

AAA 재정의로 Catalyst 9800 무선 컨트롤러에 대한 QoS(BDRL) 속도 제한 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[예: 게스트 및 기업 QoS 정책](#)

[구성](#)

[AAA 서버 및 메서드 목록](#)

[WLAN 정책, 사이트 태그 및 AP 태그](#)

[QoS](#)

[다음을 확인합니다.](#)

[WLC에서](#)

[AP에서](#)

[패킷이 IO 그래프 분석을 캡처함](#)

[문제 해결](#)

[Flexconnect 로컬 스위칭\(또는 패브릭/SDA\) 시나리오](#)

[설정](#)

[Flexconnect/패브릭 문제 해결](#)

[참조](#)

소개

이 문서에서는 Catalyst 9800 Series Wireless Controller의 BDRL(Bi Directional Rate Limit) 컨피그레이션 예를 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- [Catalyst Wireless 9800 구성 모델](#)
- Cisco ISE(Identity Service Engine)를 사용하는 AAA

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 16.12.1s의 Cisco Catalyst 9800-CL Wireless Controller
- 버전 2.2의 Identity Service Engine

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.

배경 정보

9800 WLC 플랫폼의 QoS는 Catalyst 9000 플랫폼과 동일한 개념과 구성 요소를 사용합니다.

이 섹션에서는 이러한 구성 요소의 작동 방식 및 서로 다른 결과를 얻을 수 있도록 구성 방법을 전체적으로 설명합니다.

기본적으로 QoS 재귀는 다음과 같이 작동합니다.

1. Class-Map: 특정 유형의 트래픽을 식별합니다. 클래스 맵은 AVC(Application Visibility and Control) 엔진을 활용할 수 있습니다.


또한 사용자 지정 클래스 맵을 정의하여 ACL(Access Control List) 또는 DSCP(Differentiated Services Code Point)와 일치하는 트래픽을 식별할 수 있습니다

2. Policy-Map: Class-map에 적용되는 정책입니다.

이러한 정책은 클래스 맵과 일치하는 트래픽을 DSCP로 표시하거나 삭제 또는 속도 제한할 수 있습니다

4. Service-Policy: Policy-maps는 service-policy 명령을 사용하여 특정 방향의 SSID 또는 클라이언트당 정책 프로파일에 적용할 수 있습니다.

3. (선택 사항) Table-Map: 한 유형의 마크를 다른 유형으로 변환하는 데 사용됩니다(예: CoS를 DCSP로 변환).

 참고: Table-map에서 변경할 값(4~32)을 지정하고 policy-map에서는 기술이 지정됩니다 (COS에서 DSCP로).

class-map = MATCH

- AVC (Application or Group)
- User defined
 - ACL
 - DSCP

policy-map = TAKE ACTION

- Mark DSCP
- Drop
- Police (rate-limit)

service-policy = WHERE and DIRECTION

- Client Ingress / Egress
- SSID Ingress / Egress

 참고: 대상당 둘 이상의 정책이 적용되는 경우, 이 우선 순위에 따라 정책 해결이 선택됩니다.

- AAA 재정의(최고)
- 네이티브 프로파일링(로컬 정책)
- 구성된 정책
- 기본 정책(최저)

