Cisco IP 스위치를 구성합니다

ONTAP MetroCluster

NetApp
February 13, 2026

목차

Cisco IP 스위치를 구성합니다

클러스터 상호 연결 및 백엔드 MetroCluster IP 연결을 위해 Cisco IP 스위치 구성

클러스터 인터커넥트 및 백엔드 MetroCluster IP 연결에 사용할 Cisco IP 스위치를 구성해야 합니다.

이 작업에 대해

이 섹션의 절차 중 일부는 독립 절차이며, 사용자가 직접 수행했거나 작업과 관련된 절차만 실행해야 합니다.

Cisco IP 스위치를 출하 시 기본값으로 재설정합니다

RCF 파일을 설치하기 전에 Cisco 스위치 구성을 지우고 기본 구성을 수행해야 합니다. 이전 설치가 실패한 후 동일한 RCF 파일을 다시 설치하거나 새 버전의 RCF 파일을 설치하려는 경우 이 절차가 필요합니다.

이 작업에 대해

- MetroCluster IP 구성의 각 IP 스위치에서 이 단계를 반복해야 합니다.
- 직렬 콘솔을 사용하여 스위치에 연결해야 합니다.
- 이 작업은 관리 네트워크의 구성을 재설정합니다.

단계

1. 스위치를 출하 시 기본값으로 재설정합니다.

   a. 기존 구성을 지웁니다.

      쓰기 지우기

   b. 스위치 소프트웨어를 다시 로드합니다.

      다시 로드

      시스템이 재부팅되고 구성 마법사가 시작됩니다. 부팅 중에 "'자동 프로비저닝 중단'이라는 메시지가 표시되면 일반 설정으로 계속 진행하시겠습니까? (예/아니요) [n]", 계속하려면 "예"라고 답해야 합니다.

   c. 구성 마법사에서 기본 스위치 설정을 입력합니다.

      - 관리자 암호입니다
      - 스위치 이름
      - 대역외 관리 구성
      - 기본 게이트웨이
      - SSH 서비스(RSA)

        구성 마법사를 완료하면 스위치가 재부팅됩니다.

   d. 메시지가 표시되면 사용자 이름과 암호를 입력하여 스위치에 로그인합니다.

다음 예에서는 스위치를 구성할 때 프롬프트 및 시스템 응답을 보여 줍니다. 꺾쇠 괄호(<<<<)는 사용자가 정보를 입력하는 위치를 표시합니다.

```
---- 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.
```

스위치 이름, 관리 주소 및 게이트웨이를 포함하여 다음 프롬프트 세트에 기본 정보를 입력하고 SSH with RSA를 선택합니다.

> ⓘ 이 예에서는 RCF를 구성하는 데 필요한 최소 정보를 보여 주며, RCF를 적용한 후 추가 옵션을 구성할 수 있습니다. 예를 들어 RCF를 적용한 후 SNMPv3, NTP 또는 SCP/SFTP를 구성할 수 있습니다.

```
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]:
```

마지막 프롬프트 세트가 구성을 완료합니다.

```
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. 구성을 저장합니다.

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

3. 스위치를 재부팅하고 스위치가 다시 로드될 때까지 기다립니다.

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

4. MetroCluster IP 구성의 다른 3개 스위치에 대해 이전 단계를 반복합니다.

Cisco 스위치 NX-OS 소프트웨어 다운로드 및 설치

MetroCluster IP 구성의 각 스위치에 스위치 운영 체제 파일과 RCF 파일을 다운로드해야 합니다.

이 작업에 대해

이 작업에는 FTP, TFTP, SFTP 또는 SCP와 같은 파일 전송 소프트웨어가 필요합니다. 스위치에 파일을 복사합니다.

이러한 단계는 MetroCluster IP 구성의 각 IP 스위치에서 반복해야 합니다.

지원되는 스위치 소프트웨어 버전을 사용해야 합니다.

"NetApp Hardware Universe를 참조하십시오"

단계

1. 지원되는 NX-OS 소프트웨어 파일을 다운로드합니다.

   "Cisco 소프트웨어 다운로드"

2. 스위치 소프트웨어를 스위치에 복사합니다.

   'copy sftp://root@server-ip-address/tftpboot/nx-os-file-name bootflash:vrf management'

   이 예에서 nxos.7.0.3.I4.6.bin 파일과 EPLD 이미지는 SFTP 서버 10.10.99.99에서 로컬 부트플래시로 복사됩니다.

