Cisco IP スイッチを設定する

ONTAP MetroCluster

NetApp
April 25, 2024

目次

Cisco IP スイッチを設定する

Cisco IP スイッチの設定

クラスタインターコネクトおよびバックエンド MetroCluster IP 接続用に Cisco IP スイッチを設定する必要があります。

このタスクについて

このセクションの手順のいくつかは独立した手順であり、実行する必要があるのは自分がタスクに指示された手順、またはタスクに関連する手順のみです。

Cisco IP スイッチを工場出荷時のデフォルトにリセットする

RCF ファイルをインストールする前に、 Cisco スイッチの設定を消去し、基本的な設定を完了する必要があります。この手順 は、以前のインストールに失敗したあとに同じ RCF ファイルを再インストールする場合、または新しいバージョンのファイルをインストールする場合に必要です。

このタスクについて

- この手順は、 MetroCluster IP 構成の各 IP スイッチで実行する必要があります。
- シリアルコンソールを使用してスイッチに接続する必要があります。
- このタスクでは、管理ネットワークの設定をリセットします。

手順

1. スイッチを工場出荷時のデフォルトにリセットします。

   a. 既存の設定を消去します。

      「 write erase 」を入力します

   b. スイッチソフトウェアをリロードします。

      「再ロード」

      システムがリブートし、設定ウィザードが表示されます。起動中に「 Abort Auto Provisioning and continue with normal setup ？」というプロンプトが表示された場合は、(yes/no)[n]`" 、続行するには 'yes' と応答する必要があります。

   c. 設定ウィザードで、スイッチの基本設定を入力します。

      - 管理パスワード
      - スイッチ名
      - アウトオブバンド管理設定
      - デフォルトゲートウェイ
      - SSH サービス（ RSA ）

        設定ウィザードが完了すると、スイッチがリブートします。

d. プロンプトが表示されたら、ユーザ名とパスワードを入力してスイッチにログインします。

次の例は、スイッチを設定する際のプロンプトとシステム応答を示しています。山括弧（「 <<<`) 」）は、情報を入力する場所を示します。

```
---- 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.
```

次の一連のプロンプトで、スイッチ名、管理アドレス、ゲートウェイなどの基本情報を入力し、 SSH with RSA を選択します。

```
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]:
```

最後の一連のプロンプトで設定が完了します。

```
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. 設定を保存します。

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

3. スイッチをリブートし、スイッチがリロードされるまで待ちます。

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

4. MetroCluster IP 構成の他の 3 つのスイッチについて、上記の手順を繰り返します。

Cisco スイッチの NX-OS ソフトウェアのダウンロードとインストール

MetroCluster IP 構成の各スイッチにスイッチのオペレーティングシステムファイルと RCF ファイルをダウンロードする必要があります。

このタスクについて

この作業には、 FTP 、 TFTP 、 SFTP 、 SCP などのファイル転送ソフトウェアが必要です。 ファイルをスイッチにコピーします。

この手順は、 MetroCluster IP 構成の各 IP スイッチで実行する必要があります。

サポートされているバージョンのスイッチソフトウェアを使用する必要があります。

"NetApp Hardware Universe の略"

手順

1. サポートされている NX-OS ソフトウェアファイルをダウンロードします。

   "シスコソフトウェアのダウンロード"

2. スイッチソフトウェアをスイッチにコピーします。

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

   この例では、 nxos.7.0.3.I4.6.bin ファイルを SFTP サーバ 10.10.99.99 からローカルブートフラッシュにコピーしています。

```
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. 各スイッチの bootflash ディレクトリにスイッチの NX-OS ファイルがあることを確認します。

   「 IR bootflash: 」のように表示されます

   次の例は、 FC_switch_A_1 にファイルが存在することを示しています。

```
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. スイッチソフトウェアをインストールします。

   すべての nxos bootflash:nxos.version-number.bin をインストールします

   スイッチソフトウェアがインストールされると、スイッチは自動的にリロード（リブート）します。

   次の例は、 FC_switch_A_1 へのソフトウェアのインストールを示しています。

```
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. スイッチがリロードされるまで待ってから、スイッチにログインします。

スイッチがリブートされると、ログインプロンプトが表示されます。

```
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. スイッチソフトウェアがインストールされていることを確認します :+`show version`

   次の例は、の出力を示しています。

```
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. MetroCluster IP 構成の残りの 3 つの IP スイッチについて、上記の手順を繰り返します。

