsci.eu/nl241](http://www.campbellsci.eu/nl241)

## 6. Wi-Fi

### 6.1 Introduction to Wi-Fi for WLANs

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 datalogger will generally be governed by the speed of serial communication.

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 communication 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.

---

**NOTE**

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

---

### 6.2 Wireless Network Modes

#### Join a Network:

The NL241 can be configured to join an already established infrastructure wireless network (WLAN) (see FIGURE 6-1). 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.

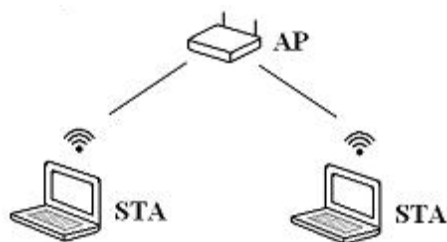


FIGURE 6-1. Infrastructure network

**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 select a channel on which to operate that has minimal interference from other networks detected in the area. A network created by the NL241 supports up to 8 joiners.

**DHCP Server in a Created Network**

When configured to **Create a Network**, the device will run a DHCP server to assign addresses to joiners 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.

## 6.3 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 *DevConfig*.

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 metres (120 feet) indoors and 95 metres (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.

## 6.4 Antennas

Antenna selection and placement can greatly affect the strength of the signal you transmit and receive and therefore can impact the quality of communications with your device. 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; care should be taken 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.

## 6.5 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 your critical communication needs. See [Section 5, Specifications \(p. 11\)](#) (Typical Power Consumption), and [Appendix C.2, Wi-Fi Tab \(p. C-4\)](#), for more details.

## 6.6 LED

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

### Normal Operation

After power-up, the LED turns solid red while the NL241 is searching for and trying to join a Wi-Fi network (or while creating a network).

After successfully joining or creating a network, the LED will flicker green with network activity. Note that the LED may only blink green once every few seconds on the created network or networks that aren't very busy.

If the device is unsuccessful at joining or creating a network, the LED will periodically double-strobe 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 datalogger, the LED will be off. See Section 6.7, *Mode Button (p. 16)*, for information on the **Mode** button configuration.

### Operating System Upgrade

When a new operating system is sent to the NL241, the LED will blink repeatedly while the NL241 copies the operating system into its internal flash memory. This process takes about 10 seconds. While the LED is blinking, 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 and blinking of the LED, the device will power up and start copying the new firmware to the Wi-Fi module. The LED will also blink during this process. It will start out as a slow blink 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.

## 6.7 Mode Button

The behavior of the **Mode** button is determined by the **Mode Button Configuration** setting on the *DevConfig Wi-Fi* tab:

### 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.

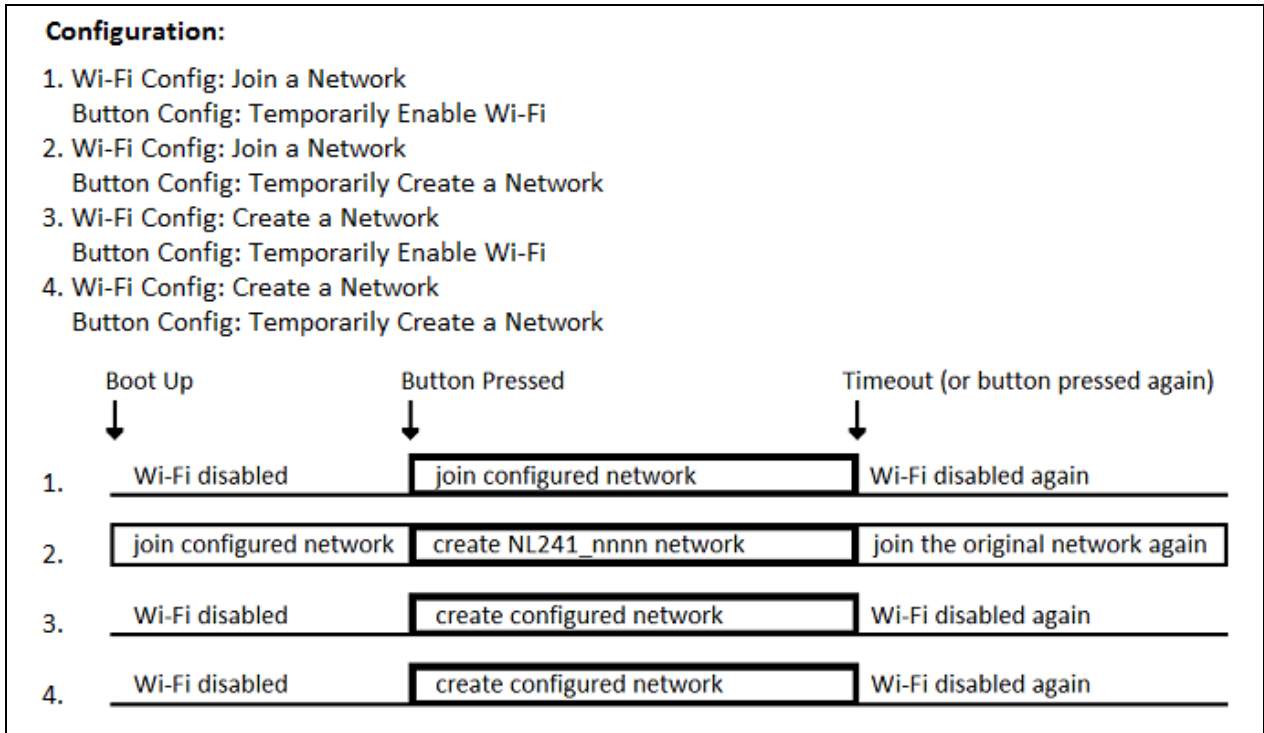
### Temporary Network Duration

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 5-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.

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



## 7. Configuring the NL241

The NL241 is configured using *DevConfig* 2.15 or greater. You can connect your NL241 to *DevConfig* using either a Wi-Fi connection or USB.

### 7.1 Configuring the NL241 with *DevConfig* via USB

#### NOTE

INSTALL the DEVICE DRIVER BEFORE plugging the NL241 into your computer for the first time. You will need the device driver properly installed before you can connect to the NL241 via USB. To install the device driver, download the latest version of *DevConfig* from our website. Under **Device Type**, select **Network Peripheral | NL241**. Click **Install USB Driver** and follow the prompts.

1. Ensure the NL241 is powered.
2. Connect the supplied USB cable between a USB port on your computer and the **USB** port on the NL241.

3. Open *DevConfig*.
4. Under **Device Type**, select **Network Peripheral | NL241**.
5. Click the **Browse** button next to **Communication Port**.
6. Select the port labelled **NL241**.
7. Click **OK**.
8. Click **Connect**.
9. Configure the NL241 as needed for your application.
10. Click **Apply** to save your changes.

