Migrate from Cisco IOS XR to SONiC Software

Table 1: Feature History Table

Feature Name	Release Information	Description
Securely migrate from Cisco IOS XR to SONiC software through extended device ownership	Release 7.10.1	Configure the modular chassis with extended ownership to securely migrate the operating system from Cisco IOS XR to SONiC image. Only the signed-SONiC image that is authorized by Cisco using ownership voucher (OV) and authentication variables (AV) is allowed to be installed on the router. This authorization prevents tampering the software with unauthorized third-party images.

This section describes the process involved in configuring extended ownership and securely migrating to SONiC software on Cisco 8000 series routers with modular chassis. The router supports installation of only the signed SONiC image that is authorized by Cisco using ownership voucher (OV) and authentication variables (AV).

SONiC can be installed on the following closed product ID (PID) modular-form factors of Cisco 8000 series routers:

Product ID (PID)	Description
88-LC0-36FH-M	Cisco 8800 36x400 GbE QSFP56-DD Line Card with MACsec based on Q200 Silicon
88-LC0-36FH	Cisco 8800 36x400 GbE QSFP56-DD Line Card based on Q200 Silicon
8800-RP	Cisco 8800 Route Processor (also known as Supervisor)
8800-LC-48H	Cisco 8800 48x100 GbE QSFP28 Line Card based on Q100 Silicon

Prepare the Router for Software Migration

In this section, you prepare the router for migration from Cisco IOS XR software to SONiC software.

Step 1 Configure the Management interface.

Example:

```
Router#conf t
Router(config)#interface mgmtEth 0/RP0/CPU0/0
Router(config-if)#ipv4 address 192.0.2.0/241.66.13.141/16
Router(config-if)#no shut
Router(config-if)#commit
```

Step 2 Configure the SSH server.

Example:

```
Router(config)#ssh server
Router(config)#commit
Router(config)#end
```

Step 3 Ensure peer RP is not configured on the router.

Step 4 Copy the following files from the Github repository to the router. In this example, the images are copied from the repository with address 192.0.2.0 to the harddisk: directory on the router.

Example:

```
sonic@host:~$scp sonic-migutil.py cisco@192.0.2.0:/harddisk:/
sonic@host:~$scp sonic-cisco-8000.bin cisco@192.0.2.0:/harddisk:/onie-installer.bin
sonic@host:~$scp onie-recovery-x86_64-cisco_8000-r0.efi64.pxe
cisco@192.0.2.0:/harddisk:/onie-recovery-x86_64-cisco_8000-r0.efi64.pxe
```

Step 5 Identify one of the working LC as staged LC with address 172.0.<slot>.1, where <*slot*> is the LC number. Copy the following files from RP to staged LC.

Example:

```
Router#run scp /tmp/sonic-migutil.py root@172.0.0.1:/harddisk:/
Router#run scp /harddisk:/onie-recovery-x86_64-cisco_8000-r0.efi64.pxe root@172.0.0.1:/www/pages
Router#run scp /harddisk:/onie-installer.bin root@172.0.0.1:/www/pages/onie-installer.bin
```

With this, the router is prepared to be migrated from Cisco IOS XR to SONiC software.

Configure Extended Ownership

Table 2: Feature History Table

Feature Name	Release Information	Description
Securely transfer device ownership	Release 7.10.1	Establish extended device ownership to allow transfer of device control between Cisco and the customer. With this feature, you can install only the customer-signed images that are authorized by Cisco using an ownership voucher (OV) and an authentication variables (AV).

This section provides information about configuring extended ownership on the router via Ownership Voucher (OV). The OV contains an authentication variable (AV) that moves the state of Cisco Trusted Platform Module (TPM) and platform keys to allow customized control on the router. With this voucher, you can securely transfer the control of the UEFI database ownership from Cisco generic mode to an extended mode, owned by both Cisco and the Customer.

Use the following instructions to enable extended ownership on the router:

Before you begin

Verify that the device ownership is in Cisco generic mode.

```
Router#show platform security boot mode location <device-location>
```

The following example shows the mode of all devices on the router.

```
Router#show platform security boot mode location all
Tue Feb 21 16:40:16.207 UTC
Performing operation on all nodes...
=========================
Location  :  0/RP0/CPU0
=========================
Aikido mode: Generic Mode
Aikido mode value: 43

=========================
Location  :  0/1/CPU0
=========================
Aikido mode: Generic Mode
Aikido mode value: 43
```

The `Aikido mode: Generic Mode` in the output indicates that the router is controlled by the Cisco mode. Proceed to step 3 to download the voucher and configure extended ownership on the router.

