



AN706: EZSP-UART Host Interfacing Guide

This application note describes how to connect a Host processor to a Network Co-Processor (NCP) using the UART-based EmberZNet Serial Protocol (EZSP). It assumes that you already have a basic understanding of the EZSP-UART Gateway protocol, as well as the signals needed by the UART interface. If not, refer to *UG101: UART Gateway Protocol Reference Guide* and *UG115: ASH v3 Protocol Reference* before continuing. This application note has been updated to EmberZNet PRO 6.6 to reflect a minor update to the Silicon Labs Zigbee application framework, though the content of the EZSP-UART interface still applies to earlier versions of the EmberZNet PRO stack.

KEY POINTS

- EZSP-UART protocol overview
- Physical interfaces
- Command line options for Host applications
- Hardware design considerations
- Powering up, power cycling, and rebooting
- Bootloading

1. Protocol Overview

Silicon Labs designed EZSP as a protocol to allow communications between components running pieces of the EmberZNet PRO wireless mesh stack, namely a Host processor and an NCP. The Host processor runs the application layer and executes on the POSIX platform such as Mac OS, Linux, or a Windows PC running Cygwin or the new Windows 10 BASH shell. You can also run this on an embedded platform like the Raspberry Pi. This lets you develop and test your application on an easy-to-use platform before porting your solution to a different Host processor with few changes. The NCP runs the EmberZNet PRO stack and physical layer (PHY). It is deployed and executed on a Silicon Labs wireless mesh chip processor in either the Wireless Gecko EFR32™ or Ember EM35x portfolio.

2. EZSP-UART Physical Interfaces

The following figure represents the EZSP-UART physical interfaces.

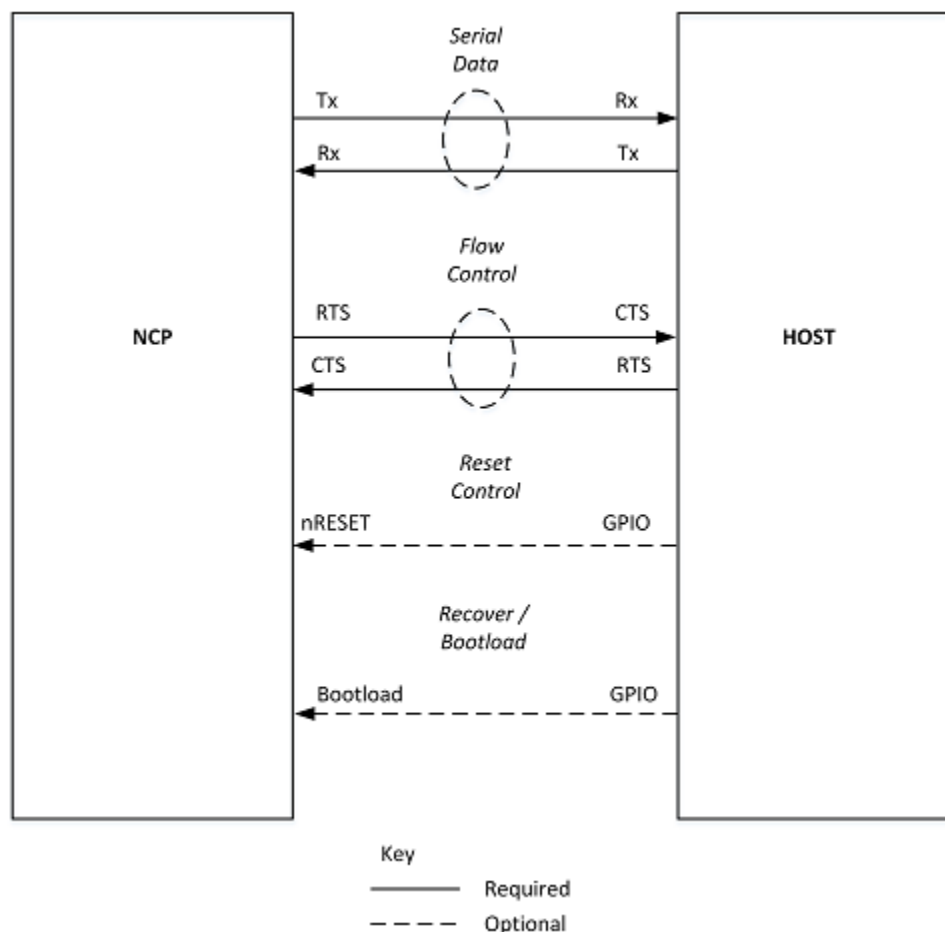


Figure 2.1. EZSP-UART Physical Interfaces

2.1 Serial Data: Tx and Rx

The EZSP protocol sends data in both directions, utilizing a standard Universal Asynchronous Receiver-Transmitter (UART). Both the Tx and Rx pins are utilized on the NPC and Host. When connecting the NCP and Host, the connections should be from NCP Tx to Host Rx and NCP Rx to Host Tx. This interface is required for NCP-to-Host communications.

