Configurar switches IP Cisco

ONTAP MetroCluster

NetApp
January 10, 2025

Índice

Configurar switches IP Cisco 1
Configurar switches IP Cisco 1
Configure a criptografia MACsec em switches Cisco 9336C 14

Configurar switches IP Cisco

Configurar switches IP Cisco

Você deve configurar os switches IP Cisco para uso como interconexão de cluster e para conetividade IP do MetroCluster de back-end.

Sobre esta tarefa

Vários dos procedimentos nesta seção são procedimentos independentes e você só precisa executar aqueles para os quais você é direcionado ou é relevante para a sua tarefa.

Repor as predefinições de fábrica do interrutor IP do Cisco

Antes de instalar qualquer arquivo RCF, você deve apagar a configuração do switch Cisco e executar a configuração básica. Este procedimento é necessário quando você deseja reinstalar o mesmo arquivo RCF depois de uma instalação anterior falhar, ou se você quiser instalar uma nova versão de um arquivo RCF.

Sobre esta tarefa

- Você deve repetir estas etapas em cada um dos switches IP na configuração IP do MetroCluster.
- Você deve estar conetado ao switch usando o console serial.
- Esta tarefa repõe a configuração da rede de gestão.

Passos

1. Repor as predefinições de fábrica do interrutor:

   a. Apagar a configuração existente:

      ```
      write erase
      ```

   b. Recarregue o software do switch:

      ```
      reload
      ```

      O sistema reinicia e entra no assistente de configuração. Durante a inicialização, se você receber o prompt "'Cancelar provisionamento automático e continuar com a configuração normal? (sim/não)", `you should respond `yes` para continuar.

   c. No assistente de configuração, introduza as definições básicas do interrutor:

      - Palavra-passe de administrador
      - Mudar nome
      - Configuração de gerenciamento fora da banda
      - Gateway predefinido
      - Serviço SSH (RSA)

        Depois de concluir o assistente de configuração, o switch reinicia.

   d. Quando solicitado, introduza o nome de utilizador e a palavra-passe para iniciar sessão no comutador.

      O exemplo a seguir mostra os prompts e as respostas do sistema ao configurar o switch. Os colchetes

de ângulo (<<<) mostram onde você insere as informações.

```
---- 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.
```

Você insere informações básicas no próximo conjunto de prompts, incluindo o nome do switch, endereço de gerenciamento e gateway, e seleciona SSH com 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]:
```

O conjunto final de prompts completa a configuração:

```
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. Guardar a configuração:

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

3. Reinicie o switch e aguarde até que o switch recarregue:

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

4. Repita as etapas anteriores nos outros três switches na configuração IP do MetroCluster.

Transferir e instalar o software Cisco switch NX-os

Você deve baixar o arquivo do sistema operacional switch e o arquivo RCF para cada switch na configuração IP do MetroCluster.

Sobre esta tarefa

Esta tarefa requer software de transferência de arquivos, como FTP, TFTP, SFTP ou SCP, para copiar os arquivos para os switches.

Estas etapas devem ser repetidas em cada um dos switches IP na configuração IP do MetroCluster.

Tem de utilizar a versão do software de comutação suportada.

"NetApp Hardware Universe"

Passos

1. Transfira o ficheiro de software NX-os suportado.

   "Transferência do software Cisco"

2. Copie o software do interrutor para o interrutor:

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

   Neste exemplo, o arquivo nxos.7.0.3.I4.6.bin é copiado do servidor SFTP 10.10.99.99 para o flash de inicialização local:

   ```
   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. Verifique em cada switch se os arquivos NX-os estão presentes no diretório bootflash de cada switch:

   ```
   dir bootflash:
   ```

   O exemplo a seguir mostra que os arquivos estão presentes no 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. Instale o software do interrutor:

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

   O interrutor recarregará (reiniciará) automaticamente após a instalação do software do interrutor.

   O exemplo a seguir mostra a instalação do software em 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. Aguarde até que o interrutor seja recarregado e, em seguida, inicie sessão no interrutor.

   Depois que o switch reiniciar, o prompt de login é exibido:

```
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. Verifique se o software do switch foi instalado `show version`