Note If the output displays `Aikido mode: Customer Mode`, proceed to provision the customer keys in the database. This indicates that the extended voucher is already applied and the device is in the Customer mode. See, Provision Customer Keys in Database, on page 6.

If the output displays `Aikido Mode: Setup Mode`, the device is not upgraded with supported image. Check the software version, upgrade FPDs, BIOS and TAM as described in step 1. After the upgrade, the mode changes to `Aikido mode: Generic Mode`.

Step 1 Download the ownership voucher to the router.

a) Access the Github repository. Identify the specific serial number of interest. Download the voucher to a remote server. The voucher is available for download as a .vcj file. For example, `DCA213140YX.vcj`. You can download more than one vouchers for the respective serial numbers based on the requirement.

Note You can submit a request to generate OV for a new serial number that is not published in the Github repository. For more information, see .

b) Convert the .vcj file into .tar file. This is applicable for single or multiple .vcj files.

c) Copy the voucher in .tar format to the router.

Example:

```
Router#scp <user>@<ip_address>:<directory>/<filename> /harddisk:
```

For example, the vouchers are converted into a `sampleOV.tar` file and copied to the harddisk on the router from the server with address `10.0.0.1`.

```
Router#scp cisco@10.0.0.1:/ws/sampleOV.tar /harddisk:
```

Step 2 Apply the voucher on the device to enable the extended ownership.

Example:

```
Router#platform security device-ownership <path-to-OV-file> location <device-location>
```

If you are applying a .tar file with one .vcj voucher, apply the file to the single device location based on the serial number. If you are applying multiple .tar files, zip all the .tar files into a single file and apply the file to the devices using **location all** keyword.

In this example, the vouchers for line card (LC) and route processor (RP) are zipped into a `multiple-ov.tar.gz` file, and saved under the harddisk of the router. Use the **location all** keywords to apply the voucher to both LC and RP.

```
Router#platform security device-ownership /harddisk:/multiple-ov.tar.gz location all
Thu Feb 23 16:42:19.207 UTC
Successfully applied ownership voucher in node0_RP0_CPU0.
Successfully applied ownership voucher in node0_1_CPU0
Power-cycle of the node is required for the dual ownership transfer to take affect.
```

Attention An error messgae is displayed if the ownership voucher is not applied. The possible causes for failure can be due to an invalid AV, expired or unrecognized OV and so on. Contact Cisco with the debug logs to resolve the error.

Step 3 Power cycle the device.

Example:

```
Router#reload location all
```

Wait for the reload operation to complete.

Step 4 Verify that the nodes are operational.

Example:

```
Router#show platform
Thu Feb 23 03:53:24.923 UTC
Node         Type                State          Config state
--------------------------------------------------------------------
0/RP0/CPU0   8800-RP(Active)     IOS XR RUN     NSHUT
0/0/CPU0     88-LC0-36FH         IOS XR RUN     NSHUT
0/1/CPU0     8800-LC-48H         IOS XR RUN     NSHUT
0/5/CPU0     88-LC0-36FH-M       IOS XR RUN     NSHUT
0/FC0        8808-FC0            OPERATIONAL    NSHUT
```

Step 5 Verify that the device ownership is in Customer mode

Example:

```
Router#show platform security boot mode location <device-location>
```

The following example shows the mode of all devices on the router.

```
Router#show platform security boot mode location all
Thu Feb 23 16:47:19.207 UTC
Performing operation on all nodes..
==============================
Location  :  0/RP0/CPU0
==============================
Aikido mode: Customer Mode
Aikido mode value: 127

==============================
Location  :  0/1/CPU0
==============================
Aikido mode: Customer Mode
Aikido mode value: 127
```

The `Aikido mode: Customer Mode` in the output indicates the change in ownership from Cisco to customer dB mode is sucessful.

Step 6 Verify that the platform key certificate is active and registered successfully.