## 7.2 Configuring the NL241 with *DevConfig* 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 flicker green with network activity. Note that the LED may only blink green 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. Launch *DevConfig*.
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 you do not know the address of the device and the device is connected to your local area network, you may be able to use the browse button to the right of **Communication Port** 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 *DevConfig* **Deployment | NL241** tab.)
9. Click **OK**.
10. Click **Connect**.

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

The NL241 must have an IP address before connecting via Telnet. Configuration via Telnet is not available in bridge mode.

1. Ensure the NL241 is powered and connected to your network.
2. Create a telnet session with the device over port 23.
3. Type the NL241 admin password (default password is **nl241**).
4. Type **help** to see a list of the functionality available when connected to the NL241 through Telnet.
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. 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's serial port to the **RS-232** port on the NL241.
2. Connect to the NL241 using a terminal emulator. The *DevConfig* "Unknown" device type or *HyperTerminal* are examples of simple terminal emulators. The default settings for this interface are 115200 baud, 8 data bits, no parity, 1 stop bit, no flow control.
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 through Telnet.

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.
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 Section 6, *Wi-Fi (p. 13)*, for more information about the types of Wi-Fi connections available. See Section 4, *Overview (p. 7)*, 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 *DevConfig* (see Section 7, *Configuring the NL241 (p. 17)*).
2. Click the **Wi-Fi** tab.
3. Set **Configuration** to **Join a Network**.
4. Press the browse button next to the **Network Name (SSID)** field to see a list of the available networks in the area. 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 your 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 joiners.

### 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 *DevConfig* (see Section 7, *Configuring the NL241* (p. 17)).
2. Click the **Wi-Fi** tab.
3. Set **Configuration** to **Create a Network**.
4. By default, the name of the network will be “NL241\_SerialNumber.” If you wish to change the name of this network, type a new name in the **Network Name (SSID)** field.
5. If you want your network to be encrypted, type the password to be used for the network in the **Password** field. (See Appendix C, *NL241 Settings* (p. C-1), for details on the password requirements.)
6. Other Wi-Fi settings are available from the **Settings Editor**, but can often be left at their default values. See Appendix C.2, *Wi-Fi Tab* (p. C-4), for more information on these settings.
7. Click **Apply** to save your 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-neighbour lists.

**Beacon Interval** – Devices in a PakBus network may broadcast a hello message to other devices in order to determine neighbour devices. Neighbour 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 neighbour if no other communication has taken place within the interval. If **Verify Interval** is set to **0**, the verify interval becomes 2.5 times the **Beacon Interval**. If both the **Beacon Interval** and **Verify Interval** are set to **0**, the verify interval becomes 300 seconds. 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 you are using the NL241 as a PakBus router to allow scheduled

collection of a network of dataloggers every 15 minutes, consider setting the **Verify Interval** to 30 minutes.

**Neighbours Allowed** (RS-232 port only) – You can set a list of “acceptable neighbours” which the NL241 expects to hear from within set intervals (the verify interval). If the NL241 does not hear from neighbours 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 **Neighbours Allowed** list except if the PakBus address is  $\geq 4000$ . Following a hello message, devices with PakBus addresses  $\geq 4000$  are automatically accepted as neighbours.

### 8.2.1.1 Physical Setup

Using the supplied serial cable, connect the NL241 **CS I/O** port or **RS-232** port to the datalogger **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

- Connect to the NL241 in *DevConfig* (see Section 7, *Configuring the NL241* (p. 17)).
- On the **NL241** tab:
  - Set **Bridge Mode** to **disable**.
- On the **RS-232** tab:
  - Set **Configuration** to **PakBus**.
  - Set **Baud Rate** to baud rate of attached device.
  - Set **Beacon Interval**, **Verify Interval**, and **PakBus Neighbours Allowed** as described above. Often, the default values can be used. However, an allowed neighbours list can be useful in restricting communication paths.
- 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

- Connect to the NL241 in *DevConfig* (see Section 7, *Configuring the NL241* (p. 17)).
  - Set **Bridge Mode** to **disable**.

- On the **CS I/O** tab:
  - Set **Configuration** to **PakBus**.
  - Set **SDC address**. (Note that if multiple peripherals are connected to a datalogger **CS I/O** port, each must have a unique SDC address.)
  - Set **Beacon Interval** and **Verify Interval** as described above. Often, the default values can be used.
- On the **Network Services** tab:
  - Make note of the **PakBus/TCP 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 datalogger and type the PakBus address of the datalogger.
5. Press **Apply** to save the changes.

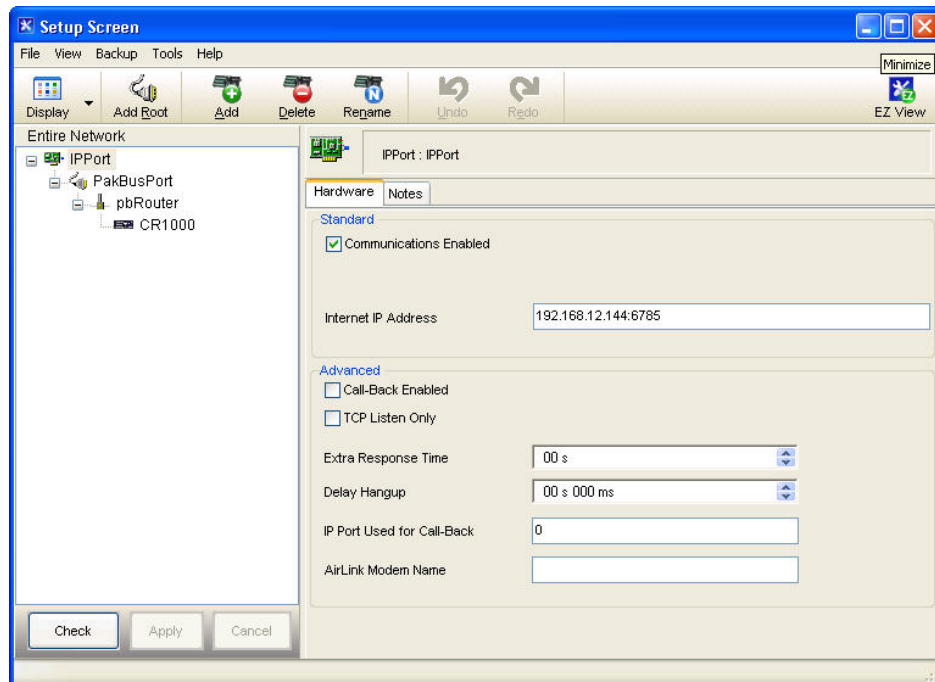


FIGURE 8-1. PakBus router LoggerNet setup

#### 8.2.1.4 Connect

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

### 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 datalogger over the CS I/O port. This enables the datalogger to use its TCP/IP stack to interpret the packet and, therefore, all of the datalogger TCP services are available. In bridge mode, only the Wi-Fi settings are valid. All other functionality is disabled. All settings (that is, IP, netmask, gateway) are configured in the datalogger. However, in bridge mode, the device will intercept any TCP traffic on the **TCP Configuration Port Number**. This allows the device to still be configured remotely by IP connection using *DevConfig*. The **TCP Configuration Port Number** is a user setting with a default value of **6786**.