```
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. 각 스위치에서 스위치 NX-OS 파일이 각 스위치의 bootflash 디렉토리에 있는지 확인합니다.

   'dir bootflash:'

   다음 예제는 파일이 IP_SWITCH_A_1에 있음을 보여줍니다.

```
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. 스위치 소프트웨어를 설치합니다.

   nxos bootflash: nxos.version-number.bin을 모두 설치합니다

   스위치 소프트웨어가 설치되면 스위치는 자동으로 다시 로드(재부팅)됩니다.

   다음 예에서는 IP_SWITCH_A_1에 설치된 소프트웨어를 보여 줍니다.

```
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. 스위치가 다시 로드될 때까지 기다린 다음 스위치에 로그인합니다.

스위치가 재부팅되면 로그인 프롬프트가 표시됩니다.

```
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. 스위치 소프트웨어가 설치되어 있는지 확인합니다

   다음 예는 출력을 보여줍니다.

```
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. EPLD 이미지를 업그레이드하고 스위치를 reboot한다.

```
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. 스위치 재부팅 후 다시 로그인하여 새 버전의 EPLD가 성공적으로 로드되었는지 확인합니다.

```
show version module 1 epld
```

9. MetroCluster IP 구성의 나머지 3개 IP 스위치에 대해 이 단계를 반복합니다.

Cisco IP RCF 파일 다운로드 및 설치

MetroCluster IP 구성의 각 스위치에 RCF 파일을 생성하고 설치해야 합니다.

이 작업에 대해

이 작업에는 FTP, TFTP, SFTP 또는 SCP와 같은 파일 전송 소프트웨어가 필요합니다. 스위치에 파일을 복사합니다.

이러한 단계는 MetroCluster IP 구성의 각 IP 스위치에서 반복해야 합니다.

지원되는 스위치 소프트웨어 버전을 사용해야 합니다.

"NetApp Hardware Universe를 참조하십시오"

QSFP-SFP+ 어댑터를 사용하는 경우 ISL 포트를 브레이크아웃 속도 모드 대신 기본 속도 모드로 구성해야 할 수 있습니다. ISL 포트 속도 모드를 확인하려면 스위치 공급업체의 설명서를 참조하십시오.

RCF 파일은 MetroCluster IP 구성의 4개 스위치당 하나씩 4개의 파일로 구성됩니다. 사용 중인 스위치 모델에 적합한 RCF 파일을 사용해야 합니다.

스위치	RCF 파일
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

단계

1. MetroCluster IP에 대한 Cisco RCF 파일을 생성합니다.
   a. 를 다운로드하십시오 "MetroCluster IP용 RcfFileGenerator입니다"
   b. MetroCluster IP용 RcfFileGenerator를 사용하여 구성에 대한 RCF 파일을 생성합니다.

      다운로드 후 RCF 파일을 수정할 수 없습니다.

2. RCF 파일을 스위치에 복사합니다.
   a. RCF 파일을 첫 번째 스위치에 복사합니다.

      복사 sftp://root@ftp-server-ip-address/tftpboot/switch-specific-bootRCF flash:vrf management

      이 예에서 NX3232_v1.80_Switch-A1.txt RCF 파일은 SFTP 서버(10.10.99.99)에서 로컬 bootflash로 복사됩니다. TFTP/SFTP 서버의 IP 주소와 설치해야 하는 RCF 파일의 파일 이름을 사용해야 합니다.

```
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. 일치하는 RCF 파일을 해당 스위치에 복사하도록 나머지 세 스위치 각각에 대해 이전 하위 단계를 반복합니다.

3. 각 스위치에서 RCF 파일이 각 스위치의 bootflash 디렉토리에 있는지 확인합니다.

   'dir bootflash:'

   다음 예제는 파일이 IP_SWITCH_A_1에 있음을 보여줍니다.

```
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 및 Cisco 3232C 스위치에서 TCAM 영역을 구성합니다.

   Cisco 3132Q-V 또는 Cisco 3232C 스위치가 없는 경우 이 단계를 건너뛰십시오.

   a. Cisco 3132Q-V 스위치에서 다음 TCAM 영역을 설정합니다.