Example:

```
Router#show platform security variable customer PKCustomer location <device-location>
```

The following example shows the PKCustomer security keys of all devices on the router.

```
Router#show platform security variable customer PKCustomer location all
Thu Feb 23 04:05:22.628 UTC
Performing operation on all nodes..
=========================
Location : 0/RP0/CPU0
=========================
Variable : PKCustomer
+--------------------
Signature List # 0
GUID : f79d17d1-88d4-40dd-aff8-9f9da3c30e9e
Extension type : X509

Entry # 0
Owner GUID : 7dc87112-2bd5-4154-950a-ce3183107619
Size : 1066
```

```
Serial Number : ED:88:CD:A6:35:C2:59:B4
Subject:
O=Cisco,OU=RELEASE,CN=IOSXR-WHITEBOX-PK
Issued By :
O=Cisco,OU=RELEASE,CN=IOSXR-WHITEBOX-PK
Validity Start : 06:18:18 UTC Thu Jan 27 2022
Validity End : 06:18:18 UTC Wed Jan 22 2042
SHA1 Fingerprint:
ECA9C7F3872B842336BA39D8B73E43FFD843FCA5

Total Signature Lists # 1
Total Certificates # 1


=========================
Location : 0/1/CPU0
=========================
Variable : PKCustomer
+--------------------

Signature List # 0
GUID : f79d17d1-88d4-40dd-aff8-9f9da3c30e9e
Extension type : X509

Entry # 0
Owner GUID : 7dc87112-2bd5-4154-950a-ce3183107619
Size : 1066

Serial Number : ED:88:CD:A6:35:C2:59:B4
Subject:
O=Cisco,OU=RELEASE,CN=IOSXR-WHITEBOX-PK
Issued By :
O=Cisco,OU=RELEASE,CN=IOSXR-WHITEBOX-PK
Validity Start : 06:18:18 UTC Thu Jan 27 2022
Validity End : 06:18:18 UTC Wed Jan 22 2042
SHA1 Fingerprint:
ECA9C7F3872B842336BA39D8B73E43FFD843FCA5

Total Signature Lists # 1
Total Certificates # 1
```

The extended ownership is enabled with both Cisco and customer keys authenticated succesfully. The Platform Key Certificate is activated in the database. This certificate is used to authenticate further key management operations such as adding the SONiC or ONIE keys to the database.

Provision Customer Keys in Database

After the transfer of ownership, the router is in the Customer mode with the PKCustomer key added to the UEFI database. You can add or delete the KEKCustomer, dbCustomer and dbxCustomer keys using authenticated variable (AV) that is signed with the PKCustomer key.

Before you begin

You must create the AVs to provision the KEKCustomer key, dbCustomer key and Cisco ONIE key in Customer database. If you do not have the AVs created, see for instructions.

Note Key management:

- You can use the PKCustomer key, which is the master key, to create other keys. We recommend that you create the KEKCustomer key using PKCustomer as the signer.
- Use the KEKCustomer key to create and manage dbCustomer and dbxCustomer database keys.
- Use the ONIE key to securely install the Cisco-signed ONIE image.

Step 1 Use the following commands to apply the AV.

- Add the certificates or hashes to the certificate database.

```
Router#platform security variable customer append <key> <path-to-AV> location <device-location>
```

Example 1: Add a `KEKCustomer` certificate from the AV. This is optional. You can use the PKCustomer private key to create AV and to add SONiC image key into the dbCustomer database.

```
Router#platform security variable customer append KEKCustomer /harddisk:/append_kekcustomer.auth
 location all
Fri Feb 24 05:15:35.765 UTC
Performing operation on all nodes..
=========================
Location : 0/RP0/CPU0
=========================
Successfully applied AV /harddisk:/append_kekcustomer.auth for KEKCustomer
* WARNING *: Immediate reboot is recommended to avoid system instantly!
=========================
Location : 0/1/CPU0
=========================
Successfully applied AV /harddisk:/append_kekcustomer.auth for KEKCustomer
* WARNING *: Immediate reboot is recommended to avoid system instantly!
```

Example 2: Add a `dbCustomer` certificate from the AV.

```
Router#platform security variable customer append dbCustomer /harddisk:/append_dbcustomer.auth
location all
Fri Feb 24 06:23:23.111 UTC
Performing operation on all nodes..
=========================
Location : 0/RP0/CPU0
=========================
Successfully applied AV /harddisk:/append_dbcustomer.auth for dbCustomer
* WARNING *: Immediate reboot is recommended to avoid system instantly!
=========================
Location : 0/1/CPU0
=========================
Successfully applied AV /harddisk:/append_dbcustomer.auth for dbCustomer
* WARNING *: Immediate reboot is recommended to avoid system i
```

Step 2 Reload the nodes on the router.

Example:

```
Router#reload location all
```

Step 3 Verify that the keys are provisioned successfully.

