配置 Cisco IP 交换机

ONTAP MetroCluster

NetApp
February 13, 2026

目录

配置 Cisco IP 交换机

配置Cisco IP 交换机以实现集群互连和后端MetroCluster IP 连接

您必须将 Cisco IP 交换机配置为用作集群互连以及用于后端 MetroCluster IP 连接。

关于此任务

本节中的几个过程是独立的，您只需执行引导到您或与您的任务相关的过程即可。

将 Cisco IP 交换机重置为出厂默认值

在安装任何 RCF 文件之前，您必须擦除 Cisco 交换机配置并执行基本配置。如果要在先前安装失败后重新安装同一个 RCF 文件，或者要安装新版本的 RCF 文件，则需要此操作步骤 。

关于此任务

- 您必须对 MetroCluster IP 配置中的每个 IP 交换机重复这些步骤。
- 您必须使用串行控制台连接到交换机。
- 此任务将重置管理网络的配置。

步骤

1. 将交换机重置为出厂默认设置：

   a. 擦除现有配置：

      写入擦除

   b. 重新加载交换机软件：

      `re`负载

      系统将重新启动并进入配置向导。在启动期间，如果您收到提示 "`Abort Auto Provisioning and continue with normal setup ？（是 / 否） [n]` " ，您应回答 是 以继续。

   c. 在配置向导中，输入基本交换机设置：

      - 管理员密码
      - 交换机名称
      - 带外管理配置
      - 默认网关
      - SSH 服务（ RSA ）

        完成配置向导后，交换机将重新启动。

   d. 出现提示时，输入用户名和密码以登录到交换机。

以下示例显示了配置交换机时的提示和系统响应。尖括号（` <<<` ）显示信息的输入位置。

```
---- 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.
```

您可以在下一组提示中输入基本信息，包括交换机名称，管理地址和网关，然后选择 SSH with RSA 。

> 此示例显示了配置RC框架 所需的最低信息、在应用RC框架 后、可以配置其他选项。例如、您可以在应用RCP后配置SNMPv3、NTP或SCP或SFTP。

```
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]:
```

最后一组提示将完成配置：

```
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. 保存配置：

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

3. 重新启动交换机并等待交换机重新加载：

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

4. 对 MetroCluster IP 配置中的其他三台交换机重复上述步骤。

下载并安装 **Cisco** 交换机 **NX-OS** 软件

您必须将交换机操作系统文件和 RCF 文件下载到 MetroCluster IP 配置中的每个交换机。

关于此任务

此任务需要使用文件传输软件，例如 FTP ， TFTP ， SFTP 或 SCP ， 将文件复制到交换机。

必须对 MetroCluster IP 配置中的每个 IP 交换机重复执行这些步骤。

您必须使用支持的交换机软件版本。

"NetApp Hardware Universe"

步骤

1. 下载支持的 NX-OS 软件文件。

   "Cisco 软件下载"

2. 将交换机软件复制到交换机：

   ```
   copy sftp ： //root@server-IP-address/tftpboot/NX-os-file-name bootflash ： vRF
   management
   ```

   在本例中，nxos.7.0.3.I4.6.bin 文件和 EPLD 映像从 SFTP 服务器 10.10.99.99 复制到本地 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. 在每个交换机上验证交换机 NX-OS 文件是否位于每个交换机的 bootflash 目录中：

   d的 `bootflash` ：

   以下示例显示文件位于 ip_switch_A_1 上：

```
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. 安装交换机软件：

   安装所有 `nxos bootflash ： nxos.version-number.bin`

   安装交换机软件后，交换机将自动重新加载（重新启动）。

   以下示例显示了 IP_switch_A_1 上的软件安装：

```
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. 等待交换机重新加载，然后登录到交换机。

交换机重新启动后，将显示登录提示：

```
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. 验证是否已安装交换机软件： + `show version`

以下示例显示了输出：

```
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. 升级 EPLD 映像并重新启动交换机。

