



Upgrading the Cisco cBR-8 Router System to Cisco IOS XE Everest 16.6.1

This section contains the upgrade procedures for the Cisco cBR-8 Router System.

- [Upgrading from Cisco IOS-XE 3.18.1aSP to Cisco IOS XE Everest 16.6.1, on page 1](#)
- [Upgrading from Cisco IOS XE Everest 16.5.1 to Cisco IOS XE Everest 16.6.1, on page 8](#)

Upgrading from Cisco IOS-XE 3.18.1aSP to Cisco IOS XE Everest 16.6.1

The correct firmware versions are listed in the tables below. Use the commands in the tables to verify the firmware versions.

Table 1: Firmware Versions

Internal Name	Component Name	Correct Version	Command
Supervisor CPLD	CBR-CCAP-SUP-160G Rommon CPLD	16052011	show platform
Supervisor ROMMON	CBR-CCAP-SUP-160G Rommon	16.6(1r)S	show platform
Linecard CPLD	CBR-CCAP-LC-40G CPLD	00000025	show platform
Linecard Uboot	CBR-CCAP-LC-40G Rommon	2011.03.18	show platform
Linecard PSOC	CBR-CCAP-LC-40G PSOC	4.6	show platform diag
Docsis 3.0 downstream module PSOC	CBR-CCAP-LC-40G Gemin1 PSOC	3.9	show platform diag

Docsis 3.0 downstream module CPLD	CBR-CCAP-LC-40G Gemini1 CPLD	0.7	show platform diag
Docsis 3.0 downstream module Micro	CBR-CCAP-LC-40G Gemini1 Micro	1.E	show platform diag
Docsis 3.0 downstream module FPGA	CBR-CCAP-LC-40G Gemini1 Apollo	2.F	show platform diag
Docsis 3.1 downstream module PSOC	CBR-CCAP-LC-40G Gemini2 PSOC	4.4	show platform diag
Docsis 3.1 downstream module CPLD	CBR-CCAP-LC-40G Gemini2 CPLD	0.7	show platform diag
Docsis 3.1 downstream module Micro	CBR-CCAP-LC-40G Gemini2 Micro	3.19	show platform diag
Docsis 3.1 downstream module FPGA	CBR-CCAP-LC-40G Gemini2 Apollo	4.484B	show platform diag

Upgrading Manually

Before you begin

Before upgrading the system, make sure the following requirements are met:

- The firmware versions are not lower than the ones listed in [Firmware versions](#) table. Otherwise upgrade the firmware versions, see [Upgrading the Cisco cBR-8 Router Firmware](#).
- Make sure Line Card CPLD version is 00000025. If the value is lower than 00000025, follow this procedure to upgrade the Line Card CPLD to version 00000025 first:
http://www.cisco.com/c/en/us/td/docs/cable/cbr/upgrade/guide/b_cbr_upgrade-3-18s/b_cbr_upgrade_hardware.html#task_E0B78DCCC88A41749DA2783736CE37A6
- Download two files from the following Cisco.com Software Center URL:
<https://software.cisco.com/download/type.html?mdfid=286283913&flowid=73842>
 - IOS XE Software Version 16.6.1: **cbrsup-universalk9.16.06.01.SPA.bin**
 - IOS XE Hardware Programmable Devices Version 16.6.1:
cbrsup-programmable_firmware.16.06.01.SPA.pkg
- Console access for both SUPs are required.
- Ability to power cycle the chassis. Power cycle chassis is required to upgrade Supervisor CPLD.



Note Do not power cycle the cBR-8 router during the firmware upgrade process. Power cycling the chassis may corrupt the ROMMON/Uboot image.