   O exemplo a seguir mostra a saída:

```
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. Repita estas etapas nos três switches IP restantes na configuração IP do MetroCluster.

Transferir e instalar os ficheiros Cisco IP RCF

Você deve gerar e instalar o arquivo RCF em cada switch na configuração IP do MetroCluster.

Sobre esta tarefa

Esta tarefa requer software de transferência de arquivos, como FTP, TFTP, SFTP ou SCP, para copiar os

arquivos para os switches.

Estas etapas devem ser repetidas em cada um dos switches IP na configuração IP do MetroCluster.

Tem de utilizar a versão do software de comutação suportada.

"NetApp Hardware Universe"

Existem quatro arquivos RCF, um para cada um dos quatro switches na configuração IP do MetroCluster. Você deve usar os arquivos RCF corretos para o modelo de switch que você está usando.

Interrutor	Ficheiro RCF
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

Passos

1. Gerar os arquivos RCF do Cisco para MetroCluster IP.
   a. Transfira o. "RcfFileGenerator para MetroCluster IP"
   b. Gere o arquivo RCF para sua configuração usando o RcfFileGenerator para MetroCluster IP.

      As modificações nos arquivos RCF após o download não são suportadas.

2. Copie os arquivos RCF para os switches:
   a. Copie os arquivos RCF para o primeiro switch:

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

      Neste exemplo, o arquivo RCF NX3232_v1.80_Switch-A1.txt é copiado do servidor SFTP em 10.10.99.99 para o flash de inicialização local. Você deve usar o endereço IP do servidor TFTP/SFTP e o nome do arquivo RCF que você precisa instalar.

```
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. Repita a subetapa anterior para cada uma das outras três centrais, certificando-se de copiar o arquivo RCF correspondente para a central correspondente.

3. Verifique em cada switch se o arquivo RCF está presente no diretório bootflash de cada switch:

   `dir bootflash:`

   O exemplo a seguir mostra que os arquivos estão presentes no 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 as regiões TCAM nos switches Cisco 3132Q-V e Cisco 3232C.

   Ignore esta etapa se você não tiver switches Cisco 3132Q-V ou Cisco 3232C.

   a. No interrutor Cisco 3132Q-V, defina as seguintes regiões TCAM:

```
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. No switch Cisco 3232C, defina as seguintes regiões TCAM:

```
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. Depois de definir as regiões TCAM, salve a configuração e recarregue o switch:

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

5. Copie o arquivo RCF correspondente do flash de inicialização local para a configuração em execução em cada switch:

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

6. Copie os arquivos RCF da configuração em execução para a configuração de inicialização em cada switch:

   `copy running-config startup-config`

   Você deve ver saída semelhante ao seguinte:

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

7. Recarregue o interrutor:

   `reload`

```
IP_switch_A_1# reload
```

8. Repita as etapas anteriores nos outros três switches na configuração IP do MetroCluster.

Definição de correção de erro de avanço para sistemas que utilizam conetividade de 25 Gbps

Se o sistema estiver configurado usando conetividade de 25 Gbps, você precisará definir manualmente o parâmetro Correção de erros de Avanço (fec) para Desativado após a aplicação do arquivo RCF. O ficheiro RCF não aplica esta definição.

Sobre esta tarefa

As portas de 25 Gbps devem ser cabeadas antes de executar este procedimento.

"Atribuições de portas de plataforma para switches Cisco 3232C ou Cisco 9336C"

Esta tarefa aplica-se apenas a plataformas que utilizam conetividade de 25 Gbps:

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

Esta tarefa deve ser executada em todos os quatro switches na configuração IP do MetroCluster.

Passos

1. Defina o parâmetro fec como Desligado em cada porta de 25 Gbps conetada a um módulo de controladora e copie a configuração em execução para a configuração de inicialização:

   a. Entre no modo de configuração: `config t`

   b. Especifique a interface de 25 Gbps para configurar: `interface interface-ID`

   c. Defina fec para Off (Desligado): `fec off`

   d. Repita as etapas anteriores para cada porta de 25 Gbps no switch.

   e. Sair do modo de configuração: `exit`

   O exemplo a seguir mostra os comandos da interface Ethernet1/25/1 no 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. Repita a etapa anterior nos outros três switches na configuração IP do MetroCluster.

Desative portas ISL e canais de portas não utilizados

A NetApp recomenda a desativação de portas e canais de portas ISL não utilizados para evitar alertas de integridade desnecessários.