#### 8.2.2.1 Physical Setup

Attach an antenna to the NL241 antenna connector. Using the supplied serial cable, connect the NL241 **CS I/O** port to the datalogger **CS I/O** port. Ensure that the device is powered up by inspecting the LED.

#### 8.2.2.2 Configuring the NL241

Connect to the NL241 in *DevConfig* (see Section 7, *Configuring the NL241* (p. 17)). In 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 datalogger.

#### 8.2.2.3 Configuring the Datalogger

1. Connect a serial cable from the computer COM port to the datalogger **RS-232** port.
2. Open *DevConfig*. Select the device type of the datalogger (CR800, CR1000, or CR3000), the appropriate **Communication Port**, and the **Baud Rate**. Click **Connect** to connect to the datalogger.
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. You will find the information acquired by DHCP in the info box on the **Ethernet** and **CS I/O IP** tabs.
4. Press **Apply** to save the changes and then close *DevConfig*.

**NOTES**

The NL241 must be connected to the datalogger before configuring the datalogger with *DevConfig*. If it is not connected, the Ethernet settings will not be displayed.

By default, the NL241 uses the datalogger CS I/O Interface #2. If connecting more than one NL241 to a datalogger, one NL241 can be configured to use CS I/O Interface #1. This is done by connecting to the NL241 in *DevConfig*, going to the **Settings Editor** 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 datalogger **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.

**8.2.2.4 LoggerNet Setup**

The next step is to run *LoggerNet* and configure it to connect to the datalogger via the Wi-Fi port. (See example in FIGURE 8-2 below.) Note that your *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**. Type the datalogger IP address and port number. The IP address and port number are input on the same line separated by a colon. (The datalogger default port number is 6785. It can be changed using *DevConfig*. Unless firewall issues exist, the port number does not need to be changed from its default value.)
2. Add a PakBus Port.
3. Add the datalogger (CR6, CR800, CR1000, or CR3000) and input the PakBus address of the datalogger.
4. You can verify that your settings are correct by selecting the datalogger in the **Network Map**, clicking the **Clock** tab, and clicking **Check Clocks**. If your settings are correct, you should see the current clock of your server and datalogger.

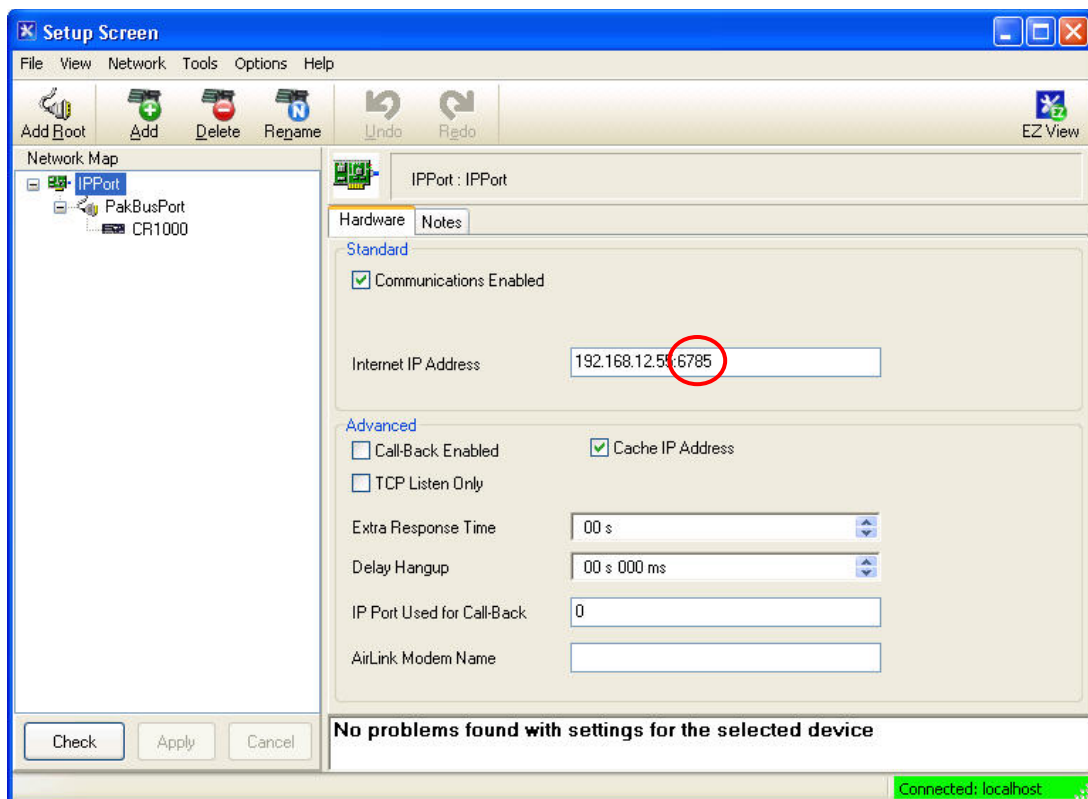


FIGURE 8-2. Bridge mode LoggerNet setup

### 8.2.2.5 Connect

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

## 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, and 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 datalogger **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 Power LED.

### 8.2.3.2 Configuring the NL241

#### RS-232 Serial Server

Connect to the NL241 in *DevConfig* (see Section 7, *Configuring the NL241* (p. 17)).

- On the **NL241** tab:
  - Set **Bridge Mode** to **disable**.
- On the **RS-232** tab:
  - Set **Configuration** to **TCP Serial Server**.
  - Set **Baud Rate** to baud rate of attached device.
  - Make note of the **Serial 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

Connect to the NL241 in *DevConfig* (see Section 7, *Configuring the NL241* (p. 17)).

- On the **NL241** tab:
  - Set **Bridge Mode** to **disable**.
- On the **CS I/O** tab:
  - Set **Configuration** to **TCP Serial Server**.
  - Set **SDC address**. (Note that if multiple peripherals are connected to a datalogger **CS I/O** port, each must have a unique SDC address.)
  - Make 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 datalogger via the Wi-Fi port. (See example in FIGURE 8-3 below.)

1. In the *LoggerNet Setup Screen*, click **Add Root** and choose **IPPort**. Input 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.
3. Add the datalogger and input the PakBus address of the datalogger.
4. Press **Apply** to save the changes.
5. You can verify your settings are correct by selecting the datalogger in the **Network Map**, clicking the **Clock** tab, and clicking **Check Clocks**. If your settings are correct, you should see the current clock of your server and datalogger.