```
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 스위치에서 다음 TCAM 영역을 설정합니다.

```
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 영역을 설정한 후 구성을 저장하고 스위치를 다시 로드합니다.

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

5. 로컬 bootflash에서 각 스위치의 실행 구성으로 일치하는 RCF 파일을 복사합니다.

   bootflash: switch-specific-RCF.txt running-config를 복사합니다

6. RCF 파일을 실행 중인 구성에서 각 스위치의 시작 구성으로 복사합니다.

   'copy running-config startup-config'를 선택합니다

   다음과 유사한 출력이 표시됩니다.

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

7. 스위치를 다시 로드하십시오.

   다시 로드

```
IP_switch_A_1# reload
```

8. MetroCluster IP 구성의 다른 3개 스위치에 대해 이전 단계를 반복합니다.

25Gbps 연결을 사용하는 시스템에 대한 Forward Error Correction 설정

시스템이 25Gbps 연결을 사용하여 구성된 경우 RCF 파일을 적용한 후 FEC(Forward Error Correction) 매개변수를 수동으로 OFF로 설정해야 합니다. RCF 파일은 이 설정을 적용하지 않습니다.

이 작업에 대해

이 절차를 수행하기 전에 25Gbps 포트를 케이블로 연결해야 합니다.

"Cisco 3232C 또는 Cisco 9336C 스위치에 대한 플랫폼 포트 할당"

이 작업은 25Gbps 연결을 사용하는 플랫폼에만 적용됩니다.

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

이 작업은 MetroCluster IP 구성의 4개 스위치 모두에서 수행해야 합니다.

단계

1. 컨트롤러 모듈에 연결된 각 25Gbps 포트에서 FEC 매개변수를 OFF로 설정한 다음 실행 중인 구성을 시작 구성으로 복사합니다.

   a. 설정 모드 'config t'로 진입한다

   b. 구성할 25Gbps interface를 지정한다:'interface-id'

   c. FEC를 OFF: FEC OFF로 설정한다

   d. 스위치의 각 25Gbps 포트에 대해 이전 단계를 반복합니다.

   e. 설정 모드 종료: '종료

   다음 예에서는 스위치 IP_SWITCH_A_1의 인터페이스 Ethernet1/25/1에 대한 명령을 보여 줍니다.

```
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 구성의 다른 3개 스위치에 대해 이전 단계를 반복합니다.

사용되지 않는 ISL 포트 및 포트 채널을 비활성화합니다

불필요한 상태 경고를 방지하기 위해 사용하지 않는 ISL 포트 및 포트 채널을 비활성화하는 것이 좋습니다 NetApp.

1. 사용되지 않는 ISL 포트 및 포트 채널 식별:

인터페이스 요약

2. 사용되지 않는 ISL 포트 및 포트 채널을 비활성화합니다.

   식별된 미사용 포트 또는 포트 채널에 대해 다음 명령을 실행해야 합니다.

```
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.
```

MetroCluster IP 사이트의 Cisco 9336C 스위치에서 MACsec 암호화 구성

MACsec 암호화는 WAN ISL 포트에만 적용할 수 있습니다.

Cisco 9336C 스위치에서 MACsec 암호화를 구성합니다

사이트 간에 실행되는 WAN ISL 포트에서만 MACsec 암호화를 구성해야 합니다. 올바른 RCF 파일을 적용한 후 MACsec을 구성해야 합니다.

MACsec에 대한 라이센스 요구 사항

MACsec에는 보안 라이센스가 필요합니다. Cisco NX-OS 라이센스 체계에 대한 전체 설명 및 라이센스 취득 및 적용 방법은 을 참조하십시오 "Cisco NX-OS 라이센스 가이드 를 참조하십시오"

MetroCluster IP 구성에서 Cisco MACsec 암호화 WAN ISL을 활성화합니다

MetroCluster IP 구성에서 WAN ISL의 Cisco 9336C 스위치에 대해 MACsec 암호화를 설정할 수 있습니다.

단계

1. 글로벌 구성 모드 시작:

   '터미널 구성'을 선택합니다

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

2. 장치에서 MACsec 및 MKA 활성화:

피처 MACsec

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

3. 실행 중인 구성을 시작 구성으로 복사합니다.