Example:

```
Router#show platform security variable customer <key> location <device-location>
```

In this example, you verify that the keys are added in the database for all devices.

```
Router#show platform security variable customer all location all
Thu Feb 23 04:14:17.793 UTC
Performing operation on all nodes..
=========================
Location : 0/RP0/CPU0
=========================

Variable : PKCustomer
+--------------------

Signature List # 0
GUID : f79d17d1-88d4-40dd-aff8-9f9da3c30e9e
Extension type : X509

Entry # 0
Owner GUID : f79d17d1-88d4-40dd-aff8-9f9da3c30e9e
Size : 1066

  Serial Number  : ED:88:CD:A6:35:C2:59:B4
  Subject:
        O=Cisco,OU=RELEASE,CN=IOSXR-WHITEBOX-PK
  Issued By      :
        O=Cisco,OU=RELEASE,CN=IOSXR-WHITEBOX-PK
  Validity Start : 06:18:18 UTC Thu Jan 27 2022
  Validity End   : 06:18:18 UTC Wed Jan 22 2042
  SHA1 Fingerprint:
         ECA9C7F3872B842336BA39D8B73E43FFD843FCA5

Total Signature Lists # 1
Total Certificates # 1

Variable : KEKCustomer
+--------------------

Signature List # 0
GUID : f79d17d1-88d4-40dd-aff8-9f9da3c30e9e
Extension type : X509

Entry # 0
Owner GUID : f79d17d1-88d4-40dd-aff8-9f9da3c30e9e
Size : 799

  Serial Number  : A3:EC:C0:B0:61:FF:9C:42
  Subject:
        CN=Signature-KEK key
  Issued By      :
        CN=Signature-KEK key
  Validity Start : 22:16:45 UTC Wed Feb 22 2023
  Validity End   : 22:16:45 UTC Sat Feb 19 2033
  SHA1 Fingerprint:
         9F38C251A46F59420B8714E566681A0668ABEEBF

Total Signature Lists # 1
Total Certificates # 1

Variable : dbCustomer
+--------------------

Signature List # 0
GUID : f79d17d1-88d4-40dd-aff8-9f9da3c30e9e
Extension type : X509
```

```
Entry # 0
Owner GUID : f79d17d1-88d4-40dd-aff8-9f9da3c30e9e
Size : 797

  Serial Number  : 81:83:BD:97:2D:4B:42:B8
  Subject:
        CN=DB_CUST_TEST_KEY
  Issued By      :
        CN=DB_CUST_TEST_KEY
  Validity Start : 14:25:12 UTC Thu Feb 23 2023
  Validity End   : 14:25:12 UTC Sun Feb 20 2033
  SHA1 Fingerprint:
         C6140B381FAEF88BA4A9AD63E47926C7134F48C4

Total Signature Lists # 1
Total Certificates # 1

Variable : dbxCustomer
+--------------------
Variable dbxCustomer has no entries

========================
Location : 0/1/CPU0
========================

Variable : PKCustomer
+--------------------

Signature List # 0
GUID : f79d17d1-88d4-40dd-aff8-9f9da3c30e9e
Extension type : X509

Entry # 0
Owner GUID : f79d17d1-88d4-40dd-aff8-9f9da3c30e9e
Size : 1066

  Serial Number  : ED:88:CD:A6:35:C2:59:B4
  Subject:
        O=Cisco,OU=RELEASE,CN=IOSXR-WHITEBOX-PK
  Issued By      :
        O=Cisco,OU=RELEASE,CN=IOSXR-WHITEBOX-PK
  Validity Start : 06:18:18 UTC Thu Jan 27 2022
  Validity End   : 06:18:18 UTC Wed Jan 22 2042
  SHA1 Fingerprint:
         ECA9C7F3872B842336BA39D8B73E43FFD843FCA5

Total Signature Lists # 1
Total Certificates # 1

Variable : KEKCustomer
+--------------------

Signature List # 0
GUID : f79d17d1-88d4-40dd-aff8-9f9da3c30e9e
Extension type : X509

Entry # 0
Owner GUID : f79d17d1-88d4-40dd-aff8-9f9da3c30e9e
Size : 799

  Serial Number  : A3:EC:C0:B0:61:FF:9C:42
  Subject:
        CN=Signature-KEK key
```

```
  Issued By      :
        CN=Signature-KEK key
  Validity Start : 22:16:45 UTC Wed Feb 22 2023
  Validity End   : 22:16:45 UTC Sat Feb 19 2033
  SHA1 Fingerprint:
         9F38C251A46F59420B8714E566681A0668ABEEBF

Total Signature Lists # 1
Total Certificates # 1

Variable : dbCustomer
+--------------------

Signature List # 0
GUID : f79d17d1-88d4-40dd-aff8-9f9da3c30e9e
Extension type : X509

Entry # 0
Owner GUID : f79d17d1-88d4-40dd-aff8-9f9da3c30e9e
Size : 797

  Serial Number  : 81:83:BD:97:2D:4B:42:B8
  Subject:
        CN=DB_CUST_TEST_KEY
  Issued By      :
        CN=DB_CUST_TEST_KEY
  Validity Start : 14:25:12 UTC Thu Feb 23 2023
  Validity End   : 14:25:12 UTC Sun Feb 20 2033
  SHA1 Fingerprint:
         C6140B381FAEF88BA4A9AD63E47926C7134F48C4

Total Signature Lists # 1
Total Certificates # 1

Variable : dbxCustomer
+--------------------
Variable dbxCustomer has no entries
```