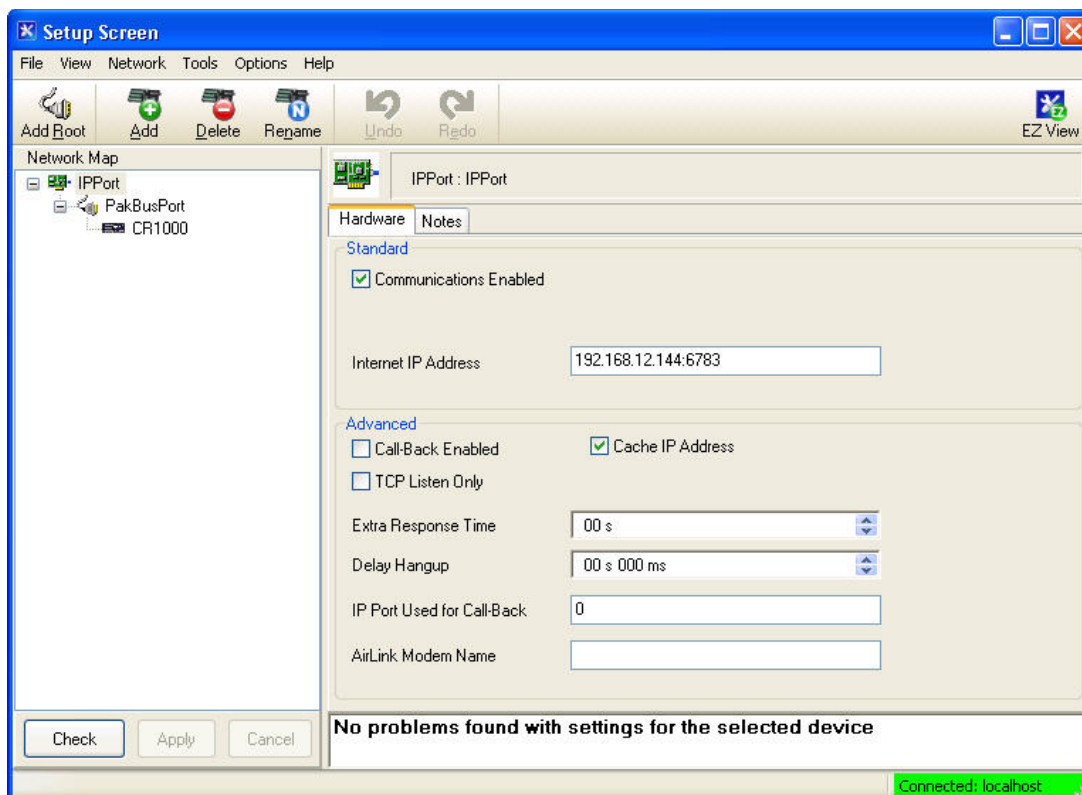


FIGURE 8-3. CS I/O serial server LoggerNet setup

#### 8.2.3.4 Connect

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

#### 8.2.3.5 Serial Sensors

The NL241 configured as an RS-232 serial server as described above can be used to communicate with a serial sensor. However, *LoggerNet* is not capable of communicating with the serial sensor. You must have some other method of communicating with the sensor.

### 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 master client. 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 master client over the established TCP connection. The Modbus RTU device is generally a datalogger connected to the RS-232 (or CS I/O) port or a datalogger located remotely over a transparent radio (for example, 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 master 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 datalogger. The NL241 TLS proxy server maintains a secure TLS connection with a remote TLS client and forwards data onto a datalogger using a standard TCP connection thus enabling communication with TLS clients. The TLS client can be a web browser using HTTPS or another user-supplied TLS client. This offloads from the datalogger 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 *DevConfig*.

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 *DevConfig*.

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

1. Load the user-supplied, PEM-formatted TLS private key using the **Set TLS Key** button. A file dialogue will open. Navigate to the key file and click **Open**.

2. Load the user-supplied, PEM-formatted TLS certificate using the **Set TLS Certificate** button. A file dialogue will open. Navigate to the certificate file and click **Open**.
3. Enter the **TLS Private Key Password** if the TLS private key is encrypted. Otherwise, leave the setting blank.
4. After loading the key and certificate, click the **Apply** button. The NL241 will reboot. Connect with *DevConfig* again and navigate to the **Settings Editor** tab and then to the **TLS** tab. The **TLS Status** should say **Initialized**.

**NOTE**


---

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

---

**NOTE**


---

If the status of the TLS stack is **Initialized**, the NL241 will automatically negotiate a secure TLS connection with *DevConfig* 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 datalogger using a standard TCP connection thus enabling communication 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 datalogger. In this way, a remote TLS client can establish a TLS connection with a datalogger.

The settings found in the **TLS Proxy Server** and **TLS** tab in *DevConfig* are used to configure the 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 FIGURE 8-4.

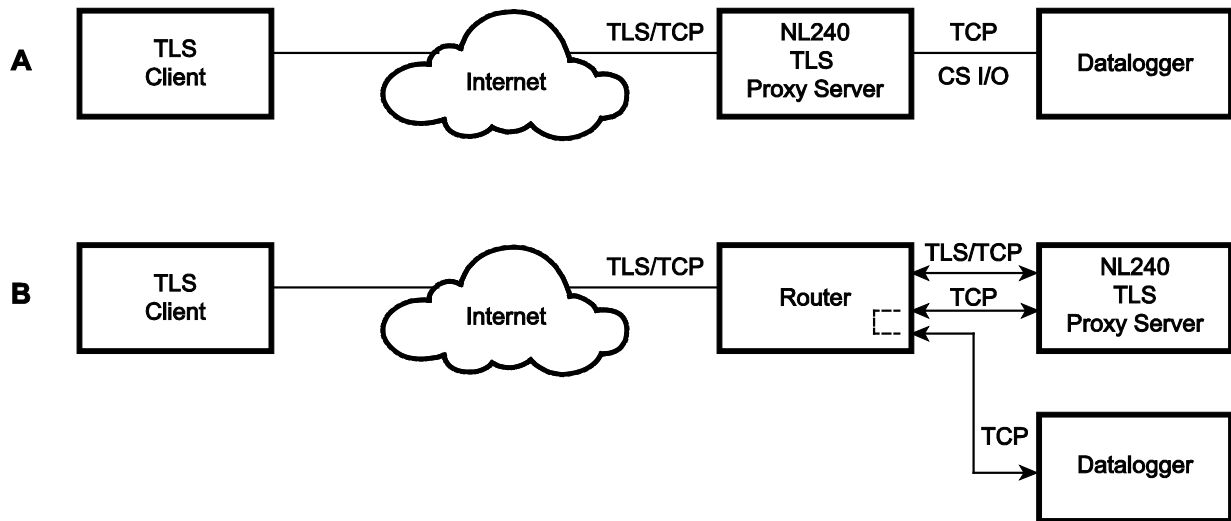


FIGURE 8-4. TLS proxy server configurations

**Configuration A**

In Configuration A, the NL241 decrypts TLS traffic and forwards the unencrypted TCP traffic to the datalogger over the **CS I/O** port. The NL241 is able to “learn” the IP address of the attached datalogger and will open a TCP connection on the “learned” IP address.