Cisco IP RCF ファイルのダウンロードとインストール

MetroCluster IP 構成の各スイッチに RCF ファイルをダウンロードする必要があります。

このタスクについて

この作業には、 FTP 、 TFTP 、 SFTP 、 SCP などのファイル転送ソフトウェアが必要です。 ファイルをスイッチにコピーします。

この手順は、 MetroCluster IP 構成の各 IP スイッチで実行する必要があります。

サポートされているバージョンのスイッチソフトウェアを使用する必要があります。

"NetApp Hardware Universe の略"

RCF ファイルは 4 つあり、それぞれが MetroCluster IP 構成の 4 つの各スイッチに対応しています。使用するスイッチのモデルに対応した正しい RCF ファイルを使用する必要があります。

スイッチ	RCF ファイル
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

手順

1. MetroCluster IP の RCF ファイルをダウンロードします。

   ダウンロード後にRCFファイルを変更することはできません。

2. RCF ファイルをスイッチにコピーします。

   a. RCF ファイルを最初のスイッチにコピーします。

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

      この例では、 NX3232_v1.80_Switch-A1.txt RCF ファイルを SFTP サーバの 10.10.99.99 からローカルブートフラッシュにコピーしています。使用する TFTP / SFTP サーバの IP アドレスと、インストールする必要がある RCF ファイルのファイル名を使用する必要があります。

```
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. 残りの 3 つのスイッチのそれぞれについて、同じ手順を繰り返します。それぞれのスイッチに対応する RCF ファイルをコピーするように注意してください。

3. 各スイッチの bootflash ディレクトリに RCF ファイルがあることを確認します。

「 IR bootflash: 」のように表示されます

次の例は、 FC_switch_A_1 にファイルが存在することを示しています。

```
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. Cisco 3132Q-V および Cisco 3232C スイッチの TCAM リージョンを設定します。

> Cisco 3132Q-V または Cisco 3232C スイッチを使用していない場合は、この手順を省略します。

a. Cisco 3132Q-V スイッチで、次の TCAM リージョンを設定します。

```
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. Cisco 3232C スイッチで、次の TCAM リージョンを設定します。

```
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. TCAM リージョンを設定したら、設定を保存してスイッチをリロードします。

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

5. 各スイッチで、対応する RCF ファイルをローカルブートフラッシュから実行中の設定にコピーします。

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

6. 各スイッチで、実行中の設定からスタートアップ設定に RCF ファイルをコピーします。

   'copy running-config startup-config

   次のような出力が表示されます。

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

7. スイッチをリロードします。

   「再ロード」

```
IP_switch_A_1# reload
```

8. MetroCluster IP 構成の他の 3 つのスイッチについて、上記の手順を繰り返します。

25Gbps 接続を使用するシステムの前方誤り訂正の設定

25Gbps 接続を使用してシステムが設定されている場合は、 RCF ファイルの適用後に前方誤り訂正（ fec ）パラメータを手動で off に設定する必要があります。この設定は RCF ファイルでは適用されません。

このタスクについて

この手順を実行する前に、 25Gbps ポートがケーブル接続されている必要があります。

"Cisco 3232C スイッチまたは Cisco 9336C スイッチのプラットフォームポートの割り当て"

このタスクでは、 25Gbps 接続を使用する環境 プラットフォームのみを使用します。

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

このタスクは、 MetroCluster IP 構成の 4 つのスイッチすべてで実行する必要があります。

手順

1. コントローラモジュールに接続されている各 25Gbps ポートで fec パラメータを off に設定し、実行中の設定をスタートアップ設定にコピーします。

   a. 構成モードを開始します :config t

   b. 設定する 25Gbps インターフェイスを「 interface interface-Id 」と指定します

   c. fec を off に設定します

   d. スイッチの各 25Gbps ポートについて、上記の手順を繰り返します。

   e. 構成モードを終了します : exit

   次の例は、スイッチ IP_switch_A_1 のインターフェイス Ethernet1/25/1 に対するコマンドを示しています。

```
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. MetroCluster IP 構成の他の 3 つのスイッチについて、上記の手順を繰り返します。

未使用のISLポートとポートチャネルを無効にする

NetAppでは、不要なヘルスアラートを回避するために、未使用のISLポートとポートチャネルを無効にすることを推奨します

1. 未使用のISLポートとポートチャネルを特定します。

   「インターフェイスの概要」

2. 未使用のISLポートとポートチャネルを無効にします。

   特定された未使用のポートまたはポートチャネルごとに、次のコマンドを実行する必要があります。