2.2 Flow Control: RTS and CTS

EZSP requires flow control for operation. This can be in the form of either XON/XOFF software flow control or RTS/CTS hardware flow control. RTS/CTS hardware flow control is part of the standard UART interface. When connecting the NCP and Host, the connections should be from NCP CTS to Host RTS and NCP RTS to Host CTS. With this interface, RTS enables transmission from the Host to the NCP and CTS enables NCP transmissions to the Host.

If needed, the Host can restrain the NCP from sending to it by deasserting the NCP's CTS input. The NCP will stop sending immediately, except to finish sending a byte already in progress. The NCP will do the same to the Host when it requires the Host to stop sending data.

While hardware or software flow control can be utilized, EZSP-UART will have better performance and speed using hardware flow control. Hardware flow control allows operation up to 115,200 bps (other baud rates may be selected by a configuration value programmed into flash during manufacturing).

2.3 Reset Control: nRESET

nRESET is a hardware input that can reset the NCP. For normal operation, the nRESET line should be held high. While pulling the line low, the NCP will hold in a reset state. Upon returning the line high, on the rising edge of the signal, the part will restart operation. Silicon Labs NCP chips include an internal pull-up resistor on this input so adding one is not necessary.

The Host must be able to reset the NCP to run the EZSP protocol. This can normally be accomplished utilizing software reset frames sent via EZSP from the Host to the NCP. However, in cases where the NCP fails to respond to EZSP frames, this hardware backup can be utilized.

While this interface is optional for NCP-to-Host communications, Silicon Labs recommends including nRESET in all Host-NCP hardware designs as a backup for situations where continued NCP operation is impossible or where unforeseen NCP operation blocks the Host.

For secure designs (utilizing secure EZSP) or security products, these connections should be considered mandatory.

2.4 Recover / Bootload: Bootload

The Bootload line allows the Host to force an NCP into bootloader mode during a reset or power cycle. For normal operation, the Bootload line should be held high. During a reset (while the nRESET line is held low) or a power cycle, the Bootload line should be pulled low. Upon release of the nRESET line or powering up the NCP, the low input on the Bootload pin will signal the bootloader software (Gecko or legacy) to override normal NCP operation, allowing the Host to update the firmware of the NCP. Because the Bootload pin can be configured on any input, a pull-up resistor should be placed on this input or set internally.

Bootloading is normally accomplished utilizing software bootloader frames sent via EZSP from the Host to the NCP. However, in cases where the NCP fails to respond to EZSP frames, this hardware backup, in conjunction with nRESET, can be utilized.

While this interface is optional for NCP-to-Host communications Silicon Labs recommends including the Bootload pin in all Host-NCP hardware designs as a backup for situations where unforeseen operation or corruption block the NCP from responding to any software commands from the Host.

For secure designs (utilizing secure EZSP) or security products, these connections should be considered mandatory.

2.5 Pin Connections

The following table lists the pin connections.

Table 2.1. Pin Connections

| Pin number | Description |
|------------|----------------|
| Tx | Output |
| Rx | Input |
| RTS | Input |
| CTS | Output |
| nRESET | Input |
| Bootload | Input, Pull-up |

3. Command Line Options for Host Applications

To test your Host-NCP interface Silicon Labs recommends that you build a Host application using AppBuilder. (If necessary, refer to *QSG106: Getting Started with EmberZNet PRO* for additional help.) <Z3GatewayHost> is the generic name for a Host application.