**Configuration B**

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

To configure the NL241 TLS proxy server to communicate with a datalogger attached to the **CS I/O** port or with a datalogger over a Wi-Fi connection, open *DevConfig* and configure the following settings.

**Settings Editor | TLS Proxy Server tab**

- Set the **TLS Proxy Server** setting to **enable**.
- 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 datalogger 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.
- Set the **TLS Proxy Forward Physical Port** to **CS I/O Port** for Configuration A or to **Wi-Fi** for Configuration B.

- For Configuration A, leave the **TLS Proxy Forward IP Address** set to **0.0.0.0**. For Configuration B, enter the datalogger IP address in the **TLS Proxy Forward IP Address** setting. This address must be configured in the datalogger. It must be a unique, static IP address on the same subnet as the 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 datalogger would be 192.168.5.2 provided there are no other devices on the subnet with that address.
- Set the **TLS Proxy Forward Port**. This is the TCP port number that the proxy server will use when it opens a TCP connection to the datalogger to forward unencrypted data. The datalogger TCP server must be set to communicate on this port number. The default value for the datalogger PakBus/TCP service port is **6785**, so this setting can likely be left at the default. The datalogger 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.
- 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.

To configure the datalogger for Configuration A, connect to the datalogger using *DevConfig* and select the **CS I/O IP** tab. Set the CS I/O Interface **IP Address** to a static IP address. Use the datalogger CS I/O Interface that corresponds to the NL241 **CS I/O IP Interface Identifier** setting. To configure the datalogger for Configuration B, connect to the datalogger using *DevConfig* and select the **TCP/IP** tab. Set the Ethernet Interface **IP Address** to a static IP address.

For either configuration, the IP address must not be 0.0.0.0, and it must be unique on the same subnet as the NL241 IP address. For example, if the NL241 IP address is 192.168.5.1 and subnet mask is 255.255.255.0, the datalogger address could be set as 192.168.5.2 provided there are no other devices on the subnet with that address. Also, set the datalogger subnet mask to match that of the NL241.

The datalogger 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 datalogger always listens on port 80 for HTTP, therefore, no TCP port configuration is necessary for using HTTP.

#### 8.2.6.2 DevConfig TCP Encrypted Communication to the NL241

In order to use *DevConfig* TCP encrypted communication with the NL241, you will need to load your TLS private key and TLS certificate into the NL241. This is done from the **Settings Editor | TLS** tab in *DevConfig*. Once the private key and certificate are loaded successfully, the **TLS Status** field should read **Initialized**.

To use TCP encrypted communication, select the **Use IP Connection** check box in *DevConfig*. Input the NL241 IP address (or press the browse button to select it from a list of NL241s connected to the network) and press **Connect**.

**NOTES**

If the status of the TLS stack is **Initialized**, the NL241 will automatically negotiate a secure TLS connection with *DevConfig* as long as the **Use IP Connection** option is selected.

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

### 9.1 Working Around Firewalls

The NL241 can be used to provide a connection between *LoggerNet* and a datalogger when both are behind firewalls as shown in FIGURE 9-1. The NL241 must be on a public IP address and will act as a common meeting place for all PakBus communications.

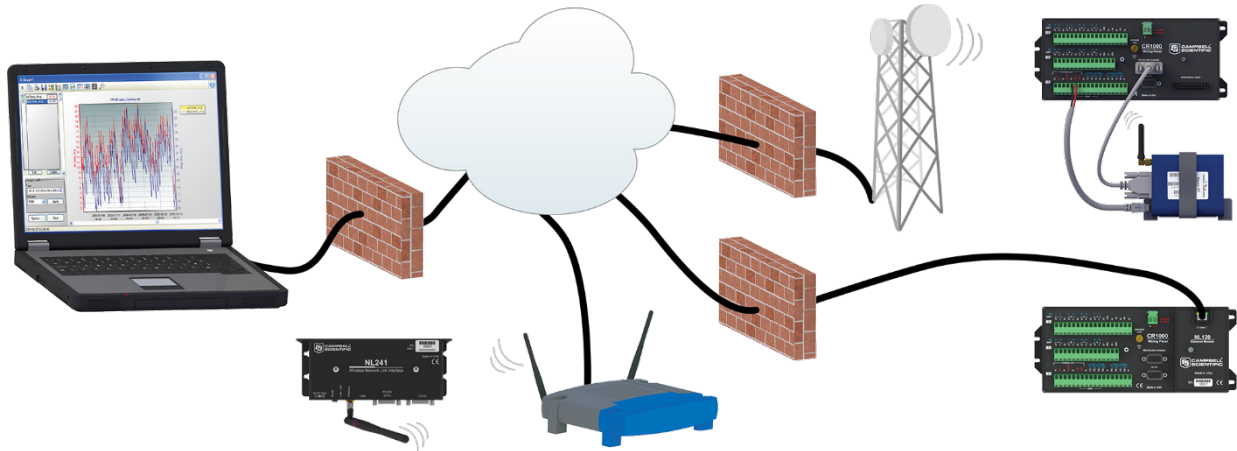


FIGURE 9-1. Working around firewalls

#### 9.1.1 Configuring the NL241

Connect to the NL241 in *DevConfig* (see Section 7, *Configuring the NL241* (p. 17)).

- On the **NL241** tab:
  - Set **Bridge Mode** to **disable**.
  - Set **DHCP Enabled** to **disable**.
  - Input the **IP Address**, **Network Mask**, and **Default Gateway**. These values can be provided by your network administrator.

- On the **Network Services** tab:
  - Make note of the **PakBus/TCP Service Port**.

### 9.1.2 Configuring the Datalogger

#### NOTE

The datalogger must first be configured for internet communication (that is, through an NL115, an NL120, a second NL241, or a cellular modem).

1. Connect a serial cable from the computer COM port to the datalogger **RS-232** port.
2. Open *DevConfig*. Select the device type of the datalogger (CR800, CR1000, or CR3000), the appropriate **Communication Port**, and **Baud Rate**. Press **Connect** to connect to the datalogger.
3. On the **Network Services** tab:
 

Under **PakBus TCP Clients**, input the NL241 **IP address** and **PakBus TCP Service Port**.
4. Press **Apply** to save the changes and then close *DevConfig*.

## 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 ability to correct simple errors without a call to Campbell Scientific technical support.

