



Replace Cisco NCS 1002 Components

This chapter describes the procedures to replace Cisco NCS 1002 components.

- [Remove and Reinsert Control Card, on page 1](#)
- [Remove Fans, on page 3](#)
- [Remove and Replace SSD, on page 4](#)
- [Replace Power Supply, on page 5](#)
- [Wipe Data in Disk Using Secure Erase, on page 6](#)

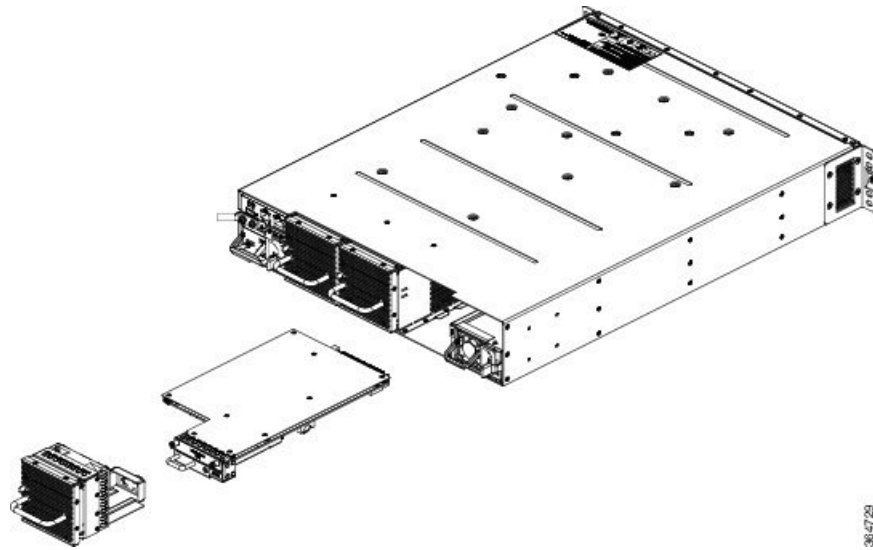
Remove and Reinsert Control Card

Cisco NCS 1002 can carry traffic with a non-functional control card (headless mode) for up to 72 hours. In case of card failure, the failed control card needs to be physically replaced within 10 minutes.

Procedure

- Step 1** Remove control card.
- a) Remove the fan on the right back side (Fan 0).
 - b) Loosen the captive screw to unlock the ejector lever.
 - c) Pull the handle to remove the control card.

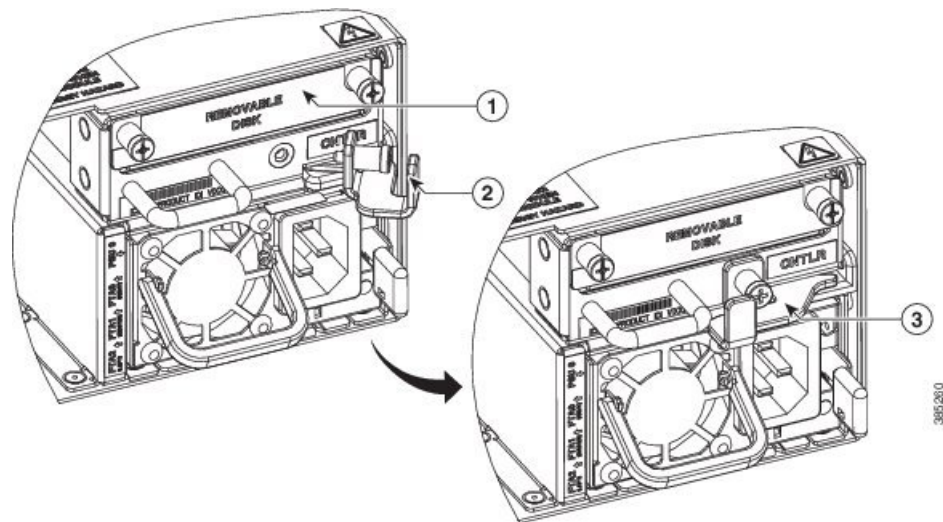
Figure 1: Remove Control Card

**Step 2**

Reinsert and lock control card.

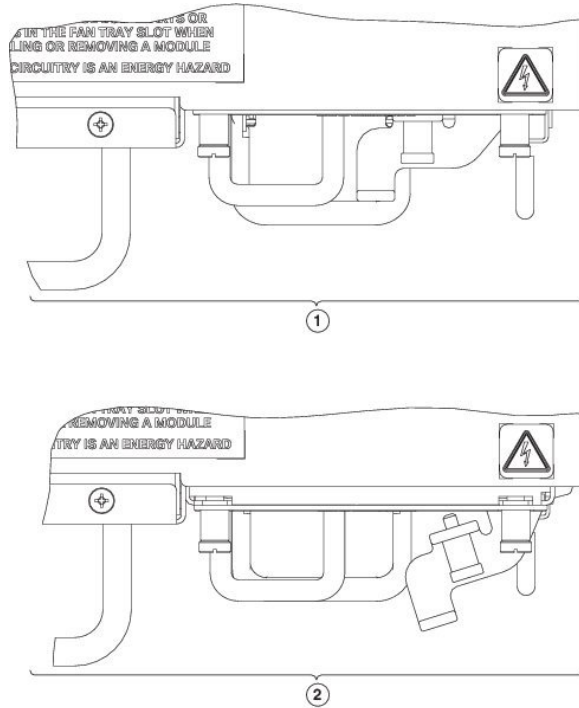
- a) Insert the control card in the NCS 1002 box guides.
- b) Slide the control card while keeping the ejector open until the faceplate is close to the box and the ejector is engaged.
- c) Press the ejector to insert the control card partially.
- d) Apply pressure on the control card faceplate to complete the insertion.
- e) Ensure that the control card faceplate is aligned to the top cover edge of NCS 1002.
- f) Verify that the position of the ejector is final.
- g) Fix the screw to lock the ejector.