자세한 내용은 9800의 공식 [QoS 컨피그레이션 가이드](#)에서 확인할 수 있습니다

QoS 이론에 대한 자세한 내용은 [9000 Series QoS 컨피그레이션 가이드](#)에서 확인할 수 있습니다

예: 게스트 및 기업 QoS 정책

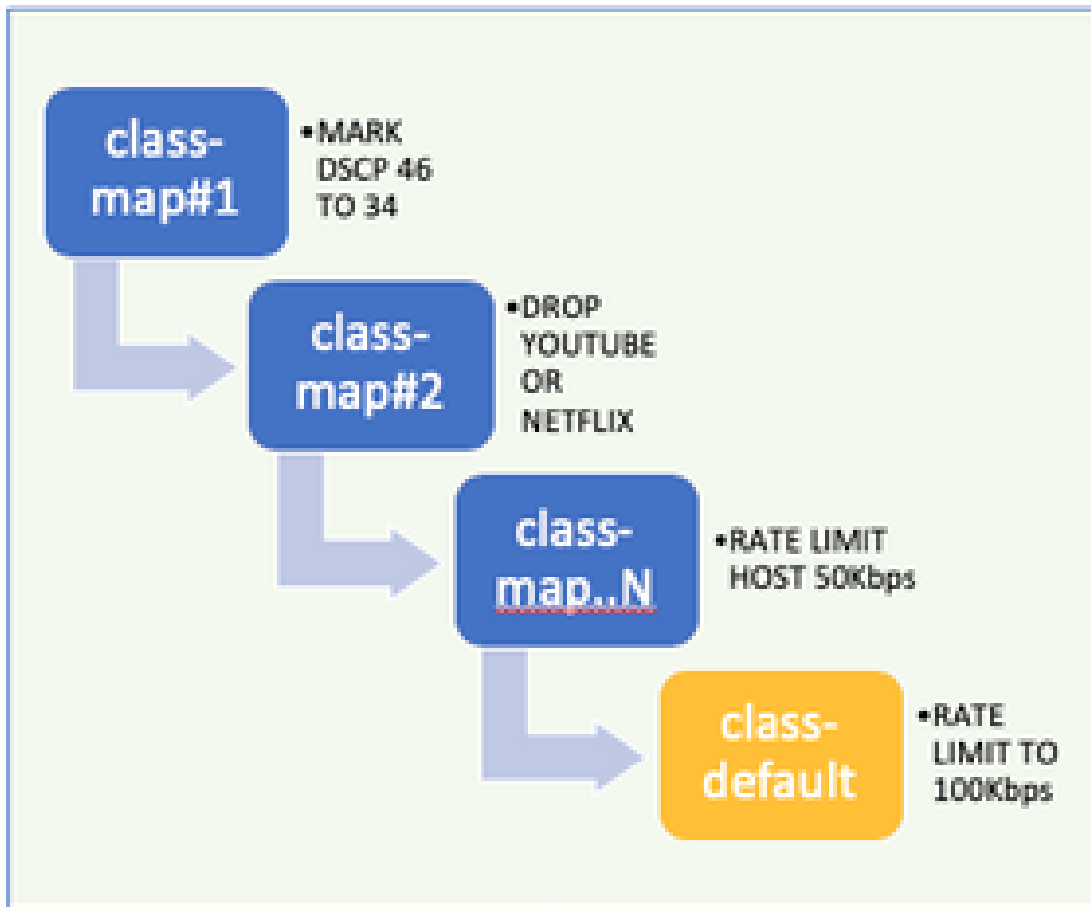
이 예에서는 설명된 QoS 구성 요소가 실제 시나리오에서 어떻게 적용되는지 보여줍니다.

이를 위해 게스트에 대해 다음과 같은 QoS 정책을 구성합니다.

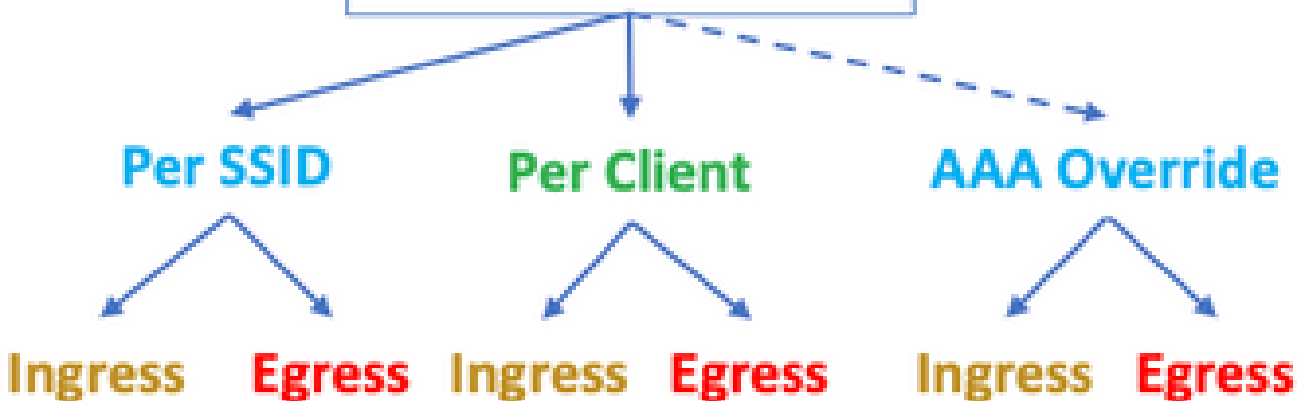
- 설명 DSCP
- Youtube 및 Netflix 비디오 삭제

- 속도 ACL에 지정된 호스트를 50Kbps로 제한
- 속도 기타 모든 트래픽을 100Kbps로 제한

POLICY MAP - Guest



POLICY-PROFILE-2



예를 들어 QoS 정책은 게스트 WLAN에 연결되는 정책 프로파일에 Ingress(인그레스) 및 Egress(이그레스) 양방향으로 SSID당 적용되어야 합니다.

구성

AAA 서버 및 메서드 목록

1단계. Configuration(컨피그레이션) > Security(보안) > AAA > Authentication(인증) > Servers/Groups(서버/그룹)로 이동하고 +Add(추가)를 선택합니다.

AAA 서버 이름, IP 주소 및 키를 입력합니다. 이는 ISE의 Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스) 아래에서 공유 비밀과 일치해야 합니다.