When your Campbell Scientific software cannot establish a link to a remote datalogger that is connected to the NL241, do the following:

1. Check all your 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 your cables and antenna.
  - Verify that your antenna is securely attached to the NL241 and oriented in the same direction as the antenna of your WAP. The **Link/Act** light on the NL241 should start blinking when it is connected to a network. Also, the WLAN activity light on your WAP (if it has one) should be blinking 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.

- Make sure you have entered the correct SSID and password (if needed) for your network.
- Make sure the NL241 is connected to the right WLAN (**Wi-Fi Status** in *DevConfig* or show | Wi-Fi settings | Wi-Fi in a telnet session).
- Make sure the wireless network you are connecting to has a RSSI level of greater than (>) -90dBm (in *DevConfig*, **Settings Editor** | **Wi-Fi** | **Wireless Networks in Area**).
- 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

- If you are using DHCP to assign an IP address to the NL241, use *DevConfig* to read the IP address assigned to your 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).
  - The IP address assigned to the NL241 must be unique on your network.
  - When bridge mode is enabled, the datalogger controls how the IP address is assigned. Make sure your datalogger is connected correctly to the 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/PC400/RTDAQ* match the settings in the NL241.
- Note that PakBus and serial server communications use different port numbers. The default port number for PakBus communications is **6785**. The default port number for CS I/O serial server communications is **6783**. The default port number for RS-232 serial sever communications is **6784**. The correct port number must follow the IP address of the 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 you have installed the latest drivers for the NL241. These can be downloaded from our website at [www.campbellsci.eu](http://www.campbellsci.eu).
8. If the NL241 is configured as a CS I/O serial server, verify that any other SDC device attached to the datalogger is using a different SDC address. For example, if the NL241 is configured for SDC7, any other device attached to the datalogger cannot use SDC7.
9. If communicating over a slow or intermittent connection, it may be necessary to lower the **Maximum Packet Size** of the datalogger in *LoggerNet Setup* and/or add **Extra Response Time** to the **PakBus Port** in *LoggerNet Setup*.
10. Reset the NL241 to its default settings.
  - If none of the above steps correct your communication problems, reset the NL241 to its default settings. This can be done using the **Factory Defaults** button in *DevConfig* or by using the **Defaults** command in a telnet session with the NL241.
11. Verify you are running the latest revision of firmware (operating system). 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.eu/downloads](http://www.campbellsci.eu/downloads). There is no charge for this download. See Appendix D, *Sending a New OS to the NL241 (p. D-1)*, 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:
  - 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 communication network.
  - Save a copy of the NL241 settings (in XML format) using *DevConfig*.
  - Save a copy of the NL241 event log. This is low-level code that can be used by Campbell Scientific's 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 favourite telnet program. Once you have logged in, type "eventlog" at the prompt. Record the date and time that you did this. Copy and paste the output into a text file.
  - Once the eventlogs have been copied, you can type "eventlog erase" at the prompt to clear the log. If you want to add a date to indicate when the logs were last cleared, you can enter "eventlog erase date" where date is a string of up to 8 characters.

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



## 11. Attributions

PakBus is a registered trademark of Campbell Scientific, Inc.

### lwIP

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

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

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

*THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.*



# Appendix A. Glossary

---

## Auto-IP

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

It is used in the NL241 when DHCP is enabled but the NL241 is not able to access a DHCP server. A local IP address is assigned in the 169.254.XXX.XXX range. This process can take up to two minutes.

## Beacon Interval

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

## 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 Wi-Fi and CS I/O ports.

## DHCP (Dynamic Host Configuration Protocol)

A TCP/IP application protocol in which IP addresses are assigned automatically by a DHCP server. Note that an IP address obtained through DHCP is not static but is leased for a period of time set by the network administrator. The address may change, if the NL241 is powered down.

## Hello Exchange

A communication exchange that establishes two PakBus devices as neighbours. 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 neighbours. Only a hello exchange can establish two devices as neighbours.

## Neighbour (PakBus Neighbour)

A device in a PakBus network that can be communicated with directly (that is, not via a router). Every PakBus device maintains its own neighbour list.

**PakBus**

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

**PakBus Node**

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

**Port Number**

A port number is a way to identify a specific process to which a network message is to be forwarded when it arrives at the NL241.

**SDC (Synchronous Device Communications)**

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

**Serial Server**

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

**Proxy (Proxy Server)**

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

**TLS (Transport Layer Security)**

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

**Verify Interval**

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

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

---

## B.1 CS I/O

The CS I/O cable is a 9-pin, straight-through cable with all 9 pins connected. The supplied SC12 cable (pn #16675) is recommended. Pin configuration for the CS I/O port is shown in TABLE B-1.

TABLE B-1. CS I/O Pinout		
Pin	Datalogger (DB9 Female) Function	Peripheral (DB9 Male) Function
1	5 Vdc	N/C
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

## B.2 RS-232

A DB9 female to DB9 male cable (such as Campbell Scientific pn #10873) is used to connect the NL24 **RS-232** port to the datalogger **RS-232** port. The supplied SC12 cable can also be used. A DB9 female null modem cable (such as Campbell Scientific pn #13657) 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 configuration for the **RS-232** port is shown in TABLE B-2.

TABLE B-2. RS-232 Pinout		
Pin	Datalogger (DCE, DB9 Female) Function	Peripheral (DTE, DB9 Male) Function
1	DCD	DCD
2	TXD	RXD
3	RXD	TXD
4	DTR	DTR
5	SIGNAL GND	SIGNAL GND
6	DSR	DSR
7	CTS	RTS
8	RTS	CTS
9	RING	RING

## B.3 USB

The USB cable is the supplied USB A to micro B style cable (Campbell Scientific pn #27555). This is used only for device configuration. Pin configuration for the **USB** port is shown in TABLE B-3.

TABLE B-3. USB Micro-B	
Pin	Function
1	VBUS (Not Used)
2	Data –
3	Data +
4	N/C
5	GND

## B.4 Power

Pin configuration for the **Power** connector is shown in TABLE B-4.

