Configure the MetroCluster IP switches

ONTAP MetroCluster

NetApp
September 12, 2021

Table of Contents

Configuring the IP switches 1
Configuring Broadcom IP switches 1
Resetting the Broadcom IP switch to factory defaults 1
Configure Cisco IP switches 11

Configuring the IP switches

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

Configuring Broadcom IP switches

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

Resetting the Broadcom IP switch to factory defaults

Before installing a new switch software version and RCFs, you must erase the Broadcom switch settings and perform basic configuration.

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. Change to the elevated command prompt (#):

   `enable`

   ```
   (Routing)> enable
   (Routing) #
   ```

2. Erase the startup configuration:

   `erase startup-config`

   ```
   (Routing) #erase startup-config
   Are you sure you want to clear the configuration? (y/n) y


   (Routing) #
   ```

   This command does not erase the banner.

3. Reboot the switch:

   `reload`

```
(IP_switch_A_1) #reload

Are you sure you would like to reset the system? (y/n) y
```

If the system asks whether to save the unsaved or changed configuration before reloading the switch, select **No**.

4. Wait for the switch to reload, and then log in to the switch.

   The default user is “admin”, and no password is set. A prompt similar to the following is displayed:

```
(Routing)>
```

5. Change to the elevated command prompt:

   `enable`

```
Routing)> enable
(Routing) #
```

6. Set the service port protocol to `none`:

   `serviceport protocol none`

```
(Routing) #serviceport protocol none
Changing protocol mode will reset ip configuration.
Are you sure you want to continue? (y/n) y

(Routing) #
```

7. Assign the IP address to the service port:

   `serviceport ip` *`ip-address netmask gateway`*

   The following example shows a service port assigned IP address "10.10.10.10" with subnet "255.255.255.0" and gateway "10.10.10.1":

```
(Routing) #serviceport ip 10.10.10.10 255.255.255.0 10.10.10.1
```

8. Verify that the service port is correctly configured:

   `show serviceport`

   The following example shows that the port is up and the correct addresses have been assigned:

```
(Routing) #show serviceport

Interface Status.............................. Up
IP Address.................................... 10.10.10.10
Subnet Mask................................... 255.255.255.0
Default Gateway............................... 10.10.10.1
IPv6 Administrative Mode...................... Enabled
IPv6 Prefix is ..............................
fe80::dac4:97ff:fe56:87d7/64
IPv6 Default Router........................... fe80::222:bdff:fef8:19ff
Configured IPv4 Protocol...................... None
Configured IPv6 Protocol...................... None
IPv6 AutoConfig Mode.......................... Disabled
Burned In MAC Address......................... D8:C4:97:56:87:D7

(Routing) #
```

9. If desired, configure the SSH server.

   The RCF file disables the Telnet protocol. If you do not configure the SSH server, you can only access the bridge using the serial port connection.

   a. Generate RSA keys.

   ```
   (Routing) #configure
   (Routing) (Config)#crypto key generate rsa
   ```

   b. Generate DSA keys.

   ```
   (Routing) #configure
   (Routing) (Config)#crypto key generate dsa
   ```

   c. Enable the SSH server.

   If necessary, exit the configuration context.

   ```
   (Routing) (Config)#end
   (Routing) #ip ssh server enable
   ```

   If keys already exist, then you might be asked to overwrite them.

10. If desired, configure the domain and name server:

```
configure
```

The following example shows the `ip domain` and `ip name server` commands:

```
(Routing) # configure
(Routing) (Config)#ip domain name lab.netapp.com
(Routing) (Config)#ip name server 10.99.99.1 10.99.99.2
(Routing) (Config)#exit
(Routing) (Config)#
```

11. If desired, configure the time zone and time synchronization (SNTP).

    The following example shows the `sntp` commands, specifying the IP address of the SNTP server and the relative time zone.

```
(Routing) #
(Routing) (Config)#sntp client mode unicast
(Routing) (Config)#sntp server 10.99.99.5
(Routing) (Config)#clock timezone -7
(Routing) (Config)#exit
(Routing) (Config)#
```

12. Configure the switch name:

    ```
    hostname IP_switch_A_1
    ```

    The switch prompt will display the new name:

```
(Routing) # hostname IP_switch_A_1

(IP_switch_A_1) #
```

13. Save the configuration:

    ```
    write memory
    ```

    You receive prompts and output similar to the following example:

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y

Config file 'startup-config' created successfully .


Configuration Saved!

