

멀티벤더 DRA 통합을 위한 컨피그레이션 가이드 사용

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[컨피그레이션 단계 및 모범 사례](#)

[1단계: DRA 연결 모드 결정\(인바운드 및 아웃바운드 피어 비교\)](#)

[2단계: 정책 구성기에서 인바운드 피어 구성](#)

[3단계: Host-IP-Address AVP 구성](#)

[4단계: 피어 기능 교환 확인](#)

[5단계: Diameter Unique Source Hostname이 각 Diameter 피어 노드에 정의되었는지 확인합니다.](#)

[6단계: DRA 피어에 대한 Next Hop 라우팅 테이블 구성](#)

소개

이 문서에서는 멀티벤더 DRA와 Cisco CPS(Policy Suite) PCRF 클러스터의 통합을 위한 모범 사례와 함께 컨피그레이션 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco는 이 솔루션을 사용하는 엔지니어가 다음 주제에 대해 숙지할 것을 권장합니다.

- Linux 운영 체제
- Cisco CPS(Policy Suite) 플랫폼 및 클러스터 아키텍처
- 정책 및 과금 규칙 기능(PCRF)
- Vi 편집기 사용
- Wireshark 네트워크 분석 툴

사용되는 구성 요소

이 문서의 정보는 CPS 25.1 버전 및 AlmaLinux 릴리스 8.10을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

컨피그레이션 단계 및 모범 사례

1단계: DRA 연결 모드 결정(인바운드 및 아웃바운드 피어 비교)

- 인바운드 피어: PCRF는 지정된 Diameter 피어로부터의 연결 요청을 수락하도록 구성됩니다. 피어 노드는 PCRF에 CER(Diameter Capabilities-Exchange-Request)를 시작합니다.
- 아웃바운드 피어: PCRF는 피어를 향해 CER를 시작하도록 구성된다.

모범 사례:
대부분의 멀티벤더 DRA 통합의 경우 DRA를 인바운드 피어로 구성합니다. 여기서 DRA는 CER를 PCRF에 시작합니다.

2단계: 정책 구성기에서 인바운드 피어 구성

Policy Builder GUI에서 Inbound Peers 및 Realms 테이블을 참조하여 인바운드 피어 이름 및 피어 영역을 구성합니다.



참고: 자세한 매개변수 설명은 CPS Mobile Configuration Guide, Release 25.1.0의 Diameter Stack Configuration 섹션을 참조하십시오.

다음 매개변수는 Inbound Peers(인바운드 피어) 아래에서 구성할 수 있습니다.

피어 테이블

매개변수	설명
피어	PCRF로의 연결을 시작할 수 있는 피어 이름을 정의합니다.

로컬 호스트 이름	다음과 같은 정책 디렉터(로드 밸런서)의 로컬 호스트 이름을 식별합니다 피어에서 들어오는 연결을 식별하고 허용합니다.
인스턴스 번호	할당된 QNS(정책 서버) 프로세스 번호를 나타냅니다. 아웃바운드 피어와의 연결을 시작합니다.  참고: 정책 구성기(로드 밸런서)의 단일 정책 서버 (QNS) 프로세스만 해당 피어와의 연결을 허용/시작할 경우 로컬 호스트 이름과 인스턴스 번호를 지정해야 합니다. 그렇지 않으면 인스턴스 번호를 0으로 유지할 수 있습니다. 이 경우 정책 관리자(로드 밸런서)의 모든 정책 서버(QNS) 프로세스는 피어와의 연결을 시도/허용해야 합니다. 기본값은 0입니다.
등급	PCRF가 시작한 요청을 전달하기 위해 이 피어에 할당된 우선순위입니다. 이 등급 값이 높을수록 피어에 할당된 우선순위가 높습니다. 기본값은 1입니다.
포트 범위	기본 전송 연결이 SCTP인 경우에만 지정해야 합니다. 동일한 가 TCP인 경우에는 필요하지 않습니다.
응답 시간 초과	이 매개변수는 사용하지 않는 것이 좋습니다.
이름 패턴	Origin-Host CER의 A VP 값은 의 이 패턴에 대해 검증해야 합니다. 연결을 설정하기 위한 순서입니다. 그렇지 않을 경우 CER는 자동으로 삭제되고 TCP 연결이 PCRF에 의해 재설정됩니다. Accept Undefined Peer(정의되지 않은 피어 수락) 옵션을 선택하면 이름 패턴 확인이 수행되지 않습니다 Diameter Stack Configuration에서 설명합니다. 이름 패턴은 표준 Java 정규식이어야 합니다