To build your application, follow these steps:

1. Launch Simplicity Studio.
2. Change your perspective to the Simplicity IDE perspective.
3. Create a new AppBuilder Host project:
 - a. Select **File > New > Project...**
 - b. Select **Silicon Labs AppBuilder Project** and click **Next>**.
 - i. Select **Silicon Labs Zigbee** and click **Next>**.
 - ii. Select **EmberZNet <version> Host** and click **Next>**.
 - iii. Select the **Z3 Gateway** application and click **Next>**.
 - iv. Enter a name for your project and click **Next>**.
 - v. On the Project setup page, leave the board section blank. For the part make, sure **None** is selected. The toolchain should also reflect no toolchain as well (or **None**).
 - vi. Click **Finish**.
4. Simplicity Studio will now be displaying your Z3 Gateway ISC project file. The default settings are enough to test your EZSP settings. Select **Generate**. This will create the files for your project. The project is a POSIX-compliant Make project. You can transfer your project to your platform and build it using a standard `make` command.
5. Once your project is built, you can run it and use the command line options to test your interface. As long as your application properly interfaces the NCP and properly executes, you can be assured that your connections are working properly. You should see a message similar to this one:

```
./Z3GatewayHost -n 0 -p /dev/ttyAMA0
Reset info: 11 (SOFTWARE)
ezsp ver 0x06 stack type 0x02 stack ver. [6.3.1 GA build 245]
Ezsp Config: set source route table size to 0x0064:Success: set
```

The following table summarizes the <Z3GatewayHost> command line options.

Table 3.1. <Z3GatewayHost> Command Line Options

| Command Line Option | Optional values | Description |
|---------------------|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -n | 0, 1 | 0=115200 bps (RTS/CTS), 1= 57600 bps (XON/XOFF) |
| -b | <baud rate> | Baud Rate: 9600, 19200, 38400, 57600, 115200, etc. |
| -f | r, x | Flow control: r=RST/CTS, x=XON/XOFF |
| -h | | Display usage information. |
| -i | 0, 1 | Enable/disable input buffering. |
| -o | 0, 1 | Enable/disable output buffering. |
| -p | <port name> | Serial port name or number (for example, COM1, ttyS0, or 1) |
| -r | d, r, c | NCP reset method: d=DTR, r=RST frame, c=custom |
| -s | 1, 2 | Stop bits |
| -t | <trace flags> | Trace B0=frames, B1=verbose frames, B2=events, B3=EZSP |
| -v | [base port] | Enables virtual ISA support. The [base-port] argument is optional. Both serial ports are available via telnet instead of local console. The RAW serial port is available on the first port (offset 0 from base port) and CLI is available on the second port (offset 1 from base port). By default, 4900 is the base port, therefore RAW access is available from port 4900 and CLI access is available on port 4901. |

| Command Line Option | Optional values | Description |
|---------------------|-----------------|------------------------------------|
| -x | 0 , 1 | Enable/disable data randomization. |

4. Design Considerations for Host and NCP Communications

Silicon Labs recommends these best practices for Host and NCP communications:

- Use a well-tuned crystal (38.4 MHz) for any wireless mesh application.
- Use of RTS/CTS hardware flow control is highly recommended. It will aid in electrically-noisy environments.
- UART-based NCP is not suitable for low-power designs due to the inability of the NCP to enter into any sleep modes. In designs where low power NCPs are required, Silicon Labs recommends using SPI-NCP instead. (For more information, refer to *AN711: SPI Host Interfacing Guide for Zigbee*.)
- Silicon Labs recommends including the nRESET and Bootload pins in all Host-NCP hardware designs as a backup for situations where serial communication are lost between the Host and NCP. For secure designs (utilizing secure EZSP) or security products, these connections should be considered mandatory.

5. Powering On, Power Cycling, and Rebooting

When the Host powers on or reboots, it cannot guarantee that the NCP is ready to receive commands. Therefore, the Host should always perform a reset of the NCP to place it into a known state. It is far simpler to reset the NCP and begin from a known state than to try to recover and resync with the previous (unknown) state of the NCP. This reset can be performed either via an ASH RST frame or toggling the nRESET line (if it is enabled). By guaranteeing that the NCP is freshly booted just like the Host, the Host can proceed with standard node and network initialization instead of consuming extra code space just trying to determine what state the NCP was left in.

When the NCP resets, it will issue an RSTACK frame to alert the Host it has reset, which includes the reset type as defined by `platform/base/hal/micro/generic/em2xx-reset-defs.h`. Once the RSTACK frame is received, the Host will know the NCP is in a known state to start operation.

6. Bootloading

The NCP can enter bootload mode through either a software command or a hardware toggle.