TABLE B-4. Power In	
Pin	Function
Centre	9 to 16 Vdc
Sleeve	Power GND

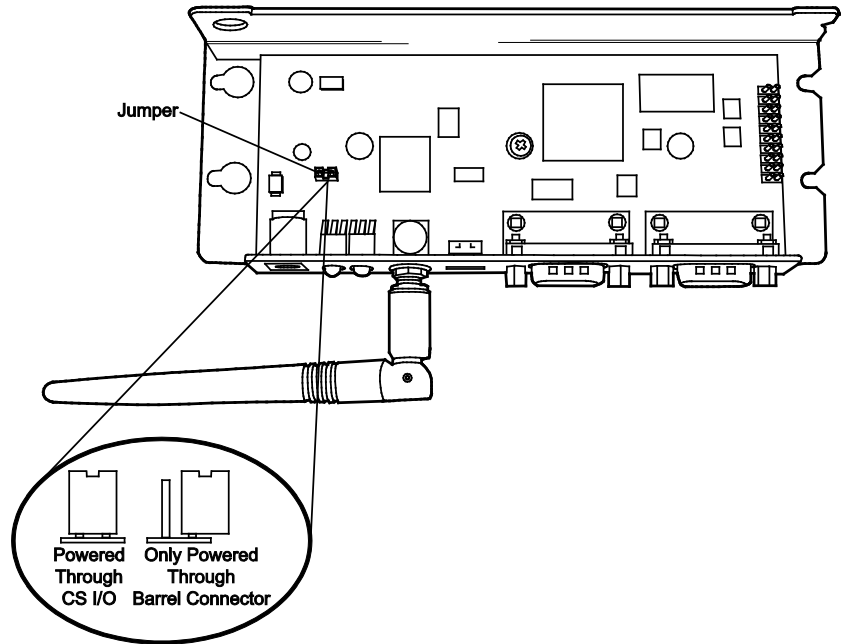
## B.5 LED

The color and light pattern of the LED indicate the state of the device as described in TABLE B-5.

TABLE B-5. LED	
State	Description
Off	The device is powered off or the Wi-Fi has been disabled via the <b>Mode</b> button configuration or via an <b>IPNetPower()</b> instruction from the datalogger. See Section 6.7, <i>Mode Button (p. 16)</i> , for information on the <b>Mode</b> button configuration.
On red solid	After power-up: scanning nearby networks and trying to join or create a Wi-Fi network.
Green flicker	After successfully joining or creating a network, the LED will flicker green with network activity. Note that the LED may only blink green once every few seconds on the created network or networks that aren't very busy.
Red double-strobe	If the device is unsuccessful at joining or creating a network, the LED will periodically double-strobe red. The device will attempt to connect to the network again after approximately one minute.
Fast red and green blink	OS Download in progress – DO NOT DISCONNECT POWER

## B.6 Power Jumper

If you wish 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 red LED 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.







# Appendix C. NL241 Settings

---

All of the NL241 settings available from the **Settings Editor** in *DevConfig* are described below.

## C.1 Main Tab

**Model** (read only)

Model name.

**Serial Number** (read only)

Specifies the NL241 serial number assigned by the factory.

**OS Version** (read only)

Operating system version currently in the NL241.

**Compile Date** (read only)

Operating system compile date.

**Bridge Mode**

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

**Bridge Mode Disabled**

With **Bridge Mode** 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 datalogger over the **CS I/O** port. Some filtering is done in order to minimize the amount of traffic on the **CS I/O** port, but every packet that is transmitted to the datalogger is sent intact as a complete Ethernet/TCP packet. This enables the datalogger to use its TCP/IP stack to interpret the packet, and, therefore, all of the datalogger 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 datalogger. However, in bridge mode, the device will intercept any TCP traffic on the TCP configuration port number. This allows the device to still be configured remotely by IP connection using *DevConfig*. The **TCP Configuration Port Number** is a user setting with a default value of 6786.

---

### NOTE

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

---

### CS I/O IP Interface Identifier

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

### Bridge Mode Forward Code

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

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

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

#### Forward Code Values

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

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

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

### DHCP

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, you may have to refresh by pressing F5.

### IP Address

The IP address uniquely identifies this node on an internet. If DHCP is disabled, a static IP address must be obtained from your network administrator for use with this device. If DHCP is enabled, the IP address obtained from the local DHCP server will be displayed in the **Status** 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 datalogger and cannot be edited here. It must be edited in the datalogger settings. The setting obtained from the datalogger will be displayed in the **Status** box on the **Deployment | NL241** tab.

### 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 datalogger and cannot be edited here. It must be edited in the datalogger settings. The setting obtained from the datalogger will be displayed in the **Status** box on the **Deployment | NL241** tab.

### 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 datalogger and cannot be edited here. It must be edited in the datalogger settings. The setting obtained from the datalogger will be displayed in the **Status** box on the **Deployment | NL241** tab.

### 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.

### 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.

### 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 *DevConfig* 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.

### TCP Configuration Port Number

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

## C.2 Wi-Fi Tab

### Wi-Fi Status

Status of the Wi-Fi Module.

### 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

If this mode is selected the device will be the creator of a network. Enter the desired name of the network in the SSID setting. A network created by the module supports up to 8 joiners. If a password is supplied, the network that is created will be secured by WPA2 encryption. If no password is supplied, the network that is 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 of **Auto**, the device will select a channel on which to operate that has minimal interference from other networks detected in the area

### 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. 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 on the ... button or view the **Wireless Networks in Area** list.

#### NOTE

When the **Browse** button is clicked or the **Refresh** button inside the resulting dialogue 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.

#### 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).

#### EAP User

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

#### EAP Password

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

#### 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 MSCHAPv2, MSCHAP, CHAP, and PAP.

#### 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 behaviour is the same for both button configurations.

### 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 select a channel on which to operate that has minimal 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 centre 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.

### 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.

---

### 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's 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 communication speed and low power consumption.

#### Mode 1

If this mode is selected, the device will disable the Wi-Fi module's 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's 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.

#### 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's IP address. For example, the datalogger's webpage can be accessed by entering the domain name specified here into a web browser.

#### 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.

## C.3 RS-232 Tab

#### RS-232 Configuration

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

##### TCP Serial Server

The device will listen for an incoming TCP connection from a remote client. The port number of the listening connection is specified in the **RS-232 Service Port** 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.

## **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).

## **RS-232 Baud Rate**

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

## **RS-232 RTS**

The 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**).



### RS-232 TCP Timeout

This setting will determine 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).

### 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 behaviour 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's 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**.

### **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 neighbouring 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.

### **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 neighbour if no other communication has taken place within the interval.

