SNIB2 Firmware Version 6.52 Release Notes

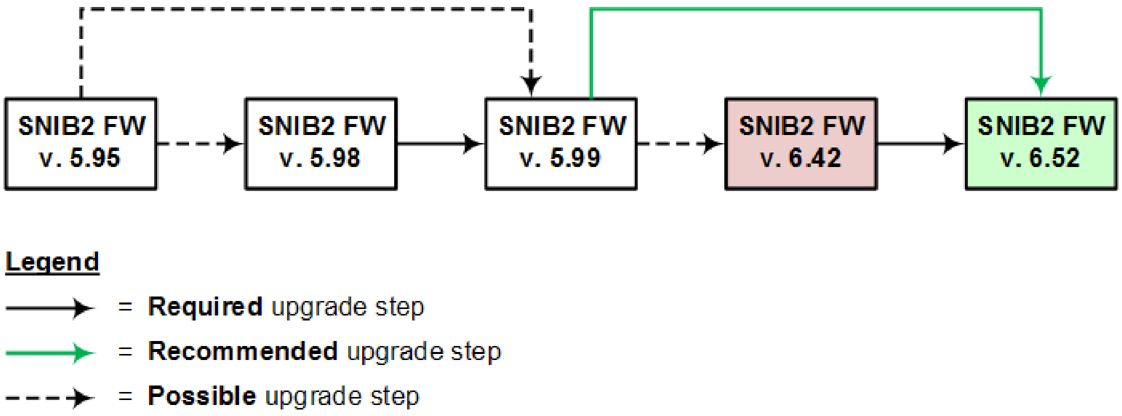
Overview

This document describes the changes in the SNIB2 firmware since version 6.42. For details, see the table of Bug Fixes.

This release does **not** require a new version of the CCM/CCMx firmware; you can continue using your currently installed version.

CAUTION: To maintain the network configuration settings of your SNIB2 board, its SNIB2 firmware must be at version 5.99 before you upgrade it to version 6.42 or 6.52.

Upgrade Paths to SNIB2 Firmware version 6.52:



UPGRADE NOTE: If a SNIB2 is running firmware version 6.42, then upgrading to version 6.52 will cause the encryption keys to reset to their default value.

- For a port which has only one controller (with a SNIB2), you don't need to manually reset encryption by flipping DIP switches; after upgrading, just open the **Port Properties** dialog for that SNIB2, check the option to **Reset encryption**, and click **OK**.
- If you have a port where a chain of controllers with SNIB2s are connected using RS-485 wiring, you can avoid having to manually reset encryption by flipping DIP switches on the SNIB2 of each downstream controller, if you perform these steps:
  1. Upgrade the SNIB2 firmware on each downstream controller, starting with the one at the end of the chain, and then working back towards the master.
  2. Upgrade the SNIB2 firmware on the master controller of the chain.
  3. Open the **Port Properties** dialog for the master SNIB2, check the option to **Reset encryption**, and click **OK**.

  This should reset the encryption between the Velocity server and the master SNIB2, then the master SNIB2 will reset the encryption for its downstream SNIB2s, and all the controllers should come back online.

After downloading the SNIB2 firmware file, follow these general instructions.

1. Click on Velocity's menu button (in the upper left corner of Velocity's main window), then choose **Data Exchange > SNIB2 Import**.
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 firmware, refer to the **Firmware Updates > Updating SNIB2 Firmware** topic in the main Velocity Help.

Bug Fixes

Reference ID	Bug	Description
DT-176	Credential downloads sometime hang waiting for a “command complete” message from a downstream controller	Batches of credential downloads could hang in the Download Monitor because the Velocity Spooler was waiting for a “command complete” message (for certain variations of CMD 23) from a downstream controller. This issue has been fixed. **Note that the behavior in the Velocity Download Monitor may change**. Specifically, it may appear that some batches stop for a minute or so while other batches to the same port keep going. *This is expected behavior*. The SNIB2 now has a mechanism where it won't send more commands that it has received to the downstream subordinate controllers while its upstream message queue is full. If you see this happening, it means the mechanism is working, and making sure that Velocity doesn't miss any of the messages coming from any of the controllers.
DT-224	Credential downloads sometime hang waiting for a “command complete” message	Batches of credential downloads could hang in the Download Monitor because the Velocity Spooler was waiting for a “command complete” message (for CMD 16). This issue has been fixed.
SNIBII-17	Restarting a SNIB2 controller could cause 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 which included a SNIB2 communications expansion board could cause other controllers with a SNIB3 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.
SNIBII-28	Batches can hang when downloading credentials to a downstream controller, if the controller goes offline during the download	If a downstream controller goes offline during a **credential** download, the batch could hang even after that controller comes back online. This happens because the Velocity Spooler is confused by malformed X message 6 messages which contain invalid data. (This was not an issue when downloading **controller configurations**.) This issue has been fixed.
SNIBII-32	In version 6.42 of the SNIB2 firmware, if the network connection is lost, the controller must be restarted to bring the SNIB2 back online	On a controller which includes a SNIB2 communications expansion board that is running version 6.42 of the SNIB2 firmware, if the network connection is lost, the controller must be restarted to bring the SNIB2 back online. This issue was an unexpected side effect of upgrading to Dynamic C libraries version 9.62b, and has been fixed by reverting to version 8.61.

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 (with more than 10 controllers) should change the value of the **SNet timeout** option (located on the **Communications** page of the **Controller Properties** dialog in Velocity) from the default value of 10 seconds to a number greater than the number of controllers on the loop.

- If you need to cross a router, all master SNIB2 boards must be configured with a **Subnet Mask** and a **Default Gateway** (in addition to an **IP Address**). (If you don’t know this information, obtain it from your network administrator.)

- All controllers should be at the same version of the CCM/CCMx firmware, and your Velocity software should be at a supported version (currently 3.5 or later).