6.1 Software Bootloading

When operating in EZSP mode, issuing the bootloader frame `launchStandaloneBootloader` will cause the NCP to enter into the bootloader. This can be used at any time when the Host wants to restart the NCP in the bootloader.

6.2 Hardware Bootloading

Asserting the bootloader pin (low) while powering up or resetting the NCP will cause the chip to enter the bootloader instead of resuming normal NCP operation. In both the Gecko Bootloader and the legacy Ember bootloaders, a recovery pin can be defined in the board configuration to initiate bootloader mode. It can be defined to be any valid GPIO pin. The pin definition method depends on the bootloader used:

- Gecko Bootloader: Through `BTL_BUTTON` settings using the Gecko Bootloader's "GPIO Activation" plugin
- Legacy Ember Bootloader: Through `BUTTON_RECOVERY_PORT_PIN` in the legacy bootloader's `bootloader-gpio.c` file

An example of performing this reset would be as follows:

1. Assert `nRESET` to hold the NCP in reset.
2. While `nRESET` is asserted, assert `BOOTLOAD`, and then deassert `nRESET` to boot the NCP.
3. The `BOOTLOAD` line can be deasserted once the reset line has been deasserted.

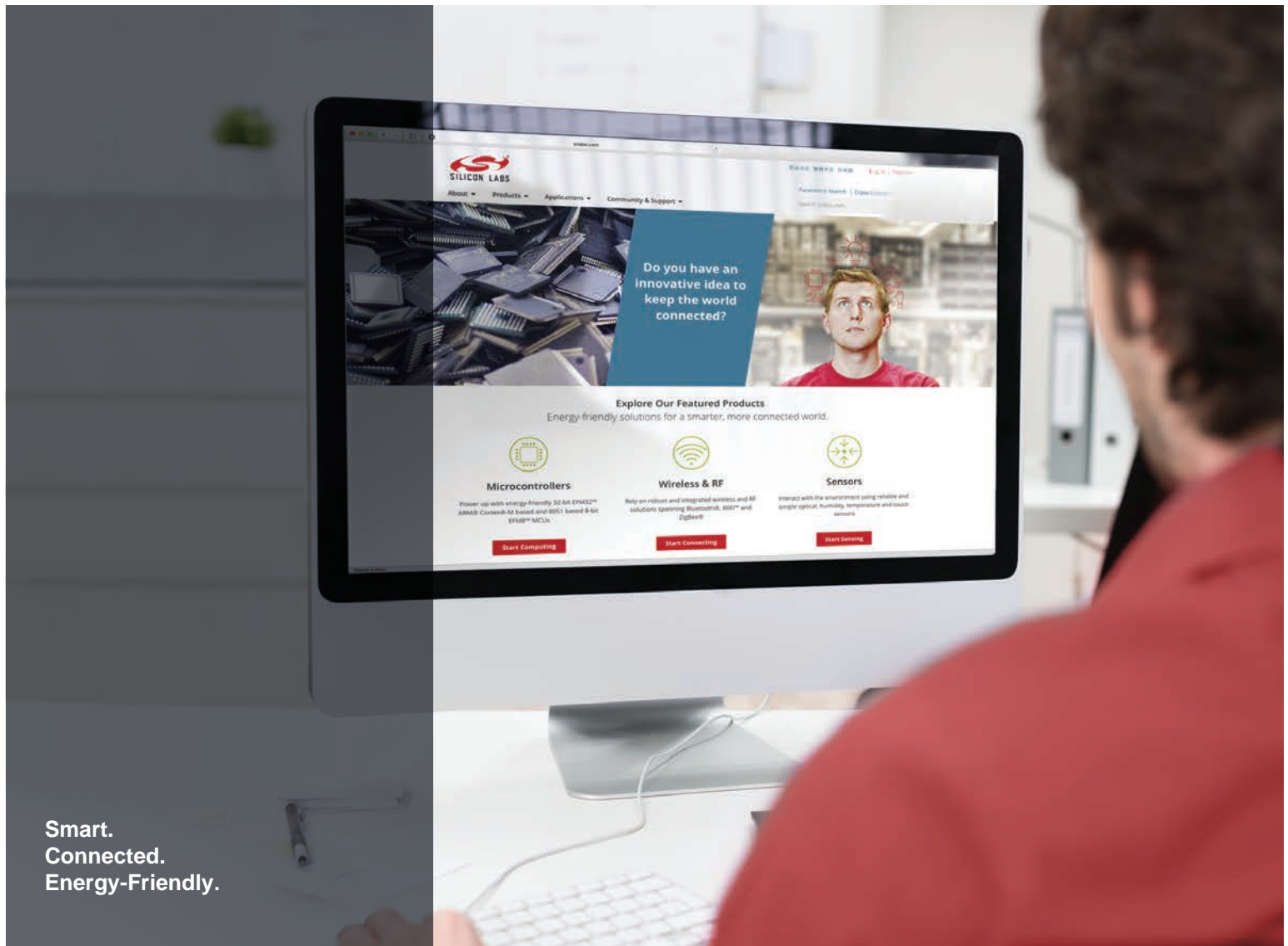
6.3 Bootloader Operation

The target device's bootloader sends output over its serial port after it receives a carriage return from the source device at the expected baud rate. This prevents the bootloader from prematurely sending commands that might be misinterpreted by other devices that are connected to the serial port. Note that serial bootloaders typically do not enforce any timeout when awaiting the initial serial handshake via carriage return, so the bootloader will wait indefinitely in this mode until guided by the source device or until the chip is reset.

After the bootloader receives a carriage return from the target device, it displays a menu with the following ASCII-based output (where `X.Y.A` corresponds to the major, minor, and sub-minor fields of the bootloader version number, respectively).

```
Gecko Bootloader vX.Y.A
1. upload gbl
2. Run
3. ebl info
BL >
```

Once this is received, the Host can be assured that the NCP is operating in bootloader mode.



Smart.
Connected.
Energy-Friendly.



Products

www.silabs.com/products



Quality

www.silabs.com/quality



Support and Community

community.silabs.com

Disclaimer