### **Neighbours Allowed RS-232**

This setting specifies the explicit list of PakBus node addresses that the NL241 will accept as neighbours on the RS-232 port. If the list is empty (the default value), any node will be accepted as a neighbour. This setting will not affect the acceptance of a neighbour if that neighbour's address is greater than 3999. The formal syntax for this setting follows:

```
neighbour : = { "(" 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 neighbours to the NL241.

### **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 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).

### **RS-232 TCP Serial Client IP Address**

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

### **RS-232 TCP Serial Client Port**

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

## C.4 CS I/O Tab

### CS I/O Configuration

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

#### TCP Serial Server

The device will listen for an incoming TCP connection from a remote client. The port number of the listening connection is specified in the **CS I/O Service Port** 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.

### 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).

### SDC Address

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

### CS I/O TCP Timeout

This setting, in units of seconds, will determine how fast the 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).

### **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 neighbouring nodes. It will also govern the default verification interval if the value of the **CS I/O Verify Interval** setting is set to **0**.

### **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 neighbour if no other communication has taken place within the interval.

### **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 slave device(s) attached to the **CS I/O** port. If no answer is received within the timeout period, the MODBUS/TCP server will reply to the MODBUS/TCP client with error code 0x0B (Target Device Failed to Respond).

## **C.5 Net Services Tab**

### **Telnet**

Enables/Disables the telnet service.

### **Telnet Port Number**

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

### **Telnet Timeout**

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

### **Ping (ICMP)**

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

### **PakBus Address**

This setting specifies the PakBus address for this device. The value for this setting must be chosen such that the address of the device will be unique in the datalogger network. Duplication of PakBus addresses in two or more devices can lead to failures and unpredictable behaviour in the PakBus network. When a device has a neighbour list or neighbour filter setting filled in for a port, any device that has an address greater than or equal to 4000 will be allowed to connect to that device regardless of the neighbour filter.

**PakBus/TCP Service Port**

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

**PakBus/TCP Password**

Specifies the password that will be used to authenticate any incoming (server) or outgoing (client) PakBus/TCP sessions. This password is used by the server to generate a challenge to any client that connects to the PakBus/TCP 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.

**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.

**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).

**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 Neighbour Address**

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

**PakBus Address**

Specifies the address that the route will reach.

**Response Time**

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

**Central Routers**

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

## C.6 TLS Proxy Server Tab

**TLS Proxy Server**

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

**NOTE**

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

**TLS Proxy 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 datalogger over the CS I/O port and do unencrypted data transfer with the datalogger. 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 datalogger 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 datalogger on the HTTP port 80 (range 1 to 65535).

### 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 datalogger over the CS I/O port and do unencrypted data transfer with the datalogger. If the **TLS Proxy Forward Physical Port** is specified to be **Wi-Fi**, the NL241 will open the TCP connection over Wi-Fi on the **TLS Proxy Forward IP Address**.

### 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 datalogger automatically. The datalogger must be configured with a static IP address that is unique and that exists on the same subnet as the NL241's 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 datalogger here.

### 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 datalogger over the CS I/O port and do unencrypted data transfer with the datalogger. If the **TLS Proxy Forward Physical Port** is specified to be **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 datalogger's TCP server, the NL241's TCP client application must open a socket to that server. The socket of the datalogger's TCP server is uniquely identified by an IP address and a port number. This entry is where the port number of the NL241's TCP client is set. The datalogger 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 datalogger 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 datalogger on the HTTP port 80.

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

### TLS Proxy Timeout

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

# C.7 TLS Tab

## TLS Status (read only)

Specifies the current status of the TLS network stack.

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

## TLS Private Key Password

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

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

## TLS Private Key

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

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

## TLS Certificate

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

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



# Appendix D. Sending a New OS to the NL241

---

Whenever a new operating system is released for the NL241, it will be available from our website, [www.campbellsci.eu/downloads](http://www.campbellsci.eu/downloads).

## D.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 *DevConfig*.
4. Select the **NL241** under **Device Type**.
5. Select the appropriate **Communication Port**.
6. Go to the **Send OS** tab.
7. Press the **Start** button.
8. In the resulting dialogue box, select the file that should be sent to the device as an operating system (this file should have an .obj extension) and press the **OK** button.
9. The operating system will be sent to the NL241.
10. After the file has been sent, the LED on the NL241 will blink 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 blinking, 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 blinking.

## D.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 datalogger **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 flicker green with network activity. Note that the LED may only blink green 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 *DevConfig*.
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, you will need to 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 **Communication Port** control on the left panel. If you do not know the address of the device and the device is connected to your local area network, you may be able to use the ... button to the right of **Communication Port** to discover the list of devices on the network. Whatever address is entered, it must end with :6786 in order to connect the device configuration service.
9. Go to the **Send OS** tab.
10. Click the **Start** button.
11. In the resulting dialogue box, select the file that should be sent to the device as an operating system (this file should have an .obj extension) and press the **OK** button.
12. The operating system will be sent to the NL241.
13. After the file has been sent, the power LED on the NL241 will blink 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 blinking, 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 blinking

# Appendix E. Radio Frequency Emission

---

Changes or modifications to the NL241 not expressly approved by Campbell Scientific 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 B digital device, pursuant to part 15 of the FCC Rules.

These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if 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.eu/nl241](http://www.campbellsci.eu/nl241)





## Campbell Scientific Worldwide Offices

---

### Australia

Location: Garbutt, QLD Australia  
Email: [info@campbellsci.com.au](mailto:info@campbellsci.com.au)  
Website: [www.campbellsci.com.au](http://www.campbellsci.com.au)

### Brazil

Location: São Paulo, SP Brazil  
Email: [andread@campbellsci.com.br](mailto:andread@campbellsci.com.br)  
Website: [www.campbellsci.com.br](http://www.campbellsci.com.br)

### Canada

Location: Edmonton, AB Canada  
Email: [dataloggers@campbellsci.ca](mailto:dataloggers@campbellsci.ca)  
Website: [www.campbellsci.ca](http://www.campbellsci.ca)

### China

Location: Beijing, P. R. China  
Email: [info@campbellsci.com.cn](mailto:info@campbellsci.com.cn)  
Website: [www.campbellsci.com.cn](http://www.campbellsci.com.cn)

### Costa Rica

Location: San José, Costa Rica  
Email: [info@campbellsci.cc](mailto:info@campbellsci.cc)  
Website: [www.campbellsci.cc](http://www.campbellsci.cc)

### France

Location: Antony, France  
Email: [info@campbellsci.fr](mailto:info@campbellsci.fr)  
Website: [www.campbellsci.fr](http://www.campbellsci.fr)

### Germany

Location: Bremen, Germany  
Email: [info@campbellsci.de](mailto:info@campbellsci.de)  
Website: [www.campbellsci.de](http://www.campbellsci.de)

### South Africa

Location: Stellenbosch, South Africa  
Email: [sales@csafrica.co.za](mailto:sales@csafrica.co.za)  
Website: [www.campbellscientific.co.za](http://www.campbellscientific.co.za)

### Southeast Asia

Location: Bangkok, Thailand  
Email: [info@campbellsci.asia](mailto:info@campbellsci.asia)  
Website: [www.campbellsci.asia](http://www.campbellsci.asia)

### Spain

Location: Barcelona, Spain  
Email: [info@campbellsci.es](mailto:info@campbellsci.es)  
Website: [www.campbellsci.es](http://www.campbellsci.es)

### UK

Location: Shepshed, Loughborough, UK  
Email: [sales@campbellsci.co.uk](mailto:sales@campbellsci.co.uk)  
Website: [www.campbellsci.co.uk](http://www.campbellsci.co.uk)

### USA

Location: Logan, UT USA  
Email: [info@campbellsci.com](mailto:info@campbellsci.com)  
Website: [www.campbellsci.com](http://www.campbellsci.com)

Please visit [www.campbellsci.com/contact](http://www.campbellsci.com/contact) to obtain contact information  
for your local US or international representative.