(IP_switch_A_1) #
```

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

Downloading and installing the Broadcom switch EFOS 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 must be repeated on each switch in the MetroCluster IP configuration.

Steps

1. Copy the switch software to the switch:

   ```
   copy sftp://user@50.50.50.50/switchsoftware/efos-3.4.3.1.stk backup
   ```

   In this example, the "efos-3.4.3.1.stk" operating system file is copied from the SFTP server at "50.50.50.50" to the backup partition. You need to 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://user@50.50.50.50/switchsoftware/efos-
3.4.3.1.stk backup
Remote Password:*************

Mode..................................... SFTP
Set Server IP.................................. 50.50.50.50
Path..................................... /switchsoftware/
Filename..................................... efos-3.4.3.1.stk
Data Type.................................... Code
Destination Filename........................... backup

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
SFTP Code transfer starting...


File transfer operation completed successfully.

(IP_switch_A_1) #
```

2. Set the switch to boot from the backup partition on the next switch reboot:

   `boot system backup`

```
(IP_switch_A_1) #boot system backup
Activating image backup ..

(IP_switch_A_1) #
```

3. Verify that the new boot image will be active on the next boot:

   `show bootvar`

```
(IP_switch_A_1) #show bootvar

Image Descriptions

 active :
 backup :


 Images currently available on Flash

 ----  -----------  --------  ---------------  ------------
 unit       active    backup   current-active   next-active
 ----  -----------  --------  ---------------  ------------

    1       3.4.3.0      3.4.3.1      3.4.3.0          3.4.3.1

(IP_switch_A_1) #
```

4. Save the configuration:

   `write memory`

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y


Configuration Saved!

(IP_switch_A_1) #
```

5. Reboot the switch:

   `reload`

```
(IP_switch_A_1) #reload

Are you sure you would like to reset the system? (y/n) y
```

6. Wait for the switch to reboot.
7. Repeat these steps on the remaining three IP switches in the MetroCluster IP configuration.

Downloading and installing the Broadcom RCF files

You must download and install the switch 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.

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	BES-53248_v1.32_Switch-A1.txt
IP_switch_A_2	BES-53248_v1.32_Switch-A2.txt
IP_switch_B_1	BES-53248_v1.32_Switch-B1.txt
IP_switch_B_2	BES-53248_v1.32_Switch-B2.txt

Steps

1. Download the MetroCluster IP RCF files for the Broadcom switch.

   Broadcom Cluster and Management Network Switch Reference Configuration File Download for MetroCluster IP

2. Copy the RCF files to the switches:

   a. Copy the RCF files to the first switch: `copy sftp://user@FTP-server-IP-address/RcfFiles/switch-specific-RCF nvram:script BES-53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr`

      In this example, the "BES-53248_v1.32_Switch-A1.txt" RCF file is copied from the SFTP server at "50.50.50.50" to the local bootflash. You need to 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://user@50.50.50.50/RcfFiles/BES-
53248_v1.32_Switch-A1.txt nvram:script BES-53248_v1.32_Switch-A1.scr

Remote Password:*************

Mode..................................... SFTP
Set Server IP.................................. 50.50.50.50
Path..................................... /RcfFiles/
Filename..................................... BES-
53248_v1.32_Switch-A1.txt
Data Type.................................... Config Script
Destination Filename......................... BES-
53248_v1.32_Switch-A1.scr

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the
duration of the transfer. Please wait...
File transfer operation completed successfully.


Validating configuration script...

config

set clibanner
"************************************************************************
************

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248


...
The downloaded RCF is validated. Some output is being logged here.
...


Configuration script validated.
File transfer operation completed successfully.

(IP_switch_A_1) #
```

b. Verify that the RCF file is saved as a script:

```
script list
```

```
(IP_switch_A_1) #script list

Configuration Script Name        Size(Bytes)  Date of Modification
-------------------------------  -----------  --------------------
BES-53248_v1.32_Switch-A1.scr            852   2019 01 29 18:41:25

1 configuration script(s) found.
2046 Kbytes free.
(IP_switch_A_1) #
```

c. Apply the RCF script:

```
script apply BES-53248_v1.32_Switch-A1.scr
```

```
(IP_switch_A_1) #script apply BES-53248_v1.32_Switch-A1.scr

Are you sure you want to apply the configuration script? (y/n) y


config

set clibanner
"**********************************************************************
************

* NetApp Reference Configuration File (RCF)

*

* Switch    : BES-53248

...
The downloaded RCF is validated. Some output is being logged here.
...

Configuration script 'BES-53248_v1.32_Switch-A1.scr' applied.

(IP_switch_A_1) #
```

d. Save the configuration:

```
write memory
```

```
(IP_switch_A_1) #write memory

This operation may take a few minutes.
Management interfaces will not be available during this time.

Are you sure you want to save? (y/n) y


Configuration Saved!

(IP_switch_A_1) #
```

e. Reboot the switch:

`reload`

```
(IP_switch_A_1) #reload

Are you sure you would like to reset the system? (y/n) y
```

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

3. Reload the switch:

`reload`

```
IP_switch_A_1# reload
```

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

Configure Cisco IP switches

Configuring Cisco IP switches

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

Resetting the Cisco IP switch to factory defaults

Before installing a new software version and RCFs, you must erase the Cisco switch configuration and perform basic configuration.

About this task

You must repeat these steps on each of the IP switches in the MetroCluster IP configuration.