Name*	ISE22
IPv4 / IPv6 Server Address*	172.16.13.6
PAC Key	<input type="checkbox"/>
Key Type	0 ▾
Key*
Confirm Key*
Auth Port	1812
Acct Port	1813
Server Timeout (seconds)	1-1000
Retry Count	0-100
Support for CoA	ENABLED <input checked="" type="checkbox"/>

2단계. Configuration(컨피그레이션) > Security(보안) > AAA > Authentication(인증) > AAA Method List(AAA 방법 목록)로 이동하고 +Add(추가)를 선택합니다. Available Server Groups(가용 서버 그룹)에서 Assigned Server Groups(할당된 서버 그룹)를 선택합니다.

Method List Name*	ISE-Auth
Type*	dot1x
Group Type	group
Fallback to local	<input type="checkbox"/>
Available Server Groups	Assigned Server Groups
radius ldap tacacs+	ISE22G

3단계. Configuration(컨피그레이션) > Security(보안) > AAA > Authorization(권한 부여) > AAA method List(AAA 메서드 목록)로 이동하고 Add(추가)를 선택합니다. 유형으로 기본 방법과 "network"를 선택합니다.

Quick Setup: AAA Authorization

Method List Name*

default

Type*

network ▼

Group Type

group ▼

Fallback to local

Authenticated

Available Server Groups

ldap
tacacs+

>

<

Assigned Server

radius

이는 컨트롤러가 AAA 서버에서 반환한 권한 부여 특성(예: QoS 정책)을 적용하는 데 필요합니다. 그렇지 않으면 RADIUS에서 받은 정책이 적용되지 않습니다.

WLAN 정책, 사이트 태그 및 AP 태그

1단계. Configuration(컨피그레이션) > Wireless Setup(무선 설정) > Advanced(고급) > Start Now(지금 시작) > WLAN Profile(WLAN 프로파일)로 이동하고 +Add(추가)를 선택하여 새 WLAN을 생성합니다. SSID, 프로파일 이름, WLAN ID를 구성하고 상태를 enabled로 설정합니다.

그런 다음 Security(보안) > Layer 2(레이어 2)로 이동하여 레이어 2 인증 매개변수를 구성합니다.

General **Security** Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode Fast Transition

MAC Filtering Over the DS

Protected Management Frame

PMF Reassociation Timeout

WPA Parameters

WPA Policy

WPA2 Policy


WPA2 Encryption

AES(CCMP128)	<input checked="" type="checkbox"/>
CCMP256	<input type="checkbox"/>
GCMP128	<input type="checkbox"/>
GCMP256	<input type="checkbox"/>

MPSK

Auth Key Mgmt

802.1x	<input checked="" type="checkbox"/>
PSK	<input type="checkbox"/>
CCKM	<input type="checkbox"/>
FT + 802.1x	<input type="checkbox"/>
FT + PSK	<input type="checkbox"/>
802.1x-SHA256	<input type="checkbox"/>
PSK-SHA256	<input type="checkbox"/>

 SSID 보안은 QoS의 요구 사항으로 802.1x일 필요는 없지만 이 컨피그레이션 예에서는 AAA 재정의의 위해 사용됩니다.

2단계. Security(보안) > AAA로 이동하고 Authentication List(인증 목록) 드롭다운 상자에서 AAA 서버를 선택합니다.

General

Security

Advanced

Layer2

Layer3

AAA

Authentication List

ISE-Auth

Local EAP Authentication

3단계. Policy Profile(정책 프로파일)을 선택하고 +Add(추가)를 선택합니다. 정책 프로파일 이름을 구성합니다.

Status(상태)를 Enabled(활성화됨)로 설정하고, Central Switching(중앙 스위칭), Authentication(인증), DHCP 및 association(연결)도 활성화합니다.

General

Access Policies

QoS and AVC

Mobility

Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name*

QoS-PP

Description

QoS-PP

Status

ENABLED

Passive Client

DISABLED

Encrypted Traffic Analytics

DISABLED

CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

2-65519

WLAN Switching Policy

Central Switching

ENABLED

Central Authentication

ENABLED

Central DHCP

ENABLED

Central Association

ENABLED

Flex NAT/PAT

DISABLED

4단계. Access Policies(액세스 정책)로 이동하고 클라이언트가 SSID에 연결할 때 무선 클라이언트가 할당되는 VLAN을 구성합니다.

General	Access Policies	QOS and AVC	Mobility	Advanced
RADIUS Profiling	<input type="checkbox"/>			
Local Subscriber Policy Name	<input type="text" value="Search or Select"/> <input type="button" value="▼"/>			
WLAN Local Profiling				
Global State of Device Classification	Disabled ⓘ			
HTTP TLV Caching	<input type="checkbox"/>			
DHCP TLV Caching	<input type="checkbox"/>			
VLAN				
VLAN/VLAN Group	<input type="text" value="VLAN2613"/> <input type="button" value="▼"/>			
Multicast VLAN	<input type="text" value="Enter Multicast VLAN"/>			

5단계. Policy Tag(정책 태그)를 선택하고 +Add(추가)를 선택합니다. 정책 태그 이름을 구성합니다.