1. Identificar as portas ISL e os canais de portas não utilizados:

   ```
   show interface brief
   ```

2. Desative as portas ISL e os canais de portas não utilizados.

   Você deve executar os seguintes comandos para cada porta ou canal de porta não utilizado identificado.

   ```
   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 a criptografia MACsec em switches Cisco 9336C

A criptografia MACsec só pode ser aplicada às portas ISL WAN.

Configure a criptografia MACsec em switches Cisco 9336C

Você só deve configurar a criptografia MACsec nas portas ISL WAN executadas entre os sites. Você deve configurar o MACsec depois de aplicar o arquivo RCF correto.

Requisitos de licenciamento para MACsec

MACsec requer uma licença de segurança. Para obter uma explicação completa do esquema de licenciamento do Cisco NX-os e como obter e solicitar licenças, consulte a. "Guia de licenciamento do Cisco NX-os"

Habilite ISLs WAN de criptografia MACsec Cisco em configurações IP MetroCluster

Você pode ativar a criptografia MACsec para switches Cisco 9336C nos ISLs de WAN em uma configuração IP MetroCluster.

Passos

1. Entre no modo de configuração global:

   ```
   configure terminal
   ```

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

2. Ativar MACsec e MKA no dispositivo:

`feature macsec`

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

3. Copie a configuração em execução para a configuração de inicialização:

`copy running-config startup-config`

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

Configure uma cadeia de chaves e chaves MACsec

Você pode criar uma cadeia de chaves MACsec ou chaves em sua configuração.

Key Lifetime e Hitless Key Rollover

Um chaveiro MACsec pode ter várias chaves pré-compartilhadas (PSKs), cada uma configurada com um ID de chave e uma vida útil opcional. Uma vida útil da chave especifica a hora em que a chave ativa e expira. Na ausência de uma configuração vitalícia, o tempo de vida padrão é ilimitado. Quando uma vida útil é configurada, o MKA passa para a próxima chave pré-compartilhada configurada no chaveiro após a expiração da vida útil. O fuso horário da chave pode ser local ou UTC. O fuso horário padrão é UTC. Uma chave pode rolar para uma segunda chave dentro do mesmo chaveiro se você configurar a segunda chave (no chaveiro) e configurar uma vida útil para a primeira chave. Quando o tempo de vida da primeira tecla expira, ela passa automaticamente para a próxima chave na lista. Se a mesma chave for configurada em ambos os lados do link ao mesmo tempo, a rolagem da chave será sem hitless (ou seja, a chave rolará sem interrupção de tráfego).

Passos

1. Entre no modo de configuração global:

`configure terminal`

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

2. Para ocultar a cadeia de carateres octeto de chave criptografada, substitua a cadeia por um caractere curinga na saída `show running-config` dos comandos e `show startup-config`:

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

> ⓘ A cadeia de carateres octeto também é oculta quando você salva a configuração em um arquivo.

Por padrão, as chaves PSK são exibidas em formato criptografado e podem ser facilmente descriptografadas. Este comando aplica-se apenas às cadeias de chaves MACsec.

3. Crie uma cadeia de chaves MACsec para manter um conjunto de chaves MACsec e entrar no modo de configuração da cadeia de chaves MACsec:

   `key chain name macsec`

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

4. Crie uma chave MACsec e entre no modo de configuração da chave MACsec:

   `key key-id`

   O intervalo é de 1 a 32 carateres de chave de dígitos hexadecimais e o tamanho máximo é de 64 carateres.

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

5. Configure a cadeia de carateres octeto para a chave:

   `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
   ```

   > O argumento octet-string pode conter até 64 carateres hexadecimais. A chave octeto é codificada internamente, portanto a chave em texto claro não aparece na saída do `show running-config macsec` comando.

6. Configure uma vida útil de envio para a chave (em segundos):

   `send-lifetime start-time duration duration`

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

   Por padrão, o dispositivo trata a hora de início como UTC. O argumento de hora de início é a hora do dia e a data em que a chave se torna ativa. O argumento duração é o comprimento do tempo de vida em segundos. A duração máxima é de 2147483646 segundos (aproximadamente 68 anos).

