



Configure Cisco IP switches

ONTAP MetroCluster

NetApp
February 13, 2026

Table of Contents

- Configure Cisco IP switches 1
 - Configure Cisco IP switches for cluster interconnect and backend MetroCluster IP connectivity 1
 - Resetting the Cisco IP switch to factory defaults 1
 - Downloading and installing the Cisco switch NX-OS software 5
 - Downloading and installing the Cisco IP RCF files 11
 - Setting Forward Error Correction for systems using 25-Gbps connectivity 15
 - Disable unused ISL ports and port channels 15
- Configure MACsec encryption on Cisco 9336C switches in a MetroCluster IP site 16
 - Configure MACsec encryption on Cisco 9336C switches 16

Configure Cisco IP switches

Configure Cisco IP switches for cluster interconnect and backend MetroCluster IP connectivity

You must configure the Cisco IP switches for use as the cluster interconnect and for backend MetroCluster IP connectivity.

About this task

Several of the procedures in this section are independent procedures and you only need to execute those you are directed to or are relevant to your task.

Resetting the Cisco IP switch to factory defaults

Before installing any RCF file, you must erase the Cisco switch configuration and perform basic configuration. This procedure is required when you want to reinstall the same RCF file after a previous installation failed, or if you want to install a new version of an RCF file.

About this task

- You must repeat these steps on each of the IP switches in the MetroCluster IP configuration.
- You must be connected to the switch using the serial console.
- This task resets the configuration of the management network.

Steps

1. Reset the switch to factory defaults:
 - a. Erase the existing configuration:

```
write erase
```

- b. Reload the switch software:

```
reload
```

The system reboots and enters the configuration wizard. During the boot, if you receive the prompt “Abort Auto Provisioning and continue with normal setup? (yes/no)[n]”, you should respond `yes` to proceed.

- c. In the configuration wizard, enter the basic switch settings:
 - Admin password
 - Switch name
 - Out-of-band management configuration
 - Default gateway
 - SSH service (RSA)

After completing the configuration wizard, the switch reboots.

- d. When prompted, enter the user name and password to log in to the switch.

The following example shows the prompts and system responses when configuring the switch. The angle brackets (<<<) show where you enter the information.

```
---- System Admin Account Setup ----
Do you want to enforce secure password standard (yes/no) [y]:y
**<<<**

    Enter the password for "admin": password
    Confirm the password for "admin": password
        ---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.

Please register Cisco Nexus3000 Family devices promptly with your
supplier. Failure to register may affect response times for initial
service calls. Nexus3000 devices must be registered to receive
entitled support services.

Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.
```

You enter basic information in the next set of prompts, including the switch name, management address, and gateway, and select SSH with RSA.



This example shows the minimum information required to configure the RCF, additional options can be configured after the RCF has been applied. For example, you can configure SNMPv3, NTP, or SCP/SFTP after you have applied the RCF.

The following configuration will be applied:

```
password strength-check
switchname IP_switch_A_1
vrf context management
ip route 0.0.0.0/0 10.10.99.1
exit
no feature telnet
ssh key rsa 1024 force
feature ssh
system default switchport
system default switchport shutdown
copp profile strict
interface mgmt0
ip address 10.10.99.10 255.255.255.0
no shutdown
```

Would you like to edit the configuration? (yes/no) [n]:

Use this configuration and save it? (yes/no) [y]:

```
2017 Jun 13 21:24:43 A1 %$ VDC-1 %$ %COPP-2-COPP_POLICY: Control-
Plane is protected with policy copp-system-p-policy-strict.
```

```
[#####] 100%
Copy complete.
```

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
.
.
.
IP_switch_A_1#
```

2. Save the configuration:

```
IP_switch-A-1# copy running-config startup-config
```

3. Reboot the switch and wait for the switch to reload:

```
IP_switch-A-1# reload
```

4. Repeat the previous steps on the other three switches in the MetroCluster IP configuration.

Downloading and installing the Cisco switch NX-OS software

You must download the switch operating system file and RCF file to each switch in the MetroCluster IP configuration.

About this task

This task requires file transfer software, such as FTP, TFTP, SFTP, or SCP, to copy the files to the switches.

These steps must be repeated on each of the IP switches in the MetroCluster IP configuration.

You must use the supported switch software version.

[NetApp Hardware Universe](#)

Steps

1. Download the supported NX-OS software file.

[Cisco Software Download](#)

2. Copy the switch software to the switch:

```
copy sftp://root@server-ip-address/tftpboot/NX-OS-file-name bootflash: vrf  
management
```

In this example, the nxos.7.0.3.I4.6.bin file and EPLD image is copied from SFTP server 10.10.99.99 to the local bootflash:

```
IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/nxos.7.0.3.I4.6.bin
bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get /tftpboot/nxos.7.0.3.I4.6.bin
/bootflash/nxos.7.0.3.I4.6.bin
Fetching /tftpboot/nxos.7.0.3.I4.6.bin to /bootflash/nxos.7.0.3.I4.6.bin
/tftpboot/nxos.7.0.3.I4.6.bin          100% 666MB 7.2MB/s
01:32
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.