WLAN-Policy Maps(WLAN-정책 맵)의 +Add(추가)에서 WLAN Profile(WLAN 프로파일)을 선택하고 Policy Profile(정책 프로파일)을 선택한 후 구성할 맵에 대한 확인란을 선택합니다.

Name*

Description

WLAN-POLICY Maps: 0

WLAN Profile	Policy Profile
0 items per page No items to display	

Map WLAN and Policy

WLAN Profile* Policy Profile*

6단계. Site Tag(사이트 태그)를 선택하고 +Add(추가)를 선택합니다. AP가 로컬 모드에서 작동하려면 Enable Local Site(로컬 사이트 활성화) 상자를 선택합니다(또는 FlexConnect의 경우 선택하지 않음).

Name*

Description

AP Join Profile

Control Plane Name

7단계. Tag APs(태그 AP)를 선택하고 AP를 선택한 다음 Policy(정책), Site(사이트) 및 RF 태그를

추가합니다.

Tags

Policy	<input type="text" value="QoS-PT"/>	▼
Site	<input type="text" value="QoS-ST"/>	▼
RF	<input type="text" value="default-rf-tag"/>	▼

Changing AP Tag(s) will cause associated AP(s) to reconnect

QoS

1단계. Configuration(컨피그레이션) > Services(서비스) > QoS로 이동하고 +Add(추가)를 선택하여 QoS 정책을 생성합니다.

이름을 지정합니다(예: BWLimitAAClients).

Add QoS

Auto QoS

DISABLED

Policy Name*

BWLimitAAAClients

Description

Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined	Actions
◀ 0 ▶ 10 items per page No items to display							
+ Add Class-Maps x Delete							

Class Default

Mark	<input type="text" value="None"/>	Police(kbps)	<input type="text" value="8 - 10000000"/>
------	-----------------------------------	--------------	---

Drag and Drop, double click or click on the button to add/remove Profiles from Selected Profiles

Available (2)

Selected (0)

Profiles

Profiles

Ingress

Egress

2단계. Youtube와 Netflix를 삭제할 클래스 맵을 추가합니다. Add Class-Maps(클래스 맵 추가)를 클릭합니다. AVC, match any, drop action을 선택하고 두 프로토콜을 모두 선택합니다.

Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined	Actions
◀ 0 ▶ 10 items per page No items to display							
+ Add Class-Maps x Delete							
AVC/User Defined	<input type="text" value="AVC"/>						
Match	<input checked="" type="radio"/> Any <input type="radio"/> All						
Drop	<input checked="" type="checkbox"/>						
Match Type	<input type="text" value="protocol"/>						
Available Protocol(s)				Selected Protocol(s)			
<input type="text" value="netbios-ssn"/> <input type="text" value="netblt"/> <input type="text" value="netflow"/>				<input type="button" value=">"/>	<input type="text" value="youtube"/> <input type="text" value="netflix"/>		
				<input type="button" value="<"/>			
							Cancel Save

Save(저장)를 누릅니다.

3단계. DSCP 46~34를 나타내는 클래스 맵을 추가합니다.

Add Class-Maps를 클릭합니다.

- 일치 모두, 사용자 정의
- 일치 유형 DSCP
- 일치 값 46
- 표시 유형 DSCP
- 표시 값 34

Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined	Actions
<input type="checkbox"/>	protocol	youtube,netflix	None	8	Enabled	AVC	

10 items per page 1 - 1 of 1 items

+ Add Class-Maps Delete

AVC/User Defined User Defined

Match Any All

Match Type DSCP

Match Value* 46

Mark Type DSCP Mark Value 34

Drop

Police(kbps) 8 - 10000000

Cancel Save

Save(저장)를 누릅니다.

4단계. 특정 호스트에 대한 트래픽을 규칙화하는 클래스 맵을 정의하려면 해당 클래스 맵에 대한 ACL을 생성합니다.

Add Class-Maps(클래스 맵 추가)를 클릭합니다.

User Defined(사용자 정의), match any(일치 모두), match type ACL(일치 유형 ACL)을 선택하고, ACL name(여기서 specifichostACL), type(유형)none(없음)을 선택하고 rate limit(속도 제한) 값을 선택합니다.

저장을 클릭합니다.

	Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined	Actions
<input type="checkbox"/>	protocol	youtube,netflix	None		8	Enabled	AVC	
<input type="checkbox"/>	DSCP	46	DSCP	34		Disabled	User Defined	

10 items per page 1 - 2 of 2 items

AVC/User Defined:

Match: Any All

Match Type:

Match Value*:

Mark Type:

Drop:

Police(kbps):

다음은 특정 호스트 트래픽을 식별하는 데 사용하는 ACL의 예입니다.