'copy running-config startup-config'를 선택합니다

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

MACsec 키 체인 및 키를 구성합니다

구성에 MACsec 키 체인 또는 키를 만들 수 있습니다.

- 키 수명 및 Hitless 키 롤오버 *

MACsec 키 체인은 미리 공유된 여러 키(PSK)를 가질 수 있으며, 각 키는 키 ID와 수명(옵션)으로 구성됩니다. 키 수명은 키가 활성화되고 만료되는 시간을 지정합니다. 수명 구성이 없을 경우 기본 수명은 무제한입니다. 수명이 구성되면 MKA는 수명이 만료된 후 키체인에 구성된 다음 사전 공유 키로 롤오버합니다. 키의 표준 시간대는 로컬 또는 UTC입니다. 기본 표준 시간대는 UTC입니다. 두 번째 키(키 체인)를 구성하고 첫 번째 키의 수명을 구성하면 동일한 키 체인 내의 두 번째 키로 키를 롤오버할 수 있습니다. 첫 번째 키의 수명이 만료되면 목록의 다음 키로 자동 롤오버됩니다. 같은 키가 링크의 양쪽에서 동시에 구성된 경우 키 롤오버는 무단위(즉, 키가 트래픽 중단 없이 롤오버됨)입니다.

단계

1. 글로벌 구성 모드로 들어갑니다.

'터미널 구성'을 선택합니다

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

2. 암호화된 키 옥텟 문자열을 숨기려면 'show running-config' 및 'show startup-config' 명령의 출력에서 문자열을 와일드카드 문자로 바꿉니다.

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

설정을 파일에 저장할 때 옥텟 문자열도 숨겨집니다.

기본적으로 PSK 키는 암호화된 형식으로 표시되며 쉽게 해독할 수 있습니다. 이 명령은 MACsec 키 체인에만 적용됩니다.

3. MACsec 키 세트를 보류하고 MACsec 키 체인 구성 모드로 전환하기 위해 MACsec 키 체인을 생성합니다.

키 체인 이름 MACsec

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

4. MACsec 키를 만들고 MACsec 키 구성 모드를 입력합니다.

   키 ID

   범위는 1 ~ 32자의 16진수 키 문자열이며 최대 크기는 64자입니다.

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

5. 키에 대한 옥텟 문자열을 구성합니다.

   'key-octet-string octet-string 암호화 알고리즘 AES_128_CMAC|AES_256_CMAC'

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

   8진수 문자열 인수는 최대 64자의 16진수 문자를 포함할 수 있습니다. 옥텟키는 내부적으로 인코딩되므로 'show running-config MACsec' 명령의 출력에는 일반 텍스트의 키가 나타나지 않는다.

6. 키의 전송 수명 구성(초):

   '수명 종료 시작-시간 지속 기간'을 선택합니다

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

   기본적으로 장치는 시작 시간을 UTC로 처리합니다. start-time 인수는 키가 활성화되는 날짜와 시간입니다. duration 인수는 초 단위의 수명 길이입니다. 최대 길이는 2147483646초(약 68년)입니다.

7. 실행 중인 구성을 시작 구성으로 복사합니다.

   'copy running-config startup-config'를 선택합니다

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

8. 키 체인 구성을 표시합니다.

   키 체인 이름

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

MACsec 정책을 구성합니다

단계

1. 글로벌 구성 모드 시작:

   '터미널 구성'을 선택합니다

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

2. MACsec 정책 만들기:

   'macsec policy name'입니다

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

3. GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128 또는 GCM-AES-XPN-256 중 하나를 구성합니다.

   암호-스위트 이름

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

4. 키 교환 중에 피어 간의 연결을 끊도록 키 서버 우선 순위를 구성합니다.

   키-서버-우선 순위 번호

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

5. 데이터 처리 및 제어 패킷을 정의할 수 있도록 보안 정책을 구성합니다.

   보안정책

   다음 옵션 중에서 보안 정책을 선택합니다.

   - 필수 보안 — MACsec 헤더를 전달하지 않는 패킷은 삭제됩니다
   - 보안 — MACsec 헤더를 전달하지 않는 패킷이 허용됩니다(기본값).