IP_switch_A_1# copy sftp://root@10.10.99.99/tftpboot/n9000-
epld.9.3.5.img bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get /tftpboot/n9000-epld.9.3.5.img /bootflash/n9000-
epld.9.3.5.img
Fetching /tftpboot/n9000-epld.9.3.5.img to /bootflash/n9000-
epld.9.3.5.img
/tftpboot/n9000-epld.9.3.5.img          161MB 9.5MB/s 00:16
sftp> exit
Copy complete, now saving to disk (please wait)...
Copy complete.
```

3. Verify on each switch that the switch NX-OS files are present in each switch's bootflash directory:

```
dir bootflash:
```

The following example shows that the files are present on IP_switch_A_1:

```

IP_switch_A_1# dir bootflash:
      .
      .
      .
698629632   Jun 13 21:37:44 2017   nxos.7.0.3.I4.6.bin
      .
      .
      .

Usage for bootflash://sup-local
 1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#

```

4. Install the switch software:

install all nxos bootflash:nxos.version-number.bin

The switch will reload (reboot) automatically after the switch software has been installed.

The following example shows the software installation on IP_switch_A_1:

```

IP_switch_A_1# install all nxos bootflash:nxos.7.0.3.I4.6.bin
Installer will perform compatibility check first. Please wait.
Installer is forced disruptive

Verifying image bootflash:/nxos.7.0.3.I4.6.bin for boot variable "nxos".
[#####] 100% -- SUCCESS

Verifying image type.
[#####] 100% -- SUCCESS

Preparing "nxos" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[#####] 100% -- SUCCESS

Preparing "bios" version info using image
bootflash:/nxos.7.0.3.I4.6.bin.
[#####] 100% -- SUCCESS          [#####] 100%
-- SUCCESS

Performing module support checks.          [#####] 100%
-- SUCCESS

Notifying services about system upgrade.    [#####] 100%

```

```
-- SUCCESS
```

```
Compatibility check is done:
```

Module	bootable	Impact	Install-type	Reason
1	yes	disruptive	reset	default upgrade is not hitless

```
Images will be upgraded according to following table:
```

Module Required	Image	Running-Version(pri:alt)	New-Version	Upg-
1	nxos	7.0(3)I4(1)	7.0(3)I4(6)	yes
1	bios	v04.24(04/21/2016)	v04.24(04/21/2016)	no

```
Switch will be reloaded for disruptive upgrade.
```

```
Do you want to continue with the installation (y/n)? [n] y
```

```
Install is in progress, please wait.
```

```
Performing runtime checks. [#####] 100% --  
SUCCESS
```

```
Setting boot variables.  
[#####] 100% -- SUCCESS
```

```
Performing configuration copy.  
[#####] 100% -- SUCCESS
```

```
Module 1: Refreshing compact flash and upgrading bios/loader/bootrom.  
Warning: please do not remove or power off the module at this time.  
[#####] 100% -- SUCCESS
```

```
Finishing the upgrade, switch will reboot in 10 seconds.  
IP_switch_A_1#
```

5. Wait for the switch to reload and then log in to the switch.

After the switch has rebooted the login prompt is displayed:

```
User Access Verification
IP_switch_A_1 login: admin
Password:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.
MDP database restore in progress.
IP_switch_A_1#

The switch software is now installed.
```

6. Verify that the switch software has been installed:

```
show version
```

The following example shows the output:

```
IP_switch_A_1# show version
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (C) 2002-2017, Cisco and/or its affiliates.
All rights reserved.
.
.
.