Silicon Labs intends to provide customers with the latest, accurate, and in-depth documentation of all peripherals and modules available for system and software implementers using or intending to use the Silicon Labs products. Characterization data, available modules and peripherals, memory sizes and memory addresses refer to each specific device, and "Typical" parameters provided can and do vary in different applications. Application examples described herein are for illustrative purposes only. Silicon Labs reserves the right to make changes without further notice to the product information, specifications, and descriptions herein, and does not give warranties as to the accuracy or completeness of the included information. Without prior notification, Silicon Labs may update product firmware during the manufacturing process for security or reliability reasons. Such changes will not alter the specifications or the performance of the product. Silicon Labs shall have no liability for the consequences of use of the information supplied in this document. This document does not imply or expressly grant any license to design or fabricate any integrated circuits. The products are not designed or authorized to be used within any FDA Class III devices, applications for which FDA premarket approval is required or Life Support Systems without the specific written consent of Silicon Labs. A "Life Support System" is any product or system intended to support or sustain life and/or health, which, if it fails, can be reasonably expected to result in significant personal injury or death. Silicon Labs products are not designed or authorized for military applications. Silicon Labs products shall under no circumstances be used in weapons of mass destruction including (but not limited to) nuclear, biological or chemical weapons, or missiles capable of delivering such weapons. Silicon Labs disclaims all express and implied warranties and shall not be responsible or liable for any injuries or damages related to use of a Silicon Labs product in such unauthorized applications.

Trademark Information

Silicon Laboratories Inc.®, Silicon Laboratories®, Silicon Labs®, SiLabs® and the Silicon Labs logo®, Bluegiga®, Bluegiga Logo®, Clockbuilder®, CMEMS®, DSPLL®, EFM®, EFM32®, EFR®, Ember®, Energy Micro logo and combinations thereof, "the world's most energy friendly microcontrollers", Ember®, EZLink®, EZRadio®, EZRadioPRO®, Gecko®, Gecko OS, Gecko OS Studio, ISOmodem®, Precision32®, ProSLIC®, Simplicity Studio®, SiPHY®, Telegesis, the Telegesis Logo®, USBXpress®, Zentri, the Zentri logo and Zentri DMS, Z-Wave®, and others are trademarks or registered trademarks of Silicon Labs. ARM, CORTEX, Cortex-M3 and THUMB are trademarks or registered trademarks of ARM Holdings. Keil is a registered trademark of ARM Limited. Wi-Fi is a registered trademark of the Wi-Fi Alliance. All other products or brand names mentioned herein are trademarks of their respective holders.



Silicon Laboratories Inc.
400 West Cesar Chavez
Austin, TX 78701
USA

<http://www.silabs.com>