Figure 2: Insert and Lock Control Card



1	Push this surface area with additional force needed to engage control card
2	Rotate and push ejector lever to engage control card to the connector
3	Lock ejector lever to secure control card

Figure 3: Verify Control Card Insertion



1	The control card is properly seated.
2	The control card is not properly seated.

- Verify that the faceplate of the control card is aligned with the top cover of the box.
- Verify that there is no gap between the ejector and the faceplate of the control card.

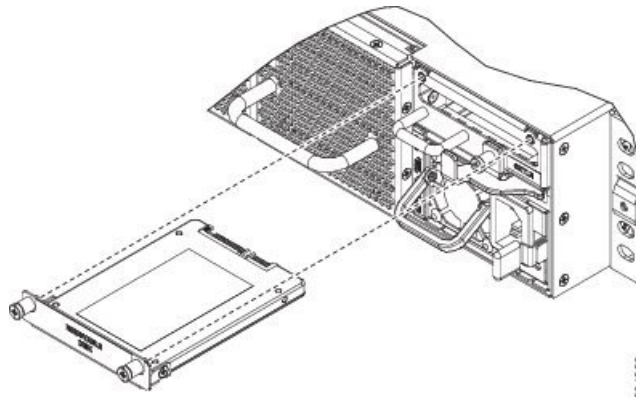
Step 3 Re-insert the fan on the right back side (Fan 0).

For information on CPU OIR LEDs, refer [LEDs in Cisco NCS 1002](#).

Remove Fans

Cisco NCS 1002 has fan redundancy protection mechanism against a single fan failure. If a fan fails, NCS 1002 can work for unlimited time without any performance degrade. When the failed fan is replaced, the new fan needs to be physically placed within 10 minutes.

Figure 5: Remove SSD



To replace a SSD:

- Step 3** Slide the SSD into the Removable Disk slot.
 - Step 4** Tighten the two captive screws to secure the SSD into place.
-

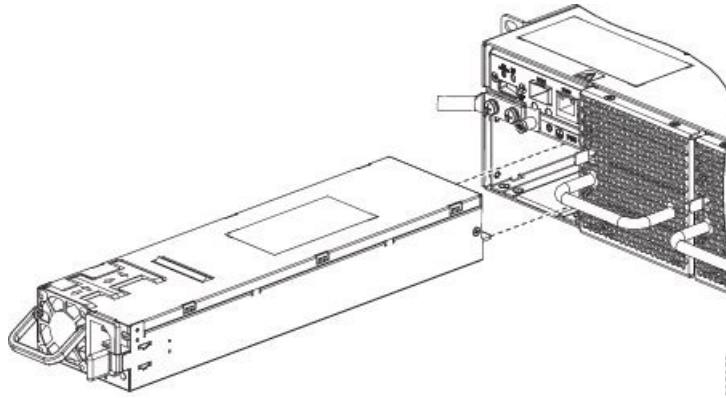
Replace Power Supply

Use this procedure to replace both the AC and DC power supply units.

Procedure

- Step 1** Open the breaker powering the PSU under replacement.
- Step 2** Remove the PSU cable.
- Step 3** Pull the handle acting on the PSU latch to remove the PSU.
- Step 4** Insert the new PSU and connect the PSU cable. See [Connect AC Power to NCS 1002](#) and [Connect DC Power to NCS 1002](#).
- Step 5** Close the breaker powering the replaced PSU.

Figure 6: Remove Power Supply



Wipe Data in Disk Using Secure Erase

When NCS 1002 becomes faulty, contact TAC to open a Return Material Authorization (RMA) request. Before opening a RMA request, the user can securely wipe data in NCS 1002 disks using the Secure Erase feature. The Secure Erase feature is supported from BIOS version v13.10.



Warning Use this procedure only during RMA.

Before you begin

The NCS 1002 unit that is planned for RMA must be taken out of the data center and the network. The user must access NCS 1002 only using the console port.

Procedure

Step 1 When NCS 1002 boots (power cycle), the following message appears.

```
Version 2.17.1245. Copyright (C) 2016 American Megatrends, Inc.
BIOS Date: 03/22/2016 11:19:42 Ver: 0ACBZ1310
Press <DEL> or <ESC> to enter setup.
```

Press DEL or ESC key to enter BIOS.

Step 2 Select the **Security** tab using the arrow keys.

The disk security details such as setting Hard Disk Drive (HDD) password and erasing HDD are displayed in the Security tab.

Step 3 Select **Set HDD Password** to set the new HDD password.

The HDD password can contain only ASCII characters and is not case sensitive. The HDD password needs to be provided after power reset and the password can be set or changed after power reset. The disk security is enabled after setting the HDD password.

Warning When HDD password is set, the user must remember the password. If the password is lost, the data in HDD cannot be recovered.

Warning When HDD password is set, BIOS prompts for HDD password to unlock the HDD after each power reset.

Step 4 Select **Erase HDD** using the arrow keys.

The Erase HDD screen appears.

Step 5 Enter the HDD password in the Erase HDD field.

Step 6 Select **OK** in the Erase Confirmation screen that indicates the data in the disk has been securely wiped.

The disk security settings are reverted to factory defaults after the secure erase. The configured HDD password is also wiped.