	구문이 여기에 설명되어 있습니다.
--	--------------------

영역 테이블

매개변수	설명
영역	연결을 시작할 수 있는 피어 영역을 정의합니다. PCRF.
피어 유형	인바운드 영역에는 사용되지 않습니다.
처리 프로토콜	영역 이름과 다음을 수행할 수 있는 특정 PCRF 로직 간의 매핑 프로토콜 처리에 대한 자세한 내용을 보려면 메시지에 적용해야 합니다. 지름 영역이 있는 지름 스택을 프로토콜 없이 가져올 경우 assigned(할당됨), 기본값을 GX_TGPP로 사용합니다.
등급	PCRF가 시작한 요청을 전달하기 위해 이 영역에 할당된 우선순위입니다. 이 는 SY_PRIME 처리 프로토콜에서만 사용됩니다. 기본값은 0입니다. 등급 값이 낮을수록 영역에 할당된 우선순위가 높습니다. 예를 들어, Rating=10인 영역은 등급=1.
통계 별칭	각 영역에 대해 생성되는 통계가 통계 별칭에 구성된 이름으로, 해당 통계에 추가됩니다. com.broadhop.message mbean 통계에만 적용됩니다.
이름 패턴	Origin-Realm CER의 VP 값은 의 이 패턴에 대해 검증해야 합니다. 처리할 수신 메시지의 순서. 그런 일이 없으면, 메시지는 자동으로 폐기되며 TCP 연결은 PCRF에 의해 재설정됩니다.

이름 패턴은 표준 Java 정규식이어야 합니다
구문이 여기에 설명되어 있습니다.

모범 사례:

좀 더 세분화된 제어를 위해 요구 사항에 따라 특정 피어 및 영역 항목을 구성하여 특정 피어로부터의 피어 생성만 허용하려면 Accept Undefined Peer(정의되지 않은 피어 수락)를 선택 취소합니다.

예:

그림 1: 인바운드 피어 테이블

REFERENCE DATA

File Tools

Systems

Summary

system-1

- Plugin Configurations
- cluster-1
 - Plugin Configurations
 - Diameter Configuration
 - Lab-PCRF
 - USuM Configuration

Account Balance Templates

Custom Reference Data Tables

Diameter Agents

Diameter Clients

Diameter Defaults

Fault List

Notifications

Policy Enforcement Points

Rule Retry Profiles

Subscriber Data Sources

Tariff Times

Diameter Stack

*Name

Lab-PCRF

*Realm

pcrf.mnc.mcc.3gppnetwoi

☐ Accept Undefined Peer

Settings

Inbound Peers

Peers

Local Host Name	Instance Number	*Rating	Port Range	*Response Timeout	*Name Pattern
	0	1			.*.*

Add

Remove

Realms

Peer Type	*Processing Protocol	Rating	Stats Alias	*Name Pattern
	GX_TGPP	0		.*
	RX_TGPP	0		.*

그림 1: 인바운드 피어 테이블

3단계: Host-IP-Address AVP 구성

Diameter Host-IP-Address AVP는 SCTP 기반 연결을 위한 CER/CEA 교환(RFC 3588) 중에 노드의 IP 주소를 전달합니다. Cisco CPS PCRF에서 이 주소는 기본적으로 내부 인터페이스 IP이며, 이는 특정 DRA 벤더에 대해 예상되는 Diameter 서비스 IP와 다릅니다.

Cisco CPS PCRF에서는 로드 밸런서 Virtual IP(LbVIP) 또는 로드 밸런서 VM의 물리적 IP를 지름-

소스-엔드포인트 IP로 사용할 수 있습니다.