```
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.
```

Cisco 9336C スイッチに MACsec 暗号化を設定します

MACsec 暗号化は、 WAN ISL ポートにのみ適用できます。

Cisco 9336C スイッチに MACsec 暗号化を設定します

サイト間で実行される WAN ISL ポートにのみ MACsec 暗号化を設定する必要があります。正しい RCF ファイルを適用したあとに MACsec を設定する必要があります。

MACsec のライセンス要件

MACsec にはセキュリティライセンスが必要です。Cisco NX-OS ライセンス方式の詳細およびライセンスの取得方法と適用方法については、を参照してください "『 Cisco NX-OS Licensing Guide 』"

MetroCluster IP構成でCisco MACsec暗号化WAN ISLを有効にします

MetroCluster IP 構成では、 WAN ISL 上の Cisco 9336C スイッチに対して MACsec 暗号化をイネーブルにできます。

手順

1. グローバルコンフィギュレーションモードを開始します。

   「 configure terminal 」をクリックします

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

2. デバイスで MACsec と MKA を有効にします。

   「 feature MACsec

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

3. 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

   'copy running-config startup-config

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

MACsecキーチェーンとキーを設定します

MACsec キーチェーンまたはキーをコンフィギュレーションに作成できます。

- キーライフタイムと Hitless Key Rollover *

MACsec キーチェーンには、複数の Pre-Shared Key （ PSK; 事前共有キー）を設定できます。各 PSKs には、キー ID とオプションのライフタイムが設定されています。キーの有効期間は、キーがアクティブになって有効期限が切れるタイミングを指定します。ライフタイム設定がない場合、デフォルトのライフタイムは無制限です。ライフタイムが設定されている場合、ライフタイムが期限切れになると、 MKA はキーチェーン内で設定されている次の事前共有キーにロールオーバーします。キーのタイムゾーンは、 local または UTC です。デフォルトのタイムゾーンは UTC です。キーを同じキーチェーン内の 2 番目のキー（キーチェーン内）にロールオーバーして、最初のキーのライフタイムを設定することができます。最初のキーの有効期間が終了すると、自動的にリスト内の次のキーにロールオーバーされます。リンクの両側で同じキーが同時に設定されている場合、キーのロールオーバーはヒットレスになります（つまり、キーはトラフィックを中断することなくロールオーバーされます）。

手順

1. グローバルコンフィギュレーションモードを開始します。

   「 configure terminal 」をクリックします

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

2. 暗号化されたキーオクテット文字列を非表示にするには、「 show running-config 」コマンドと「 show startup-config 」コマンドの出力で、文字列をワイルドカード文字に置き換えます。

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

> オクテット文字列は、コンフィギュレーションをファイルに保存するときにも非表示になります。

デフォルトでは、 PSK キーは暗号化形式で表示され、簡単に復号化できます。このコマンドは、MACsec キーチェーンにのみ適用されます。

3. MACsec キーチェーンを作成して一連の MACsec キーを保持し、 MACsec キーチェーンコンフィギュレーションモードを開始します。

   キーチェーン名 MACsec

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

4. MACsec キーを作成し、 MACsec キーコンフィギュレーションモードを開始します。

   「 key key-id 」

   指定できる 16 進数のキー文字列の範囲は 1 〜 32 で、最大サイズは 64 文字です。

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

5. キーのオクテット文字列を設定します。

   「 key-octet-string octet-string octet-string cryptographic-algorithm ae_128_CMAC | aes-256_CMAC 」という形式で指定します

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

   octet-string 引数には、最大 64 個の 16 進文字を含めることができます。オクテットキーは内部でエンコードされるため、クリアテキストのキーは、「 show running-config macsec 」コマンドの出力には表示されません。

6. キーの送信ライフタイムを設定します（秒単位）。

   「 send-lifetime start-time duration 」

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

   デフォルトでは、デバイスは開始時間を UTC として処理します。start-time 引数には、キーがアクティブになる時刻と日付を指定します。duration 引数は、ライフタイムの秒単位の長さです。最大値は 2147483646 秒（約 68 年）です。

7. 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

'copy running-config startup-config

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

8. キーチェーン設定を表示します。

   「鍵チェーン名」

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

MACsecポリシーを設定します

手順

1. グローバルコンフィギュレーションモードを開始します。

   「 configure terminal 」をクリックします

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

2. MACsec ポリシーを作成します。

   「 ACSEC ポリシー名」

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

3. 次のいずれかの暗号、 gcm-aes-128 、 gcm-aes-256 、 gcm-aes-xpN-128 、または gcm-aes-xpN-256 を設定します。

   「 cipher-site name 」

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

4. キー交換時にピア間の接続を解除するために、キーサーバの優先度を設定します。