```
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.
```

8. 在交换机重新启动后，再次登录并验证是否已成功加载新版本的 EPLD 。

   ```
   show version module 1 epld
   ```

9. 对 MetroCluster IP 配置中的其余三个 IP 交换机重复上述步骤。

下载并安装 **Cisco IP RCF** 文件

您必须为MetroCluster IP配置中的每个交换机生成并安装RCF文件。

关于此任务

此任务需要使用文件传输软件，例如 FTP ， TFTP ， SFTP 或 SCP ， 将文件复制到交换机。

必须对 MetroCluster IP 配置中的每个 IP 交换机重复执行这些步骤。

您必须使用支持的交换机软件版本。

"NetApp Hardware Universe"

如果您使用的是QSFP-SFP+适配器、则可能需要将ISL端口配置为本机速度模式、而不是分支速度模式。请参见交换机供应商文档以确定ISL端口速度模式。

有四个 RCF 文件， MetroCluster IP 配置中的四个交换机中的每个交换机一个。您必须为所使用的交换机型号使用正确的 RCF 文件。

交换机	RCF 文件
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

步骤

1. 为MetroCluster IP生成Cisco RCC文件。
   a. 下载 "适用于 MetroCluster IP 的 RcfFileGenerator"
   b. 使用适用于MetroCluster IP的RcfFileGenerator为您的配置生成RCF文件。

      不支持在下载后修改RCF文件。

2. 将 RCF 文件复制到交换机：
   a. 将 RCF 文件复制到第一个交换机：

      ```
      copy sftp ： //root@ftp-server-ip-address/tftpboot/switch-specific — rCF
      bootflash ： vrf management
      ```

      在此示例中， NX3232_v1.80_Switch-A1.txt RCF 文件将从位于 10.10.99.99 的 SFTP 服务器复制到本地 bootflash 。您必须使用 TFTP/SFTP 服务器的 IP 地址以及需要安装的 RCF 文件的文件名。

```
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#
```

a. 对其他三个交换机中的每一个交换机重复上述子步骤，确保将匹配的 RCF 文件复制到相应的交换机。

3. 在每个交换机上验证 RCF 文件是否位于每个交换机的 bootflash 目录中：

d的 `bootflash` ：

以下示例显示文件位于 ip_switch_A_1 上：

```
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. 在 Cisco 3132Q-V 和 Cisco 3232C 交换机上配置 TCAM 区域。

如果您没有 Cisco 3132Q-V 或 Cisco 3232C 交换机，请跳过此步骤。

a. 在 Cisco 3132Q-V 交换机上，设置以下 TCAM 区域：

```
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. 在 Cisco 3232C 交换机上，设置以下 TCAM 区域：

```
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. 设置 TCAM 区域后，保存配置并重新加载交换机：

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

5. 将匹配的 RCF 文件从本地 bootflash 复制到每个交换机上的运行配置：

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

6. 将 RCF 文件从正在运行的配置复制到每个交换机上的启动配置：

   `copy running-config startup-config`

   您应看到类似于以下内容的输出：

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

7. 重新加载交换机：

   `re`负载

```
IP_switch_A_1# reload
```

8. 对 MetroCluster IP 配置中的其他三台交换机重复上述步骤。

为使用 25 Gbps 连接的系统设置正向错误更正

如果您的系统配置为使用 25 Gbps 连接，则在应用 RCF 文件后，您需要手动将正向错误更正（ FEC ）参数设置为关闭。RCF 文件不应用此设置。

关于此任务

在执行此操作步骤之前，必须为 25 Gbps 端口布线。

"Cisco 3232C 或 Cisco 9336C 交换机的平台端口分配"

此任务仅限使用 25-Gbps 连接的适用场景 平台：

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

必须对 MetroCluster IP 配置中的所有四台交换机执行此任务。

步骤

1. 在连接到控制器模块的每个 25 Gbps 端口上将 FEC 参数设置为 off ，然后将正在运行的配置复制到启动配置：

   a. 进入配置模式： `config t`

   b. 指定要配置的 25-Gbps 接口： `interface interface-ID`

   c. 将 FEC 设置为 off： `fEC off`

   d. 对交换机上的每个 25 Gbps 端口重复上述步骤。

   e. 退出配置模式： `exit`

   以下示例显示了针对交换机 IP_switch_A_1 上的接口 Ethernet1/2/1 的命令：

```
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. 对 MetroCluster IP 配置中的其他三台交换机重复上述步骤。

禁用未使用的ISL端口和端口通道

NetApp建议禁用未使用的ISL端口和端口通道、以避免发出不必要的运行状况警报。

1. 确定未使用的ISL端口和端口通道：

s如何使用接口简介

2. 禁用未使用的ISL端口和端口通道。

   您必须对每个已确定的未使用端口或端口通道运行以下命令。