기본적으로 내부 인터페이스 IP는 그림과 같이 Diameter CER/CEA 메시지에서 Host-IP-Address로 전달됩니다. 캡처에서 소스 IP를 볼 수 있는 위치는 Host-IP-Address AVP에서 볼 수 있는 위치와 다릅니다.

그림 2: 내부 IP가 Host-IP-Address인 CEA 메시지

No.	Time	Source	Destination	Protocol	Length	Info
28	11.542641	DRA IP	PCRF Service IP	DIAMETER	264	cmd=Capabilities-Exchange Request(257) flags=R--- appl=Diameter Common Message
30	11.794483	PCRF Service IP	DRA IP	DIAMETER	592	cmd=Capabilities-Exchange Answer(257) flags=---- appl=Diameter Common Message

Frame 30: 592 bytes on wire (4736 bits), 592 bytes captured (4736 bits)

> Linux cooked capture v1

> Internet Protocol Version 4, Src: PCRF Service IP (10.130.11.130), Dst: DRA IP (10.118.11.18)

> Transmission Control Protocol, Src Port: 3868, Dst Port: 49151, Seq: 1, Ack: 197, Len: 524

> Diameter Protocol

Version: 0x01

Length: 524

Flags: 0x00

Command Code: Capabilities-Exchange (257)

ApplicationId: Diameter Common Messages (0)

Hop-by-Hop Identifier: 0x5992d592

End-to-End Identifier: 0x071fbd73

[Request In: 28]

[Response Time: 0.251842000 seconds]

> AVP: Origin-Host(264) l=63 f=M- val=pcrf.mnc046.mcc046.3gppnetwork.org

> AVP: Origin-Realm(296) l=42 f=M- val=pcrf.mnc046.mcc046.3gppnetwork.org

> AVP: Host-IP-Address(257) l=14 f=M- val=192.168.12.12 (192.168.12.12)

> AVP: Vendor-Id(266) l=12 f=M- val=26878

> AVP: Supported-Vendor-Id(265) l=12 f=M- val=10415

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Auth-Application-Id(258) l=12 f=M- val=3GPP Gx (16777238)

> AVP: Supported-Vendor-Id(265) l=12 f=M- val=8164

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Supported-Vendor-Id(265) l=12 f=M- val=9

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Supported-Vendor-Id(265) l=12 f=M- val=7898

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Supported-Vendor-Id(265) l=12 f=M- val=5535

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Auth-Application-Id(258) l=12 f=M- val=3GPP Rx (16777236)

> AVP: Supported-Vendor-Id(265) l=12 f=M- val=13019

> AVP: Vendor-Specific-Application-Id(260) l=32 f=M-

> AVP: Product-Name(269) l=21 f=M- val=Cisco Quantum

> AVP: Result-Code(268) l=12 f=M- val=DIAMETER_SUCCESS (2001)

그림 2: 내부 IP가 Host-IP-Address인 CEA 메시지

TCP가 전송 프로토콜로 사용되는 경우 이 AVP가 필수는 아니지만(RFC 3588 참조) 일부 DRA 벤더는 Diameter 연결을 설정하는 동안 이 AVP를 참조하며 내부 IP 대신 PCRF의 Diameter service IP를 기대합니다. 이러한 기대치가 충족되지 않으면 동료들이 확신을 갖지 못할 것이다.

모범 사례:

PCRF에서 Host-IP-Address AVP에 Diameter 서비스 IP를 광고하려면 PCRF 소스 FQDN(Diameter Stack Local End Points에 정의된 대로)을 원하는 IP 주소에 매핑하는 엔트리로 /etc/hosts 파일을 업데이트합니다.



참고: 자세한 내용은 CPS Mobile Configuration Guide, Release 25.1.0의 Diameter Stack Configuration 섹션에 있는 Local End Points 테이블을 참조하십시오.

Openstack 기반 CPS PCRF에서 추가 호스트 항목을 업데이트하려면

- CPS 클러스터가 배포된 상태인지 확인합니다.

curl -X 설치 프로그램 [API 시스템을 가져옵니다](#).