Step 1 Copy Cisco IOS-XE Everest 16.6.1 package to bootflash: and stby-bootflash:.

```
copy <location>/cbrsup-universalk9.16.06.01.SPA.bin bootflash:
copy <location>/cbrsup-universalk9.16.06.01.SPA.bin stby-bootflash:
```

Step 2 Verify Cisco IOS-XE Everest 16.6.1 package against the md5 hash as provided in the Cisco.com Software center.

```
verify /md5 bootflash:cbrsup-universalk9.16.06.01.SPA.bin
verify /md5 stby-bootflash:cbrsup-universalk9.16.06.01.SPA.bin
```

Step 3 Copy the hardware programmable devices upgrade package to harddisk: and stby-harddisk:.

```
copy <location>/cbrsup-programmable_firmware.16.06.01.SPA.pkg harddisk:
copy <location>/cbrsup-programmable_firmware.16.06.01.SPA.pkg stby-harddisk:
```

Step 4 Verify the hardware programmable devices upgrade package against the md5 hash as provided in the Cisco.com Software center.

```
verify /md5 harddisk:cbrsup-programmable_firmware.16.06.01.SPA.pkgg
verify /md5 stby-harddisk:cbrsup-programmable_firmware.16.06.01.SPA.pkgg
```

Step 5 Check system status prior to upgrade. Save the information to compare against the system status after upgrade. For the commands to use to check the status, see the **show** commands at the end of this section.

Step 6 Configure the chassis to boot the system with Cisco IOS-XE Everest 16.6.1 image.

```
Configure terminal
no boot system
boot system bootflash:cbrsup-universalk9.16.06.01.SPA.bin
end
write mem
```

Step 7 Reload the cBR-8 router.

```
Reload
```

Note The system will reload twice.

Step 8 Remove the secondary line card from line card redundancy group if redundancy is configured.

```
Configure terminal
redundancy
```

```
linecard-group 0 internal-switch
no member slot 0 secondary
end
```

Step 9 Upgrade Docsis 3.1 downstream modules in all the slots.

```
upgrade hw-programmable cable 0 dsphy all pkg_name
/harddisk/cbrsup-programmable_firmware.16.06.01.SPA.pkg
```

Step 10 Upgrade Supervisor 0/1 CPLD.

```
upgrade hw-programmable cable r0 viper pkg_name
/harddisk/cbrsup-programmable_firmware.16.06.01.SPA.pkg
upgrade hw-programmable cable r1 viper pkg_name
/harddisk/cbrsup-programmable_firmware.16.06.01.SPA.pkg
```

Step 11 Configure config-register to manual boot.

```
Configure terminal config-register 0x0 end
```

Step 12 Reload the cBR-8 router. Answer **no** to not save the configuration.

```
cBR8#reload
System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]
cBR8#
```

Step 13 Configure to automatic boot by typing following command in **rommon** > prompt.

```
rommon 1 > confreg 0x2102
rommon 2 > sync
rommon 3 >
```

Step 14 Power cycle chassis, wait for both SUPs to auto boot to 16.6.1 image.

What to do next

Perform verification test to determine if the upgrade is successful, include:

- Verify the router is running the new IOS-XE release using **show version** command.
- Check facility alarms using **show facility-alarm status** command.
- Check the status of the power supplies using **show environment power** command.
- Check PS status using **show platform hardware slot P<0-5> mcu status** command.
- Complete trace routes to known good off-network IP address using the source address of customer CPE blocks to verify routing is working.
- Check logs for error messages using **show log** command.

These **show** commands may be useful in the verification test:

- **show redundancy**
- **show platform**
- **show platform diag**
- **show environment**
- **show redundancy linecard all**
- **show isis neighbors**
- **show ip ospf neighbor**
- **show ip route rip**
- **show ip mroute**
- **show cops servers**
- **show cable modem voice**
- **show cable calls**
- **show cable metering verbose**
- **show cable licenses all**
- **show inventory**

Upgrading with Ansible

Before you begin

Before upgrading the firmware, make sure the following requirements are met:

1. Prepare Ansible Server, operating system can be Linux/Windows/Mac, with docker service pre-installed.

For docker installation guide, please check following link:

<https://docs.docker.com/engine/installation/>

2. Check if the chassis supports AAA or local authentication with username & password. If not configured, use following CLI to enable local authentication, for example:

```
Cbr8#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
cBR8(config)#username cisco privilege 15 password 0 cisco
cBR8(config)#enable secret cisco
cBR8(config)#line vty 0 15
cBR8(config)#login local
cBR8(config)#exec-timeout 0 0
cBR8(config)#session-timeout 0
cBR8(config)#exit
```