   「 key-server -priority number 」と入力します

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

5. データおよび制御パケットの処理を定義するセキュリティポリシーを設定します。

「セキュリティ・ポリシー・セキュリティ・ポリシー」を参照してください

次のオプションからセキュリティポリシーを選択します。

- must-secure — MACsec ヘッダーを伝送していないパケットはドロップされます
- must-secure — MACsec ヘッダーを伝送しないパケットは許可されます (これがデフォルト値です) 。

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

6. リプレイ保護ウィンドウを設定して、セキュアインターフェイスが設定されたウィンドウサイズより小さいパケットを受け入れないようにします。「 window-size number 」

> リプレイ保護ウィンドウのサイズは、 MACsec が受信して破棄されない最大アウトオブシーケンスフレーム数を表します。指定できる範囲は 0 〜 596000000 です。

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

7. SAK キーの再生成を強制する時間を秒単位で設定します。

「 SAK-expiry-date time 」

このコマンドを使用して、予測可能な時間間隔にセッションキーを変更できます。デフォルトは 0 です。

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

8. 暗号化を開始するレイヤ 2 フレームで、次の機密性オフセットのいずれかを設定します。

「 conf-offsetconfidentiality offset 」を参照してください

次のいずれかのオプションを選択します。

- conf-offset-0 。
- conf-offset-30 。
- conf -offset-50 。

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

> このコマンドは、中間スイッチが MPLS タグのようなパケットヘッダー（ DMAC 、 smac 、 type ）を使用するために必要な場合があります。

9. 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

'copy running-config startup-config

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

10. MACsec ポリシー設定を表示します。

    「 MACsec ポリシー」

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

インターフェイス上で**Cisco MACsec**暗号化をイネーブルにします

1. グローバルコンフィギュレーションモードを開始します。

   「 configure terminal 」をクリックします

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

2. MACsec暗号化で設定したインターフェイスを選択します。

   インターフェイスのタイプと ID を指定できます。イーサネットポートの場合は、イーサネットスロット / ポートを使用します。

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

3. インターフェイスに設定するキーチェーンとポリシーを追加して、MACsec設定を追加します。

   「MACsec keychain -name policy policy-name」という名前のキーチェーンがあります

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

4. MACsec暗号化を設定するすべてのインターフェイスで、ステップ1と2を繰り返します。
5. 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

   'copy running-config startup-config

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

MetroCluster IP構成でCisco MACsec暗号化WAN ISLをディセーブルにします

MetroCluster IP 構成では、 WAN ISL 上の Cisco 9336C スイッチに対して MACsec 暗号化を無効にする必要がある場合があります。

手順

1. グローバルコンフィギュレーションモードを開始します。

   「 configure terminal 」をクリックします

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

2. デバイスの MACsec 設定を無効にします。

   「 ACSEC SHUTDOWN 」のようになります

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

   「 no 」オプションを選択すると、 MACsec 機能が復元されます。

3. MACsec で設定済みのインターフェイスを選択します。

   インターフェイスのタイプと ID を指定できます。イーサネットポートの場合は、イーサネットスロット / ポートを使用します。

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

4. インターフェイスに設定されているキーチェーンとポリシーを削除して、MACsec設定を削除します。

   「no MACsec keychain keychain -name policy policy-name」

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

5. MACsec が設定されているすべてのインターフェイスで、ステップ 3 と 4 を繰り返します。
6. 実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーします。

   'copy running-config startup-config

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

MACsec 構成の確認

手順

1. コンフィギュレーション内の 2 番目のスイッチで上記の手順 * すべて * を繰り返して、 MACsec セッションを確立します。
2. 次のコマンドを実行して、両方のスイッチが正常に暗号化されたことを確認します。

   a. 「 How MACsec mka summary 」を実行します

   b. 実行 :'How MACsec mka session`

   c. 実行： 'How MACsec mka statistics （ MACsec mka 統計情報）

   MACsec 設定を確認するには、次のコマンドを使用します。

コマンドを実行します	表示される情報
'How MACsec mka session interface types/port number	特定のインターフェイスまたはすべてのインターフェイスの MACsec MKA セッション
「鍵チェーン名」	キーチェーン設定
「 MACsec mka の概要」を参照してください	MACsec MKA 設定
'How MACsec policy policy-name' 」を参照してください	特定の MACsec ポリシーまたはすべての MACsec ポリシーの設定