Sequence	Action	Source IP	Source Wildcard	Destination IP	Destination Wildcard	Protocol	Source Port	Destination Port	DSCP	Log
<input type="checkbox"/> 1	permit	any		192.168.1.59		ip			None	Disablec
<input type="checkbox"/> 2	permit	192.168.1.59		any		ip			None	Disablec

10 items per page 1 - 2 of 2 items

5단계. 클래스 맵 프레임에서 기본 클래스를 사용하여 다른 모든 트래픽에 대한 속도 제한을 설정합니다.

이렇게 하면 위의 규칙 중 하나의 대상이 아닌 모든 클라이언트 트래픽에 대한 속도 제한이 설정됩니다.

	Match Type	Match Value	Mark Type	Mark Value	Police Value (kbps)	Drop	AVC/User Defined	Actions
<input type="checkbox"/>	protocol	youtube,netflix	None		8	Enabled	AVC	
<input type="checkbox"/>	DSCP	46	DSCP	34		Disabled	User Defined	
<input type="checkbox"/>	ACL	specifichostACL	None		50	Disabled	User Defined	

1 - 3 of 3 items

Class Default

Mark Police(kbps)

6단계. 하단의 Apply to Device(디바이스에 적용)를 클릭합니다.


CLI 등가 컨피그레이션:

```

policy-map BWLimitAAAclients
class BWLimitAAAclients1_AVC_UI_CLASS
  police cir 8000
  conform-action drop
  exceed-action drop
class BWLimitAAAclients1_ADV_UI_CLASS
  set dscp af41
class BWLimitAAAclients2_ADV_UI_CLASS
  police cir 50000
  conform-action transmit
  exceed-action drop
class class-default
  police cir 100000
  conform-action transmit
  exceed-action drop

class-map match-all BWLimitAAAclients1_AVC_UI_CLASS
  description BWLimitAAAclients1_AVC_UI_CLASS UI_policy_DO_NOT_CHANGE
  match protocol youtube
  match protocol netflix
class-map match-any BWLimitAAAclients1_ADV_UI_CLASS
  description BWLimitAAAclients1_ADV_UI_CLASS UI_policy_DO_NOT_CHANGE
  match dscp ef
class-map match-all BWLimitAAAclients2_ADV_UI_CLASS
  description BWLimitAAAclients2_ADV_UI_CLASS UI_policy_DO_NOT_CHANGE
  match access-group name specifichostACL
  
```

참고: 이 예에서는 AAA 재지정에 의해 적용되므로 QoS 정책에서 프로파일을 선택하지 않았 습니다. 그러나 정책 프로파일에 QoS 정책을 수동으로 적용하려면 원하는 프로파일을 선택합

 니다.

2단계. ISE에서 Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization Profiles(권한 부여 프로파일)로 이동하고 +Add(추가)에서 선택하여 권한 부여 프로파일을 생성합니다.

QoS 정책을 적용하려면 Cisco AV 쌍을 통해 고급 특성 설정으로 추가합니다.

ISE 인증 및 권한 부여 정책이 올바른 규칙과 일치하고 이 권한 부여 결과를 가져오도록 구성되어 있다고 가정합니다.


특성은 ip:sub-qos-policy-in=<policy name> 및 ip:sub-qos-policy-out=<policy name>입니다

▼ Advanced Attributes Settings

Cisco:cisco-av-pair	=	ip:sub-qos-policy-in=BWLimitA...	-
Cisco:cisco-av-pair	=	ip:sub-qos-policy-out=BWLimit...	+ +

▼ Attributes Details

```
Access Type = ACCESS_ACCEPT
cisco-av-pair = ip:sub-qos-policy-in=BWLimitAAAClients
cisco-av-pair = ip:sub-qos-policy-out=BWLimitAAAClients
```

 참고: 정책 이름은 대/소문자를 구분합니다. 케이스가 올바른지 확인하십시오!

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오:

WLC에서

```
# show run wlan
# show run aaa
# show aaa servers
# show ap tag summary
# show ap name <AP-name> tag detail
# show wireless tag policy summary
# show wireless tag policy detailed <policy-tag-name>
```

```
# show wireless profile policy detailed <policy-profile-name>
# show policy-map <policy-map name>
# sh policy-map interface wireless ssid/client profile-name <WLAN> radio type <2.4/5GHz> ap name <name>

# show wireless client mac <client-MAC-address> detail
# show wireless client <client-MAC-address> service-policy input
# show wireless client <client-MAC-address> service-policy output
```

```
To verify EDCS parameters :
sh controllers dot11Radio 1 | begin EDCA
```

<#root>

```
9800#show wireless client mac e836.171f.a162 det

Client MAC Address : e836.171f.a162
Client IPv4 Address : 192.168.1.11
Client IPv6 Addresses : fe80::c6e:2ca4:56ea:ffbf
                        2a02:a03f:42c2:8400:187c:4faf:c9f8:ac3c
                        2a02:a03f:42c2:8400:824:e15:6924:ed18
                        fd54:9008:227c:0:1853:9a4:77a2:32ae
                        fd54:9008:227c:0:1507:c911:50cd:2062

Client Username : Nico
AP MAC Address : 502f.a836.a3e0
AP Name: AP780C-F085-49E6
AP slot : 1
Client State : Associated
```

(...)