3. If SSH is not enabled, use following CLI to enable SSH on cBR8, skip the domain name configuration if already configured.

```

cBR8(config)# ip domain-name domain.com
cBR8(config)#crypto key generate rsa
The name for the keys will be: cbr8.domain.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)

cBR8(config)#end
cBR8#copy running-config startup-config
cBR8#show ip ssh
SSH Enabled - version 1.99

```

4. Verify if the Ansible server can access cBR-8 using SSH.

```

[ansible@server ~]$ ssh cisco@100.0.0.1
The authenticity of host '100.0.0.1 (100.0.0.1)' can't be established.
RSA key fingerprint is c3:be:8f:cf:76:f4:31:4b:80:d8:2e:f0:76:6d:ff:bf.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '100.0.0.1' (RSA) to the list of known hosts.
Password:
cBR8#

```

5. Download three files from the following Cisco.com Software Center URL:

<https://software.cisco.com/download/type.html?mdfid=286283913&flowid=73842>

- IOS XE Software Version 16.6.1: **cbrsup-universalk9.16.06.01.SPA.bin**
 - IOS XE Hardware Programmable Devices Version 16.6.1:
cbrsup-programmable_firmware.16.06.01.SPA.pkg
 - **cbr-8_upgrade_ansible_16.6.1.tar**
6. Copy **cbrsup-universalk9.16.06.01.SPA.bin** and **cbrsup-programmable_firmware.16.06.01.SPA.pkg** to TFTP/FTP/SCP server or usb disk. Upload **cbr-8_upgrade_ansible_16.6.1.tar** to Ansible server.
7. Console access for both SUPs are required.
8. Ability to power cycle the chassis. Power cycle chassis is required to upgrade Supervisor CPLD.

Step 1 Run following CLI on the Ansible server to create the docker image.

```
docker import cbr-8_upgrade_ansible_16.6.1.tar ansible_mop
```

Step 2 Start docker container with the image and enter the container shell.

```
docker run -it --name=mop ansible_mop /bin/bash
```

Step 3 Change current directory to the playbook folder for this software and firmware upgrade.

```
cd /opt/cbr-8_upgrade_ansible_3.18sp_to_16.6.1
```

- Step 4** Modify hosts file to add target cBR-8 ip addresses, can be multiple lines if customer wants to upgrade firmware on multiple cBR8 routers simultaneously, sample file is as below:

```
[cbr]
100.110.110.110
100.185.185.185
```

- Step 5** Modify secrets.yaml file, change the username/password/enable password to reflect the real username/password/enable configuration for target cBR. If no enable password is set, just keep the sample **cisco** for **auth_pass**.

```
creds:
  username: cisco
  password: cisco
  auth_pass: cisco
```

- Step 6** Modify upgrade_vars.yaml file to indicate the firmware package name, ios image name and source (Optional if the package files are already on cbr-8 harddisk:).

```
file_info:
  image_name: cbrsup-universalk9.16.06.01.SPA.bin
  pkg_name: cbrsup-programmable_firmware.16.06.01.SPA.pkg
  #if the pkg file in the TB, just modify dst_dir to the pkg location
  #the two examples shows the usage
  #example1
  #src_dir: "ftp://username:password@20.11.0.42:~/ "
  #example2
  #src_dir: "tftp://192.168.3.47/ "
  #example3
  #src_dir: "usb0:"
  src_dir: "ftp://username:password@20.11.0.42:~/../images/"

slot_info:
  #slot_to_upgrade: [2,3,6,7,8,9]
  slot_to_upgrade: "ALL"
```

- Step 7** Execute following command to start the playbook to upgrade firmware.

```
./run_mop_upgrade
```

- Step 8** Reload the system by typing **reload** on the active SUP and answering **no** to not save the configuration.

```
cBR8#reload
System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]
cBR8#
```