7. Copie a configuração em execução para a configuração de inicialização:

   `copy running-config startup-config`

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

8. Exibe a configuração do keychain:

   `show key chain name`

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

Configurar uma política MACsec

Passos

1. Entre no modo de configuração global:

   `configure terminal`

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

2. Criar uma política MACsec:

   `macsec policy name`

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

3. Configure uma das seguintes cifras, GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128 ou GCM-AES-XPN-256:

   `cipher-suite name`

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

4. Configure a prioridade do servidor de chaves para quebrar o vínculo entre pares durante uma troca de chaves:

   `key-server-priority number`

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

5. Configure a política de segurança para definir o processamento de dados e pacotes de controle:

   `security-policy security policy`

Escolha uma política de segurança das seguintes opções:

- Must-Secure — os pacotes que não transportam cabeçalhos MACsec são descartados
- Should-secure - pacotes que não transportam cabeçalhos MACsec são permitidos (este é o valor padrão)

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

6. Configure a janela de proteção de repetição para que a interface protegida não aceite um pacote que seja menor do que o tamanho da janela configurado: `window-size number`

   O tamanho da janela de proteção de repetição representa o máximo de quadros fora de sequência que o MACsec aceita e não são descartados. O intervalo é de 0 a 596000000.

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

7. Configure o tempo em segundos para forçar um SAK rechavear:

   `sak-expiry-time time`

   Você pode usar este comando para alterar a chave da sessão para um intervalo de tempo previsível. A predefinição é 0.

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

8. Configure uma das seguintes compensações de confidencialidade no quadro da camada 2 onde a criptografia começa:

   `conf-offsetconfidentiality offset`

   Escolha entre as seguintes opções:

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

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

   Esse comando pode ser necessário para que os switches intermediários usem cabeçalhos de pacotes (dmac, smac, etype) como tags MPLS.

9. Copie a configuração em execução para a configuração de inicialização:

   `copy running-config startup-config`

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

10. Apresentar a configuração da política MACsec:

    `show macsec policy`

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

Ative a criptografia Cisco MACsec nas interfaces

1. Entre no modo de configuração global:

   `configure terminal`

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

2. Selecione a interface que você configurou com criptografia MACsec.

   Você pode especificar o tipo de interface e a identidade. Para uma porta Ethernet, use slot/porta ethernet.

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

3. Adicione o chaveiro e a política a serem configurados na interface para adicionar a configuração MACsec:

   `macsec keychain keychain-name policy policy-name`

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

4. Repita as etapas 1 e 2 em todas as interfaces onde a criptografia MACsec deve ser configurada.
5. Copie a configuração em execução para a configuração de inicialização:

   `copy running-config startup-config`

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

Desative os ISLs de WAN de criptografia Cisco MACsec em configurações IP do MetroCluster

Talvez seja necessário desativar a criptografia MACsec para switches Cisco 9336C nos ISLs de WAN em uma configuração IP MetroCluster.

Passos

1. Entre no modo de configuração global:

   `configure terminal`

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

2. Desative a configuração MACsec no dispositivo:

   `macsec shutdown`

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

   Selecionar a opção "não" restaura o recurso MACsec.

3. Selecione a interface que você já configurou com o MACsec.

   Você pode especificar o tipo de interface e a identidade. Para uma porta Ethernet, use slot/porta ethernet.

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

4. Remova o chaveiro e a política configurados na interface para remover a configuração MACsec:

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

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

5. Repita as etapas 3 e 4 em todas as interfaces onde o MACsec está configurado.
6. Copie a configuração em execução para a configuração de inicialização:

   `copy running-config startup-config`

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

Verificando a configuração do MACsec

Passos

1. Repita **All** dos procedimentos anteriores no segundo switch dentro da configuração para estabelecer uma sessão MACsec.
2. Execute os seguintes comandos para verificar se ambos os switches estão criptografados com êxito:

a. Executar: `show macsec mka summary`

b. Executar: `show macsec mka session`

c. Executar: `show macsec mka statistics`

Você pode verificar a configuração do MACsec usando os seguintes comandos:

Comando	Exibe informações sobre…
`show macsec mka session interface typeslot/port number`	A sessão MACsec MKA para uma interface específica ou para todas as interfaces
`show key chain name`	A configuração da cadeia de chaves
`show macsec mka summary`	A configuração MACsec MKA
`show macsec policy policy-name`	A configuração para uma política MACsec específica ou para todas as políticas MACsec

Informações sobre direitos autorais

Informações sobre marcas comerciais