What to do next

After the keys are successfully registered in the UEFI database, you can securely migrate from Cisco IOS XR to SONiC operating system.

Migrate from Cisco IOS XR to SONiC OS Using Automation Script

This section provides intructions to use **sonic-migutil.py** script to migrate the Cisco 8000 series modular chassis from IOS XR to SONiC operating system. This script simplifies the process to migrate route processor (RP) and line card (LC) to SONiC OS.

Alternatively, you can manually migrate the OS using a PXE server. For more information, see .

Before you begin

Complete these prerequisites before you install SONiC on a router running Cisco IOS XR Software:

- Configure the Management interface.

```
Router#conf t
Router(config)#interface mgmtEth 0/RP0/CPU0/0
Router(config-if)#ipv4 address 192.0.2.0/24
Router(config-if)#no shut
Router(config-if)#commit
```

- Configure the SSH server.

```
Router(config)#ssh server
Router(config)#commit
Router(config)#end
```

- Cisco IOS XR software version 7.5.41 installed on the router.
- Ensure peer RP is not configured on the router.
- Copy the following images from the Github repository to the RP. In this example, the images are copied from the repository with address 192.0.2.0 to the harddisk: directory on the router.

```
sonic@host:~$scp sonic-migutil.py cisco@192.0.2.0:/harddisk:/
sonic@host:~$scp sonic-cisco-8000.bin cisco@192.0.2.0:/harddisk:/onie-installer.bin
sonic@host:~$scp onie-recovery-x86_64-cisco_8000-r0.efi64.pxe
cisco@192.0.2.0:/harddisk:/onie-recovery-x86_64-cisco_8000-r0.efi64.pxe
```

- Copy below images from RP to staged LC. Identify one of the working LC as staging LC with address 172.0.<slot>.1, where <*slot*> is the LC number.

```
Router#run scp /tmp/sonic-migutil.py root@172.0.0.1:/harddisk:/
Router#run scp /harddisk:/onie-recovery-x86_64-cisco_8000-r0.efi64.pxe
root@172.0.0.1:/www/pages
Router#run scp /harddisk:/onie-installer.bin root@172.0.0.1:/www/pages/onie-installer.bin
```

Step 1 Migrate the RP from Cisco IOS XR to SONiC OS.

a) Enter the staged LC.

Example:

```
Router#run rconsole -s 1
```

b) Run iPXE service on the staged LC.

Example:

```
[ios:~]$python3 /ws/sonic-migutil.py --start
[2023-05-10 18:17:40,501] [INFO] : Discover SONiC images ...
[2023-05-10 18:17:40,501] [INFO] : Found ONIE image: /www/pages/onie.pxe
[2023-05-10 18:17:40,501] [INFO] : Found SONiC image: /www/pages/onie-installer.bin
[2023-05-10 18:17:40,505] [INFO] : Found EOBC ip address: 1.0.0.3
[2023-05-10 18:17:40,505] [INFO] : Create SONiC dhcp config for ip = 1.0.0.3
[2023-05-10 18:17:40,508] [INFO] : DHCP config file: /usr/local/etc/sonic.dhcp.conf ...created
[2023-05-10 18:17:40,528] [INFO] : start DHCPD process
[2023-05-10 18:17:50,558] [INFO] : DHCP process started ...
[2023-05-10 18:17:50,558] [INFO] : Disable headless reload
```

c) Verify the iPXE service on the staged LC.