```
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.
```

在MetroCluster IP 站点中的Cisco 9336C 交换机上配置 MACsec 加密

MACsec 加密只能应用于 WAN ISL 端口。

在 Cisco 9336C 交换机上配置 MACsec 加密

您只能在站点之间运行的 WAN ISL 端口上配置 MACsec 加密。在应用正确的 RCF 文件后，您必须配置 MACsec 。

MAC 的许可要求

MACsec 需要安全许可证。有关 Cisco NX-OS 许可方案以及如何获取和申请许可证的完整说明，请参见 "《Cisco NX-OS 许可指南》"

在MetroCluster IP配置中启用Cisco MACsec加密WAN ISL

您可以在 MetroCluster IP 配置中为 WAN ISL 上的 Cisco 9336C 交换机启用 MACsec 加密。

步骤

1. 进入全局配置模式：

   配置终端

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

2. 在设备上启用 MACsec 和 MKA：

功能 `MACsec`

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

3. 将正在运行的配置复制到启动配置：

   `copy running-config startup-config`

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

配置MACsec密钥链和密钥

您可以在配置上创建一个或多个 MACsec 密钥链。

- 密钥生命周期和无结果密钥滚动 *

一个 MACsec 密钥链可以具有多个预共享密钥（ PSK ），每个密钥都配置有一个密钥 ID 和一个可选的生命周期。密钥生命周期用于指定密钥激活和到期的时间。如果没有生命周期配置，则默认生命周期为无限制。如果配置了生命周期，则在生命周期到期后， MKA 将转至密钥链中的下一个已配置的预共享密钥。密钥的时区可以是本地或 UTC 。默认时区为 UTC 。如果配置第二个密钥（在密钥链中）并为第一个密钥配置有效期，则密钥可以滚动到同一个密钥链中的第二个密钥。当第一个密钥的生命周期到期时，它会自动滚动到列表中的下一个密钥。如果在链路两端同时配置了同一个密钥，则密钥滚动将无中断（即，密钥在不中断流量的情况下进行回滚）。

步骤

1. 进入全局配置模式：

   配置终端

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

2. 要隐藏加密的密钥八位字节字符串，请在 `show running-config` and `show startup-config` 命令的输出中将此字符串替换为通配符：

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

   将配置保存到文件时，八位组字符串也会隐藏。

   默认情况下， psk 密钥以加密格式显示，并且可以轻松解密。此命令仅适用于 MACsec 密钥链。

3. 创建一个 MACsec 密钥链以存放一组 MACsec 密钥并进入 MACsec 密钥链配置模式：

   密钥链名称 `MACsec`

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

4. 创建一个 MACsec 密钥并进入 MACsec 密钥配置模式：

   `key key-id`

   此范围为 1 到 32 个十六进制数字键字符串，最大大小为 64 个字符。

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

5. 配置密钥的八位字节字符串：

   `key-octet-string octet-string Cryptographic -orl AES-128_CMAC` AES_256_CMAC

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

   八位字节字符串参数最多可包含 64 个十六进制字符。八位字节密钥在内部进行编码，因此明文形式的密钥不会显示在 `show running-config MACsec` 命令的输出中。

6. 配置密钥的发送生命周期（以秒为单位）：

   s终生开始时间持续时间

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

   默认情况下，设备会将开始时间视为 UTC 。start-time 参数是密钥生效的日期和日期时间。duration 参数是指以秒为单位的生命周期长度。最大长度为 2147483646 秒（约为 68 年）。

7. 将正在运行的配置复制到启动配置：

   `copy running-config startup-config`

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

8. 显示密钥链配置：

   s如何使用密钥链名称

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

配置MAC秒策略

步骤

1. 进入全局配置模式：

   配置终端

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

2. 创建 MAC 秒策略：

   mAcSEC 策略名称

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

3. 配置以下密码之一 GCM-AES-128 ， GCM-AES-256 ， GCM-AES-XPN-128 或 GCM-AES-XPN-256 ：

   密码套件名称

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

4. 配置密钥服务器优先级，以便在密钥交换期间中断对等方之间的联系：

   key-server-priority number