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.

```
Would you like to enter the basic configuration dialog (yes/no): yes
  Create another login account (yes/no) [n]:
  Configure read-only SNMP community string (yes/no) [n]:
  Configure read-write SNMP community string (yes/no) [n]:
  Enter the switch name : switch-name **<<<**
  Continue with Out-of-band (mgmt0) management configuration?
(yes/no) [y]:
    Mgmt0 IPv4 address : management-IP-address  **<<<**
    Mgmt0 IPv4 netmask : management-IP-netmask  **<<<**
  Configure the default gateway? (yes/no) [y]: y **<<<**
    IPv4 address of the default gateway : gateway-IP-address  **<<<**
  Configure advanced IP options? (yes/no) [n]:
  Enable the telnet service? (yes/no) [n]:
  Enable the ssh service? (yes/no) [y]: y  **<<<**
    Type of ssh key you would like to generate (dsa/rsa) [rsa]: rsa
**<<<**
    Number of rsa key bits <1024-2048> [1024]:
  Configure the ntp server? (yes/no) [n]:
  Configure default interface layer (L3/L2) [L2]:
  Configure default switchport interface state (shut/noshut)
[noshut]: shut **<<<**
  Configure CoPP system profile (strict/moderate/lenient/dense)
[strict]:
```

The final set of prompts completes the configuration:

```
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 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)...
   ```

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       Image   Running-Version(pri:alt)         New-Version   Upg-
Required
------  ----------   ------------------------  ------------------
------------
     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. Repeat these steps on the remaining three IP switches in the MetroCluster IP configuration.

Downloading and installing the Cisco IP RCF files

You must download 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

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. Download the MetroCluster IP RCF files from the MetroCluster RCF download page.
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. Copy the matching RCF file from the local bootflash to the running configuration on each switch:

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

5. 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
   ```

6. Reload the switch:

   ```
   reload
   ```

   ```
   IP_switch_A_1# reload
   ```

7. Repeat the previous steps on the other three switches in the MetroCluster IP configuration. == Configuring 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

Enabling 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 the 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
   ```

Disabling 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 the 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, policy, and fallback-keychain configured on the interface to remove the MACsec configuration:

   `no macsec keychain` *`keychain-name`* `policy` *`policy-name`* `fallback-keychain` *`fallback-keychain-name`*

```
IP_switch_A_1(config-if)# no macsec keychain kc2 policy abc fallback-
keychain fb_kc2
```

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
```

Configuring a MACsec key chain and keys

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

About this task

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).

Fallback Key

A MACsec session can fail due to a key/key name (CKN) mismatch or a finite key duration between the switch and a peer. If a MACsec session does fail, a fallback session can take over if a fallback key is configured. A fallback session prevents downtime due to primary session failure and allows a user time to fix the key issue causing the failure. A fallback key also provides a backup session if the primary session fails to start. This feature is optional.

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. Display the keychain configuration:

   `show keychain name`

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

Configuring a MACsec policy

Steps

1. Enter the 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-XPN-128
   - GCM-AES-XPN-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
    ```

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:

   `show macsec mka summary`

```
show macsec mka session

show macsec mka statistics
```

You can verify the MACsec configuration using the following commands:

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

Configuring a MACsec fallback key on a WAN ISL port

You can configure a fallback key to initiate a backup session if the primary session fails as a result of a key/key name (CKN) mismatch or a finite key duration between the switch and peer.

Steps

1. Enter the global configuration mode:

   ```
   configure terminal
   ```

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

2. Specify the interface that you are configuring.

   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. Specify the fallback key chain for use after a MACsec session failure due to a key/key ID mismatch or a key expiration:

   `macsec keychain` *`keychain-name`* `policy` *`policy-name`* `fallback-keychain` *`fallback-keychain-name`*

   > You should configure the fallback-keychain using the steps, Configuring a MACsec key chain and keys before proceeding with this step.

```
IP_switch_A_1(config-if)# macsec keychain kc2 policy abc fallback-
keychain fb_kc2
```

4. Repeat the previous steps to configure additional WAN ISL ports with MACsec.
5. Copy the running configuration to the startup configuration:

   `copy running-config startup-config`

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

Setting Forward Error Correction for and 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.

Before you begin

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

Platform port assignments for Cisco 3232C or Cisco 9336C switches

About this task

This task only applies to AFF A300 and FAS8200 platforms using 25-Gbps connectivity.

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:

      `config t`

   b. Specify the 25-Gbps interface you want 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.

Configuring MACsec encryption on Cisco 9336C switches

If desired, 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.

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

Enabling 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.

1. Enter the 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
```

Disabling Cisco MACsec Encryption

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

If you disable encryption, you must also delete your keys, as described in XXX.

1. Enter the 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, policy and fallback-keychain configured on the interface to remove the MACsec configuration: `no macsec keychain keychain-name policy policy-name fallback-keychain keychain-name`

```
IP_switch_A_1(config-if)# no macsec keychain kc2 policy abc fallback-
keychain fb_kc2
```

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
```

Configuring a MACsec key chain and keys

For details on configuring a MACsec key chain, see the Cisco documentation for your switch.