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

6. 보안된 인터페이스가 설정된 윈도 크기보다 작은 패킷을 허용하지 않도록 재생 보호 윈도우를 설정한다

   재생 보호 창 크기는 MACsec이 수락하고 폐기하지 않는 최대 시퀀스 초과 프레임을 나타냅니다. 범위는 0에서 596000000 사이입니다.

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

7. SAK 키를 강제로 다시 입력하다

   'AK-expiry-time'입니다

   이 명령을 사용하여 세션 키를 예측 가능한 시간 간격으로 변경할 수 있습니다. 기본값은 0입니다.

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

8. 암호화가 시작되는 계층 2 프레임에서 다음 기밀 오프셋 중 하나를 구성합니다.

   'conf-offset기밀성 오프셋'

   다음 옵션 중에서 선택합니다.

   - conf-offset-0.
   - conf-offset-30
   - conf-offset-50.

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

   이 명령은 MPLS 태그와 같은 패킷 헤더(dmac, smac, etype)를 사용하기 위해 중간 스위치에 필요할 수 있습니다.

9. 실행 중인 구성을 시작 구성으로 복사합니다.

   'copy running-config startup-config'를 선택합니다

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

10. MACsec 정책 구성을 표시합니다.

    마초 정책

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

인터페이스에서 **Cisco MACsec** 암호화를 활성화합니다

1. 글로벌 구성 모드 시작:

   '터미널 구성'을 선택합니다

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

2. MACsec 암호화로 구성한 인터페이스를 선택합니다.

   인터페이스 유형 및 ID를 지정할 수 있습니다. 이더넷 포트의 경우 이더넷 슬롯/포트를 사용합니다.

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

3. 인터페이스에서 구성할 키 체인 및 정책을 추가하여 MACsec 구성을 추가합니다.

   macsec keychain-name policy-name'입니다

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

4. MACsec 암호화를 구성할 모든 인터페이스에서 1단계와 2단계를 반복합니다.
5. 실행 중인 구성을 시작 구성으로 복사합니다.

   'copy running-config startup-config'를 선택합니다

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

MetroCluster IP 구성에서 **Cisco MACsec** 암호화 **WAN ISL**을 비활성화합니다

MetroCluster IP 구성에서 WAN ISL의 Cisco 9336C 스위치에 대한 MACsec 암호화를 비활성화해야 할 수 있습니다.

단계

1. 글로벌 구성 모드 시작:

   '터미널 구성'을 선택합니다

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

2. 장치에서 MACsec 구성 비활성화:

'시스템 종료'

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

""아니오" 옵션을 선택하면 MACsec 기능이 복원됩니다.

3. MACsec로 이미 구성한 인터페이스를 선택합니다.

   인터페이스 유형 및 ID를 지정할 수 있습니다. 이더넷 포트의 경우 이더넷 슬롯/포트를 사용합니다.

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

4. MACsec 구성을 제거하기 위해 인터페이스에 구성된 키 체인 및 정책을 제거합니다.

   MACsec keychain keychain-name policy-name 없음

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

5. MACsec이 구성된 모든 인터페이스에서 3단계와 4단계를 반복합니다.
6. 실행 중인 구성을 시작 구성으로 복사합니다.

   'copy running-config startup-config'를 선택합니다

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

MACsec 구성을 확인하는 중입니다

단계

1. MACsec 세션을 설정하려면 구성 내 두 번째 스위치에 대한 이전 절차의 * ALL * 을 반복합니다.
2. 다음 명령을 실행하여 두 스위치가 모두 성공적으로 암호화되었는지 확인합니다.

   a. 'How MACsec MKA summary'를 실행합니다
   b. 'How MACsec MKA SESSION'을 실행하십시오
   c. 'How MACsec MKA statistics'를 실행합니다

      다음 명령을 사용하여 MACsec 구성을 확인할 수 있습니다.

명령	다음에 대한 정보를 표시합니다.

'How MACsec MKA session interface typeslot/port number'	특정 인터페이스 또는 모든 인터페이스에 대한 MACsec MKA 세션
키 체인 이름	키 체인 구성
'하세초 MKA 요약 정보	MACsec MKA 구성
마초 정책 정책 이름	특정 MACsec 정책 또는 모든 MACsec 정책의 구성