- REST API를 통해 additional-hosts.yaml을 검색 및 업데이트합니다.

```
curl -X GET http://<Cluster Manager IP>:8458/api/system/config/additional-hosts >> additional-hosts.yaml
```

- 제품 설명서에 설명된 대로 curl 명령으로 변경 사항을 적용합니다.

```
curl -X PUT API 시스템 추가 호스트 -H "Content-Type: application/yaml" --data-binary @additional-hosts.yaml
```

이 API 호출이 완료되면 클러스터 관리자는 새 /etc/hosts 파일로 구성되며, 구축된 다른 모든 VM은 비동기적으로 업데이트됩니다.



참고: 자세한 지침은 OpenStack용 CPS 설치 가이드, 오케스트레이션 API 섹션을 참조하십시오.

Vmware 기반 CPS PCRF에서 추가 호스트 항목을 업데이트하려면

- /var/qps/config/deploy/csv/ 경로에 있는 AdditionalHosts.csv 파일에 항목을 추가합니다.
- 클러스터 관리자 VM으로 변경 사항을 가져오려면

```
/var/qps/install/current/scripts/import/import_deploy.sh
```

- 클러스터 관리자에서 변경 사항 적용:

```
/var/qps/install/current/scripts/build_all.sh
```

```
/var/qps/install/current/scripts/upgrade/reinit.sh
```



참고: 자세한 지침은 CPS Installation Guide for VMware, Additional Hosts Configuration 섹션을 참조하십시오.

예:

그림 3: GUI 지름 스택 로컬 엔드포인트

*Local End Points						
*Local Host Name	Instance Number	*Advertised Diameter F Q D N	*Listening Port	Local Bind Ip	*Transport Protocol	Multi Homing Hosts
HOSTNAME-lb01	0	HOSTNAME.pcrf.mncXXX.mccYYY.3gppnetwork.org	3868		TCP	
HOSTNAME-lb02	0	HOSTNAME.pcrf.mncXXX.mccYYY.3gppnetwork.org	3868		TCP	

그림 3: GUI 지름 스택 로컬 엔드포인트

샘플 /etc/hosts 항목:

<#root>

10.x.x.130 HOSTNAME.pcrf.mncXXX.mccYYY.3gppnetwork.org HOSTNAME.pcrf.mncXXX.mccYYY.3gppnetwork.org

```
192.x.x.16 HOSTNAME-cluman installer
#END_QPS_OTHER_HOSTS
[root@Hostname-cluman ~]#
```

4단계: 피어 기능 교환 확인

DRA는 CER(Capabilities-Exchange-Request) 및 CEA(Capabilities-Exchange-Answer) 메시지에서 Gx(16777238) 및 Rx(16777236)와 같은 Diameter 애플리케이션에 대한 지원을 명시적으로 광고해야 합니다.

애플리케이션 ID가 0xffffffff인 릴레이 애플리케이션은 Cisco PCRF에서 지원되지 않습니다. 릴레이 애플리케이션(4294967295)만 교환되고 Gx/Rx는 교환되지 않는 경우 피어 연결이 릴레이 전용 모드로 설정되고 PCRF는 CCR-I 메시지에 응답하지 않습니다.

자세한 내용은 CPS Mobile Configuration Guide의 Next Hop Routing 섹션을 참조하십시오.

모범 사례:

피어 연결 설정 단계에서 DRA가 AVP Auth-Application-ID 값 세트 Diameter 애플리케이션(예: Gx(16777238) 또는 Rx(16777236) 또는 둘 다)을 사용하여 CER 메시지를 전송하고 PCRF가 CEA(Capabilities-Exchange-Answer) 메시지에서 유사한 값으로 응답하는지 확인하기 위해 PCRF에서 pcap를 항상 캡처합니다.