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

5. 配置安全策略以定义数据和控制数据包的处理方式：

   s安全策略安全策略

   从以下选项中选择一个安全策略：

   - must secure —未传输 MAC 秒标头的数据包将被丢弃
   - should secure —允许未传输 MAC 秒标头的数据包（这是默认值）

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

6. 配置重放保护窗口，使安全接口不接受小于配置窗口大小的数据包： `window-size number`

   重放保护窗口大小表示 MACsec 接受且不丢弃的序列外帧的最大数量。范围为 0 到 596000000 。

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

7. 配置强制重新设置 SAK 密钥的时间（以秒为单位）：

   `sAK` 到期时间

   您可以使用此命令将会话密钥更改为可预测的时间间隔。默认值为 0 。

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

8. 在开始加密的第 2 层帧中配置以下机密性偏移之一：

   `conf-offsetconfidentiality offset`

   从以下选项中进行选择：

   - CONF 偏移 -0 。
   - CON-offset-30 。
   - CONF 偏移 -50 。

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

     中间交换机可能需要使用此命令来使用 MPLS 标记等数据包标头（ DMAC ， SMaC ， etype ）。

9. 将正在运行的配置复制到启动配置：

   `copy running-config startup-config`

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

10. 显示 MACsec 策略配置：

    s如何使用 `MACsec` 策略

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

在接口上启用**Cisco MACsec**加密

1. 进入全局配置模式：

   配置终端

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

2. 选择使用MAC秒加密配置的接口。

   您可以指定接口类型和标识。对于以太网端口，请使用以太网插槽 / 端口。

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

3. 添加要在接口上配置的密钥链和策略以添加MACsec配置：

   ```
   mAcSEC keychain keychain-name policy policy-name
   ```

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

4. 对要配置MACsec加密的所有接口重复步骤1和2。
5. 将正在运行的配置复制到启动配置：

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

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

在**MetroCluster IP**配置中禁用**Cisco MACsec**加密**WAN ISL**

在 MetroCluster IP 配置中，您可能需要对 WAN ISL 上的 Cisco 9336C 交换机禁用 MACsec 加密。

步骤

1. 进入全局配置模式：

   配置终端

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

2. 在设备上禁用 MACsec 配置：

mAcSEC shutdown

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

选择 "`no` " 选项可还原 MACsec 功能。

3. 选择已配置 MAC 的接口。

   您可以指定接口类型和标识。对于以太网端口，请使用以太网插槽 / 端口。

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

4. 删除接口上配置的密钥链和策略以删除MACsec配置：

   no MACsec keychain keychain-name policy policy-name

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

5. 对配置了 MACsec 的所有接口重复步骤 3 和 4 。
6. 将正在运行的配置复制到启动配置：

   copy running-config startup-config

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

验证 **MACsec** 配置

步骤

1. 在配置中的第二台交换机上重复上述所有过程以建立 MACsec 会话。
2. 运行以下命令以验证这两个交换机是否已成功加密：

   a. Run： s如何执行 MACsec MKA 摘要

   b. Run： s如何执行 MACsec MKA 会话

   c. Run： s如何处理 MACsec MKA 统计信息

   您可以使用以下命令验证 MACsec 配置：

命令	显示有关 … 的信息

s如何使用 `MACsec MKA` 会话接口键入 `lot/` 端口号	特定接口或所有接口的 MACsec MKA 会话
s如何使用密钥链名称	密钥链配置
s如何执行 `MACsec MKA` 摘要	MACsec MKA 配置
s如何使用 `MACsec policy policy-name`	特定 MACsec 策略或所有 MACsec 策略的配置