Example:

```
[ios:~]$python3 /ws/sonic-migutil.py --verify
[2023-04-10 18:18:33,256] [INFO] : Discover SONiC images ...
[2023-04-10 18:18:33,256] [INFO] : Found ONIE image: /www/pages/onie.pxe
[2023-04-10 18:18:33,256] [INFO] : Found SONiC image: /www/pages/onie-installer.bin
[2023-04-10 18:18:33,256] [INFO] : Headless reload setup ... ok
```

```
[2023-04-10 18:18:33,256] [INFO] : DHCP config setup ... ok
[2023-04-10 18:18:33,274] [INFO] : DHCP daemon status ... ok
```

d) Setup the staging LC to not reboot if RP goes down.

Example:

```
Router#configure
Router(config)#hw-module reset auto disable location 0/1/CPU0
```

e) Shutdown all other LCs.

Example:

```
Router(config)#hw-module shutdown location 0/0/CPU0
Router(config)#hw-module shutdown location 0/5/CPU0
Router(config)#commit
Router(config)#end
```

f) Verify the state of the LCs to ensure all LCs are in shutdown state.

Example:

```
Router#show platform
Wed May 10 20:30:53.734 UTC
Node              Type                       State                    Config state
--------------------------------------------------------------------------------
0/RP0/CPU0        8800-RP(Active)            IOS XR RUN               NSHUT
0/0/CPU0          88-LC0-36FH                IOS XR RUN               NSHUT
0/1/CPU0          8800-LC-48H                IOS XR RUN               NSHUT
0/5/CPU0          88-LC0-36FH-M              IOS XR RUN               NSHUT
0/FC0             8808-FC0                   OPERATIONAL              NSHUT
0/FT0             8808-FAN                   OPERATIONAL              NSHUT
0/FT1             8808-FAN                   OPERATIONAL              NSHUT
0/FT2             8808-FAN                   OPERATIONAL              NSHUT
0/FT3             8808-FAN                   OPERATIONAL              NSHUT
0/PT0             8800-HV-TRAY               OPERATIONAL              NSHUT
0/PT1             8800-HV-TRAY               OPERATIONAL              NSHUT
0/PT2             8800-HV-TRAY               OPERATIONAL              NSHUT
```

g) Configure RP bootmedia to internal iPXE.

Example:

```
Router#run python3 /ws/sonic-migutil.py --rpconfigipxe
Wed May 10 18:24:19.048 UTC
[2023-05-10 18:24:19,145] [INFO] : Configure reload to internal ipxe
[2023-05-10 18:24:19,145] [DEBUG]: running: pcimemwrite 0xA2401100 4 0x00000004
[2023-05-10 18:24:19,150] [DEBUG]: running: pcimemread 0xA2401100 4 | grep 'a2401100 :'| awk
'{print $3}'
[2023-05-10 18:24:19,155] [INFO] : Internal ipxe config done
```

h) Reload the RP.

Example:

```
Router#reload location 0/RP0/CPU0 noprompt
```

Wait untill the RP and LC loads with SONiC OS and the login prompt appears.

Step 2 Check the status of the cards after the upgrade.

Example:

```
root@sonic#show chassis module status
        Name                                Description    Physical-Slot    Oper-Status
Admin-Status
------------  ----------------------------------------  ---------------  -------------
```

```
--------------
FABRIC-CARD0  Cisco 8808 Fabric Card for 14.4T Line Cards              18          Online
    up
FABRIC-CARD1                                              N/A          19           Empty
    up
FABRIC-CARD2                                              N/A          20           Empty
    up
FABRIC-CARD3                                              N/A          21           Empty
    up
  LINE-CARD0                                              N/A           2         Offline
    up
  LINE-CARD1                                              N/A           4         Offline
    up
  LINE-CARD2                                              N/A           6           Empty
    up
 SUPERVISOR0                    Cisco 8800 Route Processor              30          Online
    up
 SUPERVISOR1                                              N/A          31           Empty
    up
```

Wait till all RP and LCs show `Online` operational status.

Step 3 Verify that the FPD version is `0.1` on all the cards.

Example:

```
root@sonic#cardevent.py --send CV_FPDPUBLISH --slot all
root@sonic#fpd-util.py --getfpd
1.0.0.13_programed 0.1
1.0.0.3_programed 0.1
1.0.0.5_programed 0.1
1.0.0.33_programed 0.1
```

The OS is migrated from Cisco IOS XR to SONiC.