그림 4: Auth-Application-Id에 잘못된 값이 있는 CER 메시지가 릴레이로 표시됨

```

Diameter Protocol
  Version: 0x01
  Length: 196
  > Flags: 0x80, Request
  Command Code: Capabilities-Exchange (257)
  ApplicationId: Diameter Common Messages (0)
  Hop-by-Hop Identifier: 0x5b2c55d3
  End-to-End Identifier: 0x171b0936
  [Answer In: 409]
  > AVP: Origin-Host(264) l=59 f=-M- val=[redacted]01ors.mnc[redacted].mcc[redacted].3gppnetwork.org
  > AVP: Origin-Realm(296) l=41 f=-M- val=epc.mnc084.mcc404.3gppnetwork.org
  > AVP: Host-IP-Address(257) l=14 f=-M- val=10.[redacted].[redacted].146
  > AVP: Vendor-Id(266) l=12 f=-M- val=323
  > AVP: Product-Name(269) l=20 f=--- val=Eagle XG DSR
  > AVP: Auth-Application-Id(258) l=12 f=-M- val=Relay (4294967295)
    AVP Code: 258 Auth-Application-Id
    > AVP Flags: 0x40, Mandatory: Set
    AVP Length: 12
    Auth-Application-Id: Relay (4294967295)
  > AVP: Firmware-Revision(267) l=12 f=--- val=6491648
```

그림 4: Auth-Application-Id as Relay의 잘못된 값을 가진 CER 메시지

그림 5: Auth-Application-Id에 올바른 값이 있는 CER 메시지: Gx 및 Rx

Command Code: Capabilities-Exchange (257)

ApplicationId: Diameter Common Messages (0)

Hop-by-Hop Identifier: 0x38370427

End-to-End Identifier: 0x0d3fbc01

[Answer In: 30]

```
> AVP: Origin-Host(264) l=60 f=-M- val=[redacted]drax01c[redacted].mnc084.mcc404.3gppnetwork.org
> AVP: Origin-Realm(296) l=41 f=-M- val=epc.mnc084.mcc404.3gppnetwork.org
> AVP: Host-IP-Address(257) l=14 f=-M- val=10.[redacted].[redacted].151
> AVP: Vendor-Id(266) l=12 f=-M- val=323
> AVP: Product-Name(269) l=20 f=--- val=Eagle XG DSR
> AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
  AVP Code: 260 Vendor-Specific-Application-Id
  > AVP Flags: 0x40, Mandatory: Set
  AVP Length: 32
  > Vendor-Specific-Application-Id: 0000010a4000000c000028af000001024000000c01000014
    > AVP: Vendor-Id(266) l=12 f=-M- val=10415
    > AVP: Auth-Application-Id(258) l=12 f=-M- val=3GPP Rx (16777236)
      AVP Code: 258 Auth-Application-Id
      > AVP Flags: 0x40, Mandatory: Set
      AVP Length: 12
      Auth-Application-Id: 3GPP Rx (16777236)
  > AVP: Vendor-Specific-Application-Id(260) l=32 f=-M-
    AVP Code: 260 Vendor-Specific-Application-Id
    > AVP Flags: 0x40, Mandatory: Set
    AVP Length: 32
    > Vendor-Specific-Application-Id: 0000010a4000000c000028af000001024000000c01000016
      > AVP: Vendor-Id(266) l=12 f=-M- val=10415
      > AVP: Auth-Application-Id(258) l=12 f=-M- val=3GPP Gx (16777238)
  > AVP: Firmware-Revision(267) l=12 f=--- val=6557952
```

그림 5: Auth-Application-Id에 올바른 값이 있는 CER 메시지: Gx 및 Rx

5단계: Diameter Unique Source Hostname이 각 Diameter 피어 노드에 정의되었는지 확인합니다.

Cisco CPS PCRF는 연결된 각 피어 노드에 고유한 지름 소스 호스트 이름이 필요한 환경을 지원합니다.

기존 직접 Gx 또는 Rx 연결에서 DRA 매개 링크로의 직접 피어 연결에 대해 마이그레이션을 수행해야 하는 경우, PCEF 또는 P-CSCF와 DRA 사이의 각 직접 인터페이스(Gx 또는 Rx)에 대한 DRA 링크는 직접 애플리케이션에 대해 고유한 소스 호스트 이름(AVP Origin-Host의 값)을 사용해야 합니다. 이는 동일한 피어 노드와의 직접 PCRF 연결에 사용되는 것과 다릅니다.

이렇게 하면 피어 노드의 요청이 올바른 DRA 피어 링크를 통해 라우팅되고 PCRF show_peers.py 목록에 이전 직접 링크 다운 항목이 있는 경우 삭제되지 않습니다.