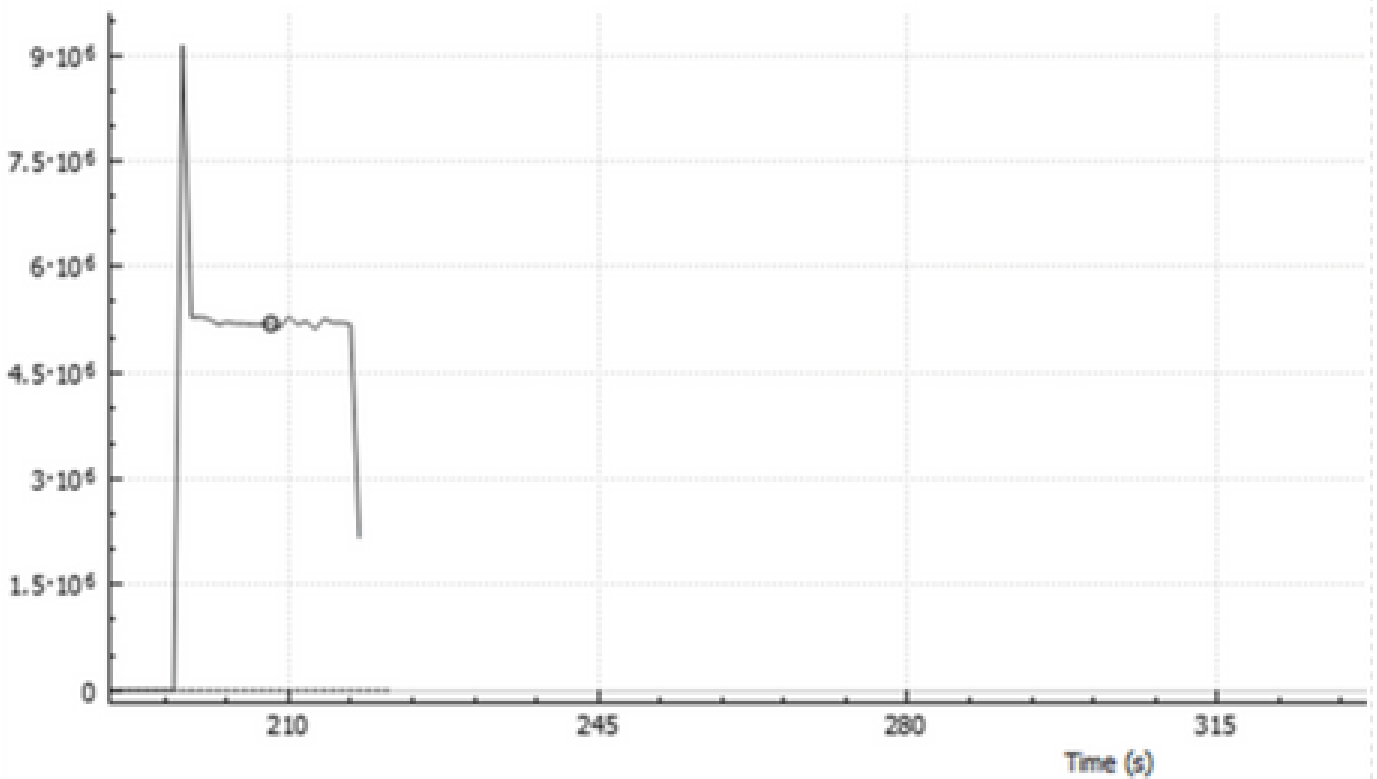
```
Local Policies:
  Service Template : wlan_svc_QoS-PP (priority 254)
    VLAN           : 1
    Absolute-Timer : 1800
Server Policies:
  Input QoS       : BWLimitAAAClients
  Output QoS      : BWLimitAAAClients
Resultant Policies:
  VLAN Name       : default
  Input QoS       : BWLimitAAAClients
  Output QoS      : BWLimitAAAClients
  VLAN           : 1
  Absolute-Timer : 1800
```

AP에서

AP가 로컬 모드이거나 SSID가 Flexconnect Central Switching 모드일 때 AP에서 트러블슈팅을 수행할 필요가 없습니다. WLC에서 QoS 및 서비스 정책을 수행했기 때문입니다.

패킷이 IO 그래프 분석을 캡처함

Wireshark IO Graphs: wireshark_59472C4E-A14B-4A09-9E28-CCECC128



Click to select packet 17372 (209s = 5.129e+6).

Enabled	Graph Name	Display Filter	Color	Style	Y Axis
<input checked="" type="checkbox"/>	All packets	tcp.port eq 8022	■	Line	Bits

문제 해결

이 섹션에서는 컨피그레이션 문제 해결에 대한 정보를 제공합니다.