- Step 9** From ROMMON issue the following command on both SUPs.

```
rommon 1 > confreg 0x2102
rommon 2 > sync
rommon 3 >
```

- Step 10** Power cycle chassis, wait for both SUPs to auto boot to 16.6.1 image.

```
rommon 1>
Initializing Hardware ...

?

System Bootstrap, Version 16.6(1r)S, RELEASE SOFTWARE
Copyright (c) 1994-2016 by cisco Systems, Inc.

Current image running: Boot ROM1

Last reset cause: PowerOn

Viper version register: 0x16052011
Set Chassis Type to 13RU
Cisco cBR-8 platform with 50331648 Kbytes of main memory
```

Step 11 After system bootup and stable, execute following command to start the playbook to check the upgrade result.

```
./run_mop_upgrade_post

...
TASK [debug] *****
Friday 17 March 2017 14:30:25 +0800 (0:00:00.014) 0:01:10.187 *****
ok: [100.185.185.185] => {
  "msg": "Mop upgrade passed!"
}
PLAY RECAP *****
100.185.185.185 : ok=120 changed=1 unreachable=0 failed=0
```

Step 12 Exit the container if finished upgrading this time to stop the container.

```
exit
```

Step 13 If user wants to start the container again, use following command to start the container and enter its shell.

```
docker start mop
docker attach mop
```

Step 14 All the file changes are kept in the container, user can run step 4-11 to upgrade again.

Upgrading from Cisco IOS XE Everest 16.5.1 to Cisco IOS XE Everest 16.6.1

The correct firmware versions are listed in the tables below. Use the commands in the tables to verify the firmware versions.

Table 2: Firmware Versions

Internal Name	Component Name	Correct Version	Command
---------------	----------------	-----------------	---------

Supervisor CPLD	CBR-CCAP-SUP-160G Rommon CPLD	16052011	show platform
Supervisor ROMMON	CBR-CCAP-SUP-160G Rommon	16.6(1r)S	show platform
Linecard CPLD	CBR-CCAP-LC-40G CPLD	00000025	show platform
Linecard Uboot	CBR-CCAP-LC-40G Rommon	2011.03.18	show platform
Linecard PSOC	CBR-CCAP-LC-40G PSOC	4.6	show platform diag
Docsis 3.0 downstream module PSOC	CBR-CCAP-LC-40G Gemin1 PSOC	3.9	show platform diag
Docsis 3.0 downstream module CPLD	CBR-CCAP-LC-40G Gemin1 CPLD	0.7	show platform diag
Docsis 3.0 downstream module Micro	CBR-CCAP-LC-40G Gemin1 Micro	1.E	show platform diag
Docsis 3.0 downstream module FPGA	CBR-CCAP-LC-40G Gemin1 Apollo	2.F	show platform diag
Docsis 3.1 downstream module PSOC	CBR-CCAP-LC-40G Gemin2 PSOC	4.4	show platform diag
Docsis 3.1 downstream module CPLD	CBR-CCAP-LC-40G Gemin2 CPLD	0.7	show platform diag
Docsis 3.1 downstream module Micro	CBR-CCAP-LC-40G Gemin2 Micro	3.19	show platform diag
Docsis 3.1 downstream module FPGA	CBR-CCAP-LC-40G Gemin2 Apollo	4.484B	show platform diag

Upgrading Manually

Before you begin

Before upgrading the system, make sure the following requirements are met:

- Download two files from the following Cisco.com Software Center URL:

<https://software.cisco.com/download/type.html?mdfid=286283913&flowid=73842>

- IOS XE Software Version 16.6.1: **cbrsup-universalk9.16.06.01.SPA.bin**
- IOS XE Hardware Programmable Devices Version 16.6.1:
cbrsup-programmable_firmware.16.06.01.SPA.pkg



Note Do not power cycle the cBR-8 router during the firmware upgrade process. Power cycling the chassis may corrupt the ROMMON/Uboot image.