모범 사례:

피어의 DRA 링크에 대한 호스트 이름을 변경할 수 없는 경우 직접 피어 링크를 제거한 후 각 로드 밸런서 VM에서 순차적으로 4개 QNS 서비스 모두를 전체 다시 시작합니다.

이렇게 하면 PCEF/P-CSCF와 PCRF 간의 직접 직경 인터페이스(Gx/Rx)를 위해 이전에 사용된 피어의 오래된 오래된(원천 호스트:) 엔트리가 더 이상 PCRF 직경 피어 연결 목록에 존재하지 않으며, show_peers.py 출력에는 DRA 피어 연결만 있으므로 직경 애플리케이션 메시지의 적절한 라우팅이 이루어집니다(예: Gx_CCA-I, Gx_CCA-T)는 DRA와 PCRF 사이의 새롭게 생성된 직경 링크에서 가져온 것입니다.



참고: LB VM에서 QNS 서비스를 다시 시작하면 트래픽에 영향을 미치고 해당 QNS 인스턴스에서 모든 Diameter 피어 연결을 재설정합니다. 계획된 유지 관리 기간 중에 이 단계를 수행합니다.

6단계: DRA 피어용 Next Hop 라우팅 테이블 구성

이 기능을 사용하면 토폴로지 숨기기 모드가 아닌 DRA와 상호 작용할 수 있습니다. DRA는 연결을 설정할 때 자체 Origin-Host 및 Realm 값을 광고합니다. 그러나 Diameter 애플리케이션 메시지는 실제 애플리케이션 호스트의 Origin-Host 및 Realm(예: PCEF, TDF, AF)을 사용하므로 PCRF는 올바른 호스트에 메시지를 전달하는 데 사용할 DRA 연결을 결정해야 합니다.



참고: Next Hop Routes 테이블은 PCRF에서 시작한 요청에만 사용됩니다. 수신 요청에 대한 응답은 항상 비대칭 라우팅을 방지하기 위해 수신한 동일한 연결을 통해 전송됩니다.

이러한 매개변수는 Next Hop Routing 테이블에서 구성할 수 있습니다.

매개변수	설명
다음 홉 영역	CER 또는 CEA의 Origin-Realm AVP에 수신된 DRA 영역 이름 메시지.
	 참고: 모든 다음 홉 영역(Next Hop Realm)은 들어오는 CER/CEA 메시지의 Origin-Realm A VP 값과 일치해야 합니다.
다음 홉 호스트	CER 또는 CEA의 Origin-Host AVP에 수신된 DRA 호스트 이름 목록

	메시지.
	 참고: 모든 다음 홉 호스트 이름(Next Hop Hosts)은 들어오는 CER/CEA 메시지의 Origin-Host A VP 값과 일치해야 합니다.
애플리케이션 ID	DRA에서 지원되는 것으로 광고된 직경 애플리케이션 ID입니다. It 에는 서비스가 제공하는 특정 서비스를 식별하는 정보가 포함되어 있습니다. 세션이 속합니다.
대상 영역 패턴	Origin-Realm AVP에 수신된 실제 대상 영역 이름 패턴 AAR 메시지. 패턴은 표준 Java 일반이어야 합니다 표현식 구문.
대상 호스트 패턴	의 Origin-Host AVP에서 수신된 실제 대상 호스트 이름 패턴 AAR 메시지 패턴은 표준 Java 패턴이어야 합니다. 표기 규칙. 패턴은 표준 Java 일반이어야 합니다 표현식 구문.

모범 사례:

의 Destination Realms Pattern(대상 영역 패턴) 및 Destination Host Pattern(대상 호스트 패턴) 열에 항목을 만드는 동안 항상 올바른 regex 패턴(와일드카드 일치)을 사용하십시오.

Next Hop Routing 테이블을 통해 Gx 및 Rx 피어의 컨피그레이션 항목을 최소화하고 컨피그레이션 오류를 방지할 수 있습니다.



참고: 자세한 컨피그레이션 지침은 Next Hop Routing(다음 홉 라우팅) 섹션 아래의 CPS Mobile Configuration Guide, Release 25.1.0을 참조하십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.