SNIB2 Firmware Version 6.42 Release Notes

Overview

This document describes the changes in the SNIB2 firmware since version 5.99. For details, see the tables of New Features and Enhancements and Bug Fixes.

NOTE: There are no known limitations in this release. However, it does require CCM/CCMx firmware version 7.5.08 (or later).

CAUTION: To maintain the configuration settings of your SNIB2 board, its firmware must be at version 5.99 before you upgrade it to version 6.42.

After downloading this firmware file, follow these instructions.

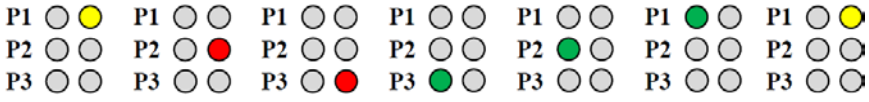
1. If you are using version 3.1 of the Hirsch Velocity software: Choose the **File > Import/Export** command, then click **SNIB2 (Import Only)**.

   If you are using version 3.5 of the Hirsch Velocity software: Click on Velocity's menu button (in the upper left corner of Velocity's main window), then choose **Data Exchange > SNIB2 Import**.

   The SNIB2 Import Wizard is displayed.
2. In the resulting SNIB2 Import Wizard, follow the onscreen instructions to import the update.
3. In Velocity's Administration window, right-click on a controller whose SNIB2 firmware needs to be updated, and select **Properties** from the pop-up menu.
4. On the General tab of the controller's Properties dialog, click **Update SNIB2 Firmware** and follow the instructions.
5. Repeat steps 3 and 4 for each controller whose SNIB2 firmware needs to be updated.

For complete instructions on updating the SNIB2, refer to the **Firmware Updates > Updating SNIB2 Firmware** topic in the main Velocity Help.

New Features and Enhancements

Reference ID	Feature	Description
SNIBII-21	SNIB2 board can be reset to factory defaults (using its DIP switches)	A SNIB2 board can be reset to the factory default values for its encryption keys and network settings. To reset a SNIB2 board to have an IP address based on its unique MAC address, perform the following steps: 1. Set all four DIP switches in Switch Bank 2 to ON, and set all eight DIP switches in Switch Bank 3 to OFF. 2. Cycle power to the controller containing this SNIB2 board. 3. Watch the status LEDs on the SNIB2 board, to ensure that they display the Lamp Test start up pattern, and then display the following SNIB2/CCM Synchronization pattern:  4. Turn off power to the controller. You can then reconfigure the SNIB2 board as needed, using its DIP switches and Velocity.

Bug Fixes

Reference ID	Bug	Description
SNIBII-3	SNIB2 random dropped connections	There was a known issue with dropped connections in the third-party firmware for the Ethernet daughterboard on the SNIB2. This issue has been fixed.
SNIBII-4	SNIB2 has an invalid IP Port 0	Version 5.98 of the SNIB2 firmware had an active port 0, which is an invalid port. This issue has been fixed, so any connections on port 0 are refused.
SNIBII-6	SNIB2 will stop communicating when DIP switch 1 on Switch Bank 2 is toggled	The SNIB2 board would stop communicating when DIP switch 1 on Switch Bank 2 was toggled. (To workaround this issue, you had to cycle power on the controller.) This issue has been fixed.
SNIBII-9	SNIB2, Controller locked up will not generate Off-line alarm	When a controller connected via SNIB2 locked up, Velocity did not receive a controller off-line alarm. This issue has been fixed, by adding a “watchdog” to the SNIB2 firmware that recognizes when its controller has stopped communicating with the Velocity server. **NOTE:** This bug fix requires version 7.5.08 (or later) of the CCM/CCMx firmware.
SNIBII-17	Restarting a SNIB2 controller causes other SNIB2 controllers to drop offline and then come back online	A customer with multiple Velocity systems on the same network found that restarting a controller could cause other controllers to briefly drop offline. This issue was caused by a bug in the third-party firmware for the Ethernet daughterboard on the SNIB2, where a UDP packet was breaking the TCP socket. This issue has been fixed by shutting down the UDP socket after Velocity establishes the TCP socket, and reopening the UDP socket only if the TCP socket is closed or broken.

Recommended Practices

- We do not recommend stopping and starting the DIGI*TRAC Network Service during peak traffic times. After restarting this service, as each controller is recognized and logged on to the Velocity Server, the system attempts to catch up on all of the events that occurred, before bringing the next controller online. In a system with many controllers, it can take much longer for them all to come online during peak traffic times (compared to an off-peak time).
- Large installations should reset the default value of the SNet host timeout (located in the Communications tab of the Controller Properties window in Velocity) from the default value of 10 seconds to a number higher than the number of controllers on the loop.
- If you need to cross a router, all master SNIB2 boards must be configured with a Default Gateway and a Subnet Mask (in addition to an IP Address). (If you don’t know this information, obtain it from your network administrator.)
- All controllers should be at version 7.5.08 (or later) of the CCM/CCMx firmware, and your Velocity software should be at either version 3.1 KB640 or 3.5 SP1 (or later).