Software
  BIOS: version 04.24
  NXOS: version 7.0(3)I4(6)  **<<< switch software version**
  BIOS compile time: 04/21/2016
  NXOS image file is: bootflash:///nxos.7.0.3.I4.6.bin
  NXOS compile time: 3/9/2017 22:00:00 [03/10/2017 07:05:18]

Hardware
  cisco Nexus 3132QV Chassis
  Intel(R) Core(TM) i3- CPU @ 2.50GHz with 16401416 kB of memory.
  Processor Board ID FOC20123GPS

  Device name: A1
  bootflash: 14900224 kB
  usb1: 0 kB (expansion flash)

Kernel uptime is 0 day(s), 0 hour(s), 1 minute(s), 49 second(s)

Last reset at 403451 usecs after Mon Jun 10 21:43:52 2017

Reason: Reset due to upgrade
System version: 7.0(3)I4(1)
Service:

plugin
  Core Plugin, Ethernet Plugin
IP_switch_A_1#
```

7. Upgrade the EPLD image and reboot the switch.

```

IP_switch_A_1# install epld bootflash:n9000-epld.9.3.5.img module 1
Compatibility check:
Module          Type          Upgradable    Impact        Reason
-----
1              SUP          Yes           disruptive    Module Upgradable

Retrieving EPLD versions.... Please wait.
Images will be upgraded according to following table:
Module  Type  EPLD          Running-Version  New-Version  Upg-
Required
-----
1  SUP  MI FPGA      0x07            0x07        No
1  SUP  IO FPGA      0x17            0x19        Yes
1  SUP  MI FPGA2     0x02            0x02        No

The above modules require upgrade.
The switch will be reloaded at the end of the upgrade
Do you want to continue (y/n) ? [n] y

Proceeding to upgrade Modules.

Starting Module 1 EPLD Upgrade

Module 1 : IO FPGA [Programming] : 100.00% (      64 of      64 sectors)
Module 1 EPLD upgrade is successful.
Module  Type  Upgrade-Result
-----
1  SUP  Success

EPLDs upgraded.

Module 1 EPLD upgrade is successful.

```

- After the switch reboot, log in again and verify that the new version of EPLD loaded successfully.

```
show version module 1 epld
```

- Repeat these steps on the remaining three IP switches in the MetroCluster IP configuration.

Downloading and installing the Cisco IP RCF files

You must generate and install the RCF file to each switch in the MetroCluster IP configuration.

About this task

This task requires file transfer software, such as FTP, TFTP, SFTP, or SCP, to copy the files to the switches.

These steps must be repeated on each of the IP switches in the MetroCluster IP configuration.

You must use the supported switch software version.

NetApp Hardware Universe

If you are using a QSFP-to-SFP+ adapter, you might need to configure the ISL port in native speed mode instead of breakout speed mode. Refer to your switch vendor documentation to determine the ISL port speed mode.

There are four RCF files, one for each of the four switches in the MetroCluster IP configuration. You must use the correct RCF files for the switch model you are using.

Switch	RCF file
IP_switch_A_1	NX3232_v1.80_Switch-A1.txt
IP_switch_A_2	NX3232_v1.80_Switch-A2.txt
IP_switch_B_1	NX3232_v1.80_Switch-B1.txt
IP_switch_B_2	NX3232_v1.80_Switch-B2.txt

Steps

1. Generate the Cisco RCF files for MetroCluster IP.
 - a. Download the [RcfFileGenerator for MetroCluster IP](#)
 - b. Generate the RCF file for your configuration using the RcfFileGenerator for MetroCluster IP.



Modifications to the RCF files after download are not supported.

2. Copy the RCF files to the switches:
 - a. Copy the RCF files to the first switch:

```
copy sftp://root@FTP-server-IP-address/tftpboot/switch-specific-RCF
bootflash: vrf management
```

In this example, the NX3232_v1.80_Switch-A1.txt RCF file is copied from the SFTP server at 10.10.99.99 to the local bootflash. You must use the IP address of your TFTP/SFTP server and the file name of the RCF file that you need to install.

```

IP_switch_A_1# copy
sftp://root@10.10.99.99/tftpboot/NX3232_v1.80_Switch-A1.txt
bootflash: vrf management
root@10.10.99.99's password: password
sftp> progress
Progress meter enabled
sftp> get /tftpboot/NX3232_v1.80_Switch-A1.txt
/bootflash/NX3232_v1.80_Switch-A1.txt
Fetching /tftpboot/NX3232_v1.80_Switch-A1.txt to
/bootflash/NX3232_v1.80_Switch-A1.txt
/tftpboot/NX3232_v1.80_Switch-A1.txt          100% 5141      5.0KB/s
00:00
sftp> exit
Copy complete, now saving to disk (please wait)...
IP_switch_A_1#

```

b. Repeat the previous substep for each of the other three switches, being sure to copy the matching RCF file to the corresponding switch.

3. Verify on each switch that the RCF file is present in each switch's bootflash directory:

```
dir bootflash:
```

The following example shows that the files are present on IP_switch_A_1:

```

IP_switch_A_1# dir bootflash:
.
.
.
5514   Jun 13 22:09:05 2017  NX3232_v1.80_Switch-A1.txt
.
.
.