Step 1 Copy Cisco IOS-XE Everest 16.6.1 package to bootflash: and stby-bootflash:.

```
copy <location>/cbrsup-universalk9.16.06.01.SPA.bin bootflash:
copy <location>/cbrsup-universalk9.16.06.01.SPA.bin stby-bootflash:
```

Step 2 Verify Cisco IOS-XE Everest 16.6.1 package against the md5 hash as provided in the Cisco.com Software center.

```
verify /md5 bootflash:cbrsup-universalk9.16.06.01.SPA.bin
verify /md5 stby-bootflash:cbrsup-universalk9.16.06.01.SPA.bin
```

Step 3 Copy the hardware programmable devices upgrade package to harddisk: and stby-harddisk:.

```
copy <location>/cbrsup-programmable_firmware.16.06.01.SPA.pkg harddisk:
copy <location>/cbrsup-programmable_firmware.16.06.01.SPA.pkg stby-harddisk:
```

Step 4 Verify the hardware programmable devices upgrade package against the md5 hash as provided in the Cisco.com Software center.

```
verify /md5 harddisk:cbrsup-programmable_firmware.16.06.01.SPA.pkg
verify /md5 stby-harddisk:cbrsup-programmable_firmware.16.06.01.SPA.pkg
```

Step 5 Check system status prior to upgrade. Save the information to compare against the system status after upgrade. For the commands to use to check the status, see the **show** commands at the end of this section.

Step 6 Configure the chassis to boot the system with Cisco IOS-XE Everest 16.6.1 image.

```
Configure terminal
no boot system
boot system bootflash:cbrsup-universalk9.16.06.1.SPA.bin
end
write mem
```

Step 7 Reload the cBR-8 router.

```
Reload
```

Note The system will reload twice.

Step 8 Remove the secondary line card from line card redundancy group if redundancy is configured.

```
Configure terminal
redundancy
linecard-group 0 internal-switch
no member slot 0 secondary
end
```

Step 9 Upgrade Docsis 3.1 downstream modules in all the slots.

```
upgrade hw-programmable cable 0 dsphy all pkg_name
/harddisk/cbrsup-programmable_firmware.16.06.01.SPA.pkg
```

Step 10 Wait for the system log message asking the user to reload the line card that was upgraded.

```
001860: Jun 15 19:05:05.904 PDT: %IOSXE-5-PLATFORM: CLC0: cdman: Suggest reload the line card for
new FW to take effect using CLI: hw slot <slot-id> reload
```

Step 11 Reload Docsis 3.1 downstream modules in all the slots.

```
hw slot <slot-id> reload
```

Step 12 Add secondary line card into line card redundancy group.

```
configure terminal
redundancy
linecard-group 0 internal-switch
member slot 0 secondary
end
```

What to do next

Perform verification test to determine if the upgrade is successful, include:

- Verify the router is running the new IOS-XE release using **show version** command.
- Check facility alarms using **show facility-alarm status** command.
- Check the status of the power supplies using **show environment power** command.
- Check PS status using **show platform hardware slot P<0-5> mcu status** command.
- Complete trace routes to known good off-network IP address using the source address of customer CPE blocks to verify routing is working.
- Check logs for error messages using **show log** command.

These **show** commands may be useful in the verification test:

- **show redundancy**
- **show platform**
- **show platform diag**
- **show environment**
- **show redundancy linecard all**
- **show isis neighbors**
- **show ip ospf neighbor**
- **show ip route rip**
- **show ip mroute**
- **show cops servers**
- **show cable modem voice**
- **show cable calls**
- **show cable metering verbose**
- **show cable licenses all**
- **show inventory**

Upgrading with Ansible

Before you begin

Before upgrading the firmware, make sure the following requirements are met:

1. Prepare Ansible Server, operating system can be Linux/Windows/Mac, with docker service pre-installed.

For docker installation guide, please check following link:

<https://docs.docker.com/engine/installation/>

2. Check if the chassis supports AAA or local authentication with username & password. If not configured, use following CLI to enable local authentication, for example:

```
Cbr8#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Cbr8(config)#username cisco privilege 15 password 0 cisco
Cbr8(config)#enable secret cisco
Cbr8(config)#line vty 0 15
Cbr8(config)#login local
Cbr8(config)#exec-timeout 0 0
Cbr8(config)#session-timeout 0
Cbr8(config)#exit
```