Usage for bootflash://sup-local
1779363840 bytes used
13238841344 bytes free
15018205184 bytes total
IP_switch_A_1#

```

4. Configure the TCAM regions on Cisco 3132Q-V and Cisco 3232C switches.



Skip this step if you do not have Cisco 3132Q-V or Cisco 3232C switches.

a. On Cisco 3132Q-V switch, set the following TCAM regions:

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

- b. On Cisco 3232C switch, set the following TCAM regions:

```
conf t
hardware access-list tcam region span 0
hardware access-list tcam region racl-lite 0
hardware access-list tcam region racl 256
hardware access-list tcam region e-racl 256
hardware access-list tcam region qos 256
```

- c. After setting the TCAM regions, save the configuration and reload the switch:

```
copy running-config startup-config
reload
```

5. Copy the matching RCF file from the local bootflash to the running configuration on each switch:

```
copy bootflash:switch-specific-RCF.txt running-config
```

6. Copy the RCF files from the running configuration to the startup configuration on each switch:

```
copy running-config startup-config
```

You should see output similar to the following:

```
IP_switch_A_1# copy bootflash:NX3232_v1.80_Switch-A1.txt running-config
IP_switch-A-1# copy running-config startup-config
```

7. Reload the switch:

```
reload
```

```
IP_switch_A_1# reload
```

8. Repeat the previous steps on the other three switches in the MetroCluster IP configuration.

Setting Forward Error Correction for systems using 25-Gbps connectivity

If your system is configured using 25-Gbps connectivity, you need to set the Forward Error Correction (fec) parameter manually to off after applying the RCF file. The RCF file does not apply this setting.

About this task

The 25-Gbps ports must be cabled prior to performing this procedure.

[Platform port assignments for Cisco 3232C or Cisco 9336C switches](#)

This task only applies to platforms using 25-Gbps connectivity:

- AFF A300
- FAS 8200
- FAS 500f
- AFF A250

This task must be performed on all four switches in the MetroCluster IP configuration.

Steps

1. Set the fec parameter to off on each 25-Gbps port that is connected to a controller module, and then copy the running configuration to the startup configuration:
 - a. Enter configuration mode: `conf t`
 - b. Specify the 25-Gbps interface to configure: `interface interface-ID`
 - c. Set fec to off: `fec off`
 - d. Repeat the previous steps for each 25-Gbps port on the switch.
 - e. Exit configuration mode: `exit`

The following example shows the commands for interface Ethernet1/25/1 on switch IP_switch_A_1:

```
IP_switch_A_1# conf t
IP_switch_A_1(config)# interface Ethernet1/25/1
IP_switch_A_1(config-if)# fec off
IP_switch_A_1(config-if)# exit
IP_switch_A_1(config-if)# end
IP_switch_A_1# copy running-config startup-config
```

2. Repeat the previous step on the other three switches in the MetroCluster IP configuration.

Disable unused ISL ports and port channels

NetApp recommends disabling unused ISL ports and port channels to avoid unnecessary health alerts.

1. Identify the unused ISL ports and port channels:

```
show interface brief
```

2. Disable the unused ISL ports and port channels.

You must run the following commands for each identified unused port or port channel.

```
SwitchA_1# config t
Enter configuration commands, one per line. End with CNTL/Z.
SwitchA_1(config)# int Eth1/14
SwitchA_1(config-if)# shutdown
SwitchA_12(config-if)# exit
SwitchA_1(config-if)# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
Copy complete.
```

Configure MACsec encryption on Cisco 9336C switches in a MetroCluster IP site

You can configure MACsec encryption on the WAN ISL ports that run between the sites. You must configure MACsec after applying the correct RCF file.



MACsec encryption can only be applied to the WAN ISL ports.

Configure MACsec encryption on Cisco 9336C switches

You must only configure MACsec encryption on the WAN ISL ports that run between the sites. You must configure MACsec after applying the correct RCF file.

Licensing requirements for MACsec

MACsec requires a security license. For a complete explanation of the Cisco NX-OS licensing scheme and how to obtain and apply for licenses, see the [Cisco NX-OS Licensing Guide](#)

Enable Cisco MACsec Encryption WAN ISLs in MetroCluster IP configurations

You can enable MACsec encryption for Cisco 9336C switches on the WAN ISLs in a MetroCluster IP configuration.

Steps

1. Enter global configuration mode:

```
configure terminal
```

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Enable MACsec and MKA on the device:

```
feature macsec
```

```
IP_switch_A_1(config)# feature macsec
```

3. Copy the running configuration to the startup configuration:

```
copy running-config startup-config
```

```
IP_switch_A_1(config)# copy running-config startup-config
```

Configure a MACsec key chain and keys

You can create a MACsec key chain or keys on your configuration.

Key Lifetime and Hitless Key Rollover

A MACsec keychain can have multiple pre-shared keys (PSKs), each configured with a key ID and an optional lifetime. A key lifetime specifies at which time the key activates and expires. In the absence of a lifetime configuration, the default lifetime is unlimited. When a lifetime is configured, MKA rolls over to the next configured pre-shared key in the keychain after the lifetime is expired. The time zone of the key can be local or UTC. The default time zone is UTC. A key can roll over to a second key within the same keychain if you configure the second key (in the keychain) and configure a lifetime for the first key. When the lifetime of the first key expires, it automatically rolls over to the next key in the list. If the same key is configured on both sides of the link at the same time, then the key rollover is hitless (that is, the key rolls over without traffic interruption).

Steps

1. Enter the global configuration mode:

```
configure terminal
```

```
IP_switch_A_1# configure terminal  
IP_switch_A_1(config)#
```

2. To hide the encrypted key octet string, replace the string with a wildcard character in the output of the `show running-config` and `show startup-config` commands:

```
IP_switch_A_1(config)# key-chain macsec-psk no-show
```



The octet string is also hidden when you save the configuration to a file.

By default, PSK keys are displayed in encrypted format and can easily be decrypted. This command applies only to MACsec key chains.

3. Create a MACsec key chain to hold a set of MACsec keys and enter MACsec key chain configuration mode:

```
key chain name macsec
```

```
IP_switch_A_1(config)# key chain 1 macsec  
IP_switch_A_1(config-macseckeychain)#
```

4. Create a MACsec key and enter MACsec key configuration mode:

```
key key-id
```

The range is from 1 to 32 hex digit key-string, and the maximum size is 64 characters.

```
IP_switch_A_1 switch(config-macseckeychain)# key 1000  
IP_switch_A_1 (config-macseckeychain-macseckey)#
```

5. Configure the octet string for the key:

```
key-octet-string octet-string cryptographic-algorithm AES_128_CMAC |  
AES_256_CMAC
```

```
IP_switch_A_1(config-macseckeychain-macseckey)# key-octet-string  
abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789  
cryptographic-algorithm AES_256_CMAC
```



The octet-string argument can contain up to 64 hexadecimal characters. The octet key is encoded internally, so the key in clear text does not appear in the output of the `show running-config macsec` command.

6. Configure a send lifetime for the key (in seconds):

```
send-lifetime start-time duration duration
```

```
IP_switch_A_1(config-macseckeychain-macseckey)# send-lifetime 00:00:00  
Oct 04 2020 duration 100000
```

By default, the device treats the start time as UTC. The start-time argument is the time of day and date that the key becomes active. The duration argument is the length of the lifetime in seconds. The maximum length is 2147483646 seconds (approximately 68 years).

7. Copy the running configuration to the startup configuration:

```
copy running-config startup-config
```

```
IP_switch_A_1(config)# copy running-config startup-config
```

8. Displays the keychain configuration:

```
show key chain name
```

```
IP_switch_A_1(config-macseckeychain-macseckey)# show key chain 1
```

Configure a MACsec policy

Steps

1. Enter global configuration mode:

```
configure terminal
```

```
IP_switch_A_1# configure terminal  
IP_switch_A_1(config)#
```

2. Create a MACsec policy:

```
macsec policy name
```

```
IP_switch_A_1(config)# macsec policy abc  
IP_switch_A_1(config-macsec-policy)#
```

3. Configure one of the following ciphers, GCM-AES-128, GCM-AES-256, GCM-AES-XPB-128, or GCM-AES-XPB-256:

```
cipher-suite name
```

```
IP_switch_A_1(config-macsec-policy)# cipher-suite GCM-AES-256
```

4. Configure the key server priority to break the tie between peers during a key exchange:

```
key-server-priority number
```

```
switch(config-macsec-policy)# key-server-priority 0
```

5. Configure the security policy to define the handling of data and control packets:

```
security-policy security policy
```

Choose a security policy from the following options:

- **must-secure** — packets not carrying MACsec headers are dropped

- should-secure — packets not carrying MACsec headers are permitted (this is the default value)

```
IP_switch_A_1(config-macsec-policy)# security-policy should-secure
```

6. Configure the replay protection window so the secured interface does not accept a packet that is less than the configured window size: `window-size number`



The replay protection window size represents the maximum out-of-sequence frames that MACsec accepts and are not discarded. The range is from 0 to 596000000.

```
IP_switch_A_1(config-macsec-policy)# window-size 512
```

7. Configure the time in seconds to force an SAK rekey:

```
sak-expiry-time time
```

You can use this command to change the session key to a predictable time interval. The default is 0.

```
IP_switch_A_1(config-macsec-policy)# sak-expiry-time 100
```

8. Configure one of the following confidentiality offsets in the layer 2 frame where encryption begins:

```
conf-offsetconfidentiality offset
```

Choose from the following options:

- CONF-OFFSET-0.
- CONF-OFFSET-30.
- CONF-OFFSET-50.

```
IP_switch_A_1(config-macsec-policy)# conf-offset CONF-OFFSET-0
```



This command might be necessary for intermediate switches to use packet headers (dmac, smac, etype) like MPLS tags.

9. Copy the running configuration to the startup configuration:

```
copy running-config startup-config
```

```
IP_switch_A_1(config)# copy running-config startup-config
```

10. Display the MACsec policy configuration:

```
show macsec policy
```

```
IP_switch_A_1(config-macsec-policy)# show macsec policy
```

Enable Cisco MACsec encryption on the interfaces

1. Enter global configuration mode:

```
configure terminal
```

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Select the interface that you configured with MACsec encryption.

You can specify the interface type and identity. For an Ethernet port, use ethernet slot/port.

```
IP_switch_A_1(config)# interface ethernet 1/15
switch(config-if)#
```

3. Add the keychain and policy to be configured on the interface to add the MACsec configuration:

```
macsec keychain keychain-name policy policy-name
```

```
IP_switch_A_1(config-if)# macsec keychain 1 policy abc
```

4. Repeat steps 1 and 2 on all interfaces where MACsec encryption is to be configured.
5. Copy the running configuration to the startup configuration:

```
copy running-config startup-config
```

```
IP_switch_A_1(config)# copy running-config startup-config
```

Disable Cisco MACsec Encryption WAN ISLs in MetroCluster IP configurations

You might need to disable MACsec encryption for Cisco 9336C switches on the WAN ISLs in a MetroCluster IP configuration.

Steps

1. Enter global configuration mode:

```
configure terminal
```

```
IP_switch_A_1# configure terminal
IP_switch_A_1(config)#
```

2. Disable the MACsec configuration on the device:

```
macsec shutdown
```

```
IP_switch_A_1(config)# macsec shutdown
```



Selecting the “no” option restores the MACsec feature.

3. Select the interface that you already configured with MACsec.

You can specify the interface type and identity. For an Ethernet port, use ethernet slot/port.

```
IP_switch_A_1(config)# interface ethernet 1/15
switch(config-if)#
```

4. Remove the keychain and policy configured on the interface to remove the MACsec configuration:

```
no macsec keychain keychain-name policy policy-name
```

```
IP_switch_A_1(config-if)# no macsec keychain 1 policy abc
```

5. Repeat steps 3 and 4 on all interfaces where MACsec is configured.
6. Copy the running configuration to the startup configuration:

```
copy running-config startup-config
```

```
IP_switch_A_1(config)# copy running-config startup-config
```

Verifying the MACsec configuration

Steps

1. Repeat **all** of the previous procedures on the second switch within the configuration to establish a MACsec session.
2. Run the following commands to verify that both switches are successfully encrypted:
 - a. Run: `show macsec mka summary`
 - b. Run: `show macsec mka session`
 - c. Run: `show macsec mka statistics`

You can verify the MACsec configuration using the following commands:

Command	Displays information about...
<code>show macsec mka session interface typeslot/port number</code>	The MACsec MKA session for a specific interface or for all interfaces
<code>show key chain name</code>	The key chain configuration
<code>show macsec mka summary</code>	The MACsec MKA configuration
<code>show macsec policy policy-name</code>	The configuration for a specific MACsec policy or for all MACsec policies

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.