3. If SSH is not enabled, use following CLI to enable SSH on cBR8, skip the domain name configuration if already configured.

```
Cbr8(config)# ip domain-name domain.com
Cbr8(config)#crypto key generate rsa
The name for the keys will be: cbr8.domain.com
```

Choose the size of the key modulus in the range of 360 to 4096 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

```
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
```

```
cBR8(config)#end
cBR8#copy running-config startup-config
cBR8#show ip ssh
SSH Enabled - version 1.99
```

4. Verify if the Ansible server can access cBR-8 using SSH.

```
[ansible@server ~]$ ssh cisco@100.0.0.1
The authenticity of host '100.0.0.1 (100.0.0.1)' can't be established.
RSA key fingerprint is c3:be:8f:cf:76:f4:31:4b:80:d8:2e:f0:76:6d:ff:bf.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '100.0.0.1' (RSA) to the list of known hosts.
Password:
cBR8#
```

5. Download three files from the following Cisco.com Software Center URL:

<https://software.cisco.com/download/type.html?mdfid=286283913&flowid=73842>

- IOS XE Software Version 16.6.1: **cbrsup-universalk9.16.06.01.SPA.bin**
- IOS XE Hardware Programmable Devices Version 16.6.1:
cbrsup-programmable_firmware.16.06.01.SPA.pkg
- **cbr-8_upgrade_ansible_16.6.1.tar**

6. Copy **cbrsup-universalk9.16.06.01.SPA.bin** and **cbrsup-programmable_firmware.16.06.01.SPA.pkg** to TFTP/FTP/SCP server or usb disk. Upload **cbr-8_upgrade_ansible_16.6.1.tar** to Ansible server.

Step 1 Run following CLI on the Ansible server to create the docker image.

```
docker import cbr-8_upgrade_ansible_16.6.1.tar ansible_mop
```

Step 2 Start docker container with the image and enter the container shell.

```
docker run -it --name=mop ansible_mop /bin/bash
```

Step 3 Change current directory to the playbook folder for this software and firmware upgrade.

```
cd /opt/cbr-8_upgrade_ansible_16.5.1_to_16.6.1
```

Step 4 Modify hosts file to add target cBR-8 ip addresses, can be multiple lines if customer wants to upgrade firmware on multiple cBR8 routers simultaneously, sample file is as below:

```
[cbr]
100.110.110.110
```

```
100.185.185.185
```

Step 5 Modify secrets.yaml file, change the username/password/enable password to reflect the real username/password/enable configuration for target cBR. If no enable password is set, just keep the sample **cisco** for **auth_pass**.

```
creds:
  username: cisco
  password: cisco
  auth_pass: cisco
```

Step 6 Modify upgrade_vars.yaml file to indicate the firmware package name, ios image name and source (Optional if the package files are already on cbr-8 harddisk:).

```
file_info:
  image_name: cbrsup-universalk9.16.06.01.SPA.bin
  pkg_name: cbrsup-programmable_firmware.16.06.01.SPA.pkg
  #if the pkg file in the TB, just modify dst_dir to the pkg location
  #the two examples shows the usage
  #example1
  #src_dir: "ftp://username:password@20.11.0.42:~/ "
  #example2
  #src_dir: "tftp://192.168.3.47/ "
  #example3
  #src_dir: "usb0:"
  src_dir: "ftp://username:password@20.11.0.42:~/../images/"

slot_info:
  #slot_to_upgrade: [2,3,6,7,8,9]
  slot_to_upgrade: "ALL"
```

Step 7 Execute following command to start the playbook to upgrade firmware.

```
./run_mop_upgrade
```

Step 8 cBR-8 router is supposed to be reloaded automatically by Ansible.

Step 9 Exit the container if finished upgrading this time to stop the container.

```
exit
```

Step 10 If user wants to start the container again, use following command to start the container and enter its shell.

```
docker start mop
docker attach mop
```

Step 11 All the file changes are kept in the container, user can run step 4-7 to upgrade again.