1단계. 기존의 모든 디버그 조건을 지웁니다.

```
# clear platform condition all
```

2단계. 해당 무선 클라이언트에 대해 디버그를 활성화합니다.

```
# debug wireless mac <client-MAC-address> {monitor-time <seconds>}
```

3단계. 문제를 재현하기 위해 무선 클라이언트를 SSID에 연결합니다.

4단계. 문제가 재현되면 디버그를 중지합니다.

```
# no debug wireless mac <client-MAC-address>
```

테스트 중에 캡처된 로그는 로컬 파일의 WLC에 다음 이름으로 저장됩니다.

```
ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

GUI 워크플로를 사용하여 이 추적을 생성하는 경우, 저장되는 파일 이름은 debugTrace_aaaa.bbb.cccc.txt입니다.

5단계. 이전에 생성된 파일을 수집하려면 ra trace .log를 외부 서버에 복사하거나 화면에 출력을 직접 표시합니다.

다음 명령을 사용하여 RA 추적 파일의 이름을 확인합니다.

```
# dir bootflash: | inc ra_trace
```

파일을 외부 서버에 복사:

```
# copy bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log tftp://a.b.c.
```

또는 내용을 표시합니다.

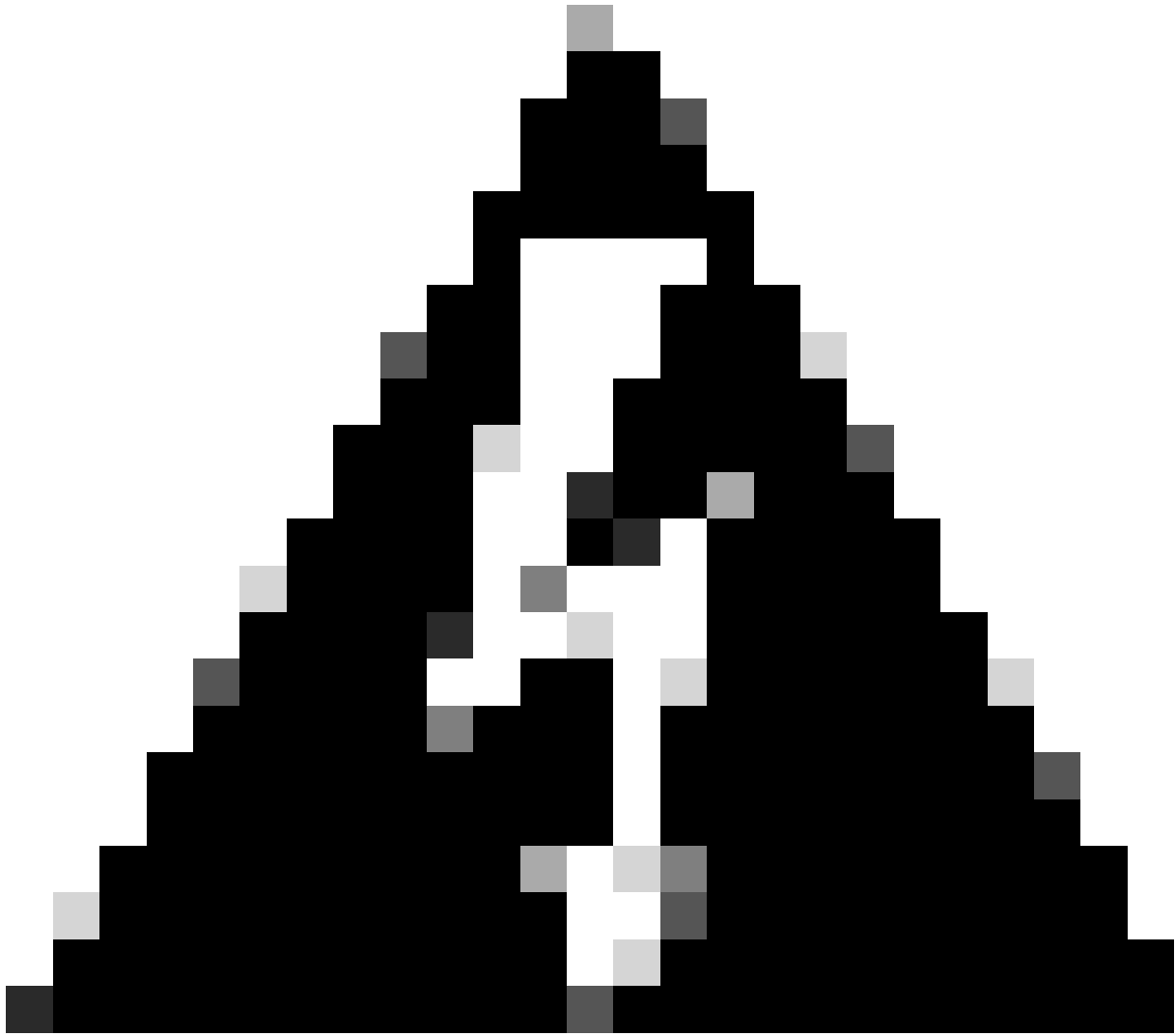
```
# more bootflash:ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log
```

6단계. 디버그 조건을 제거합니다.

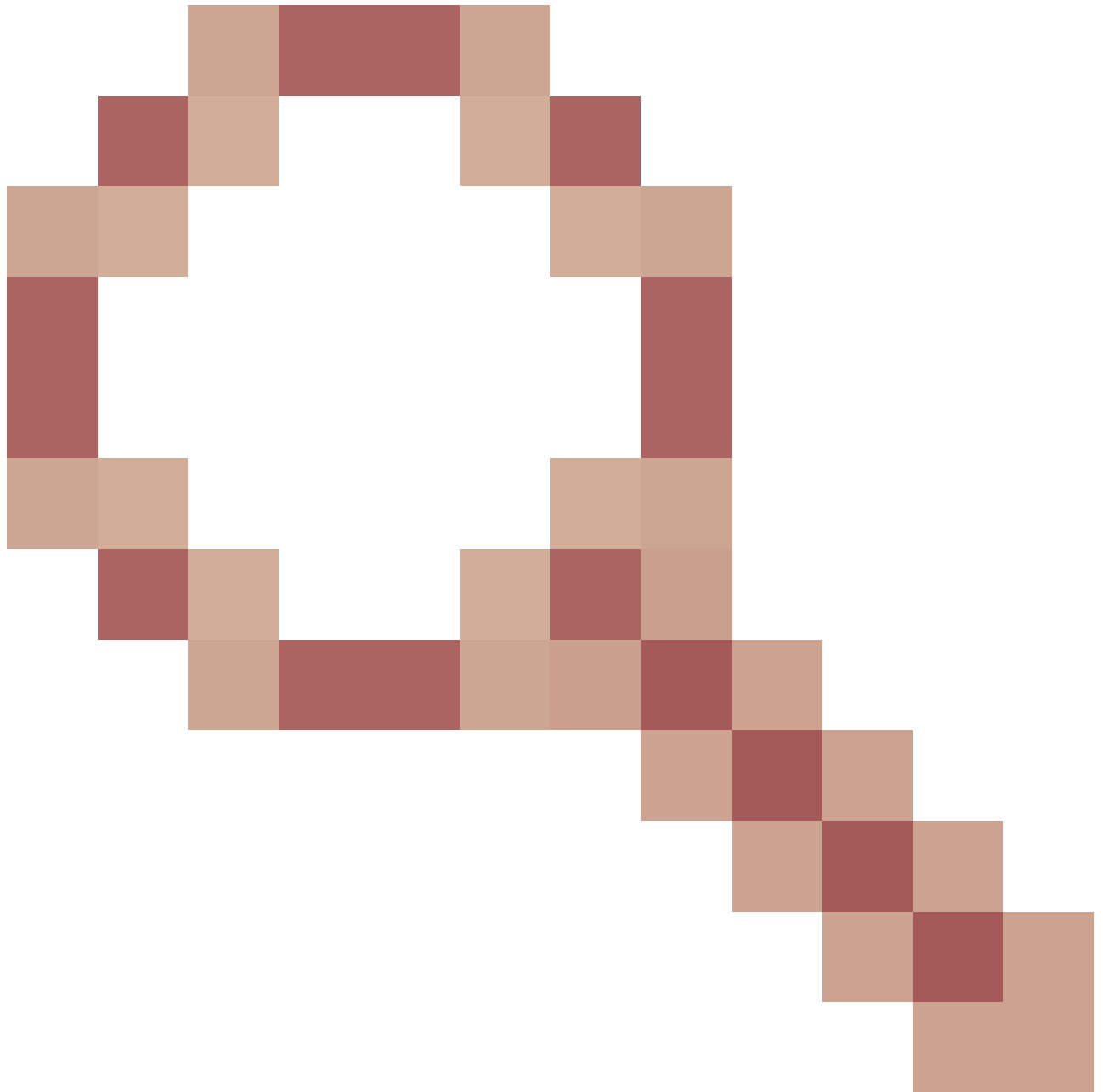
```
# clear platform condition all
```

Flexconnect 로컬 스위칭(또는 패브릭/SDA) 시나리오

flexconnect 로컬 스위칭(또는 패브릭/SDA)의 경우, WLC에서 정의한 모든 QoS 정책을 적용하는 AP입니다.



경고: Cisco 버그 ID [CSCwh74415](#)




때문에 RADIUS 서버에서 반환하는 최신 QoS 정책이 동일한 액세스 포인트에 연결하는 모든 클라이언트에 적용되므로 다른 모든 QoS 정책을 재정의합니다. AAA 재정의의 클라이언트당 속도 제한은 17.6.2 릴리스부터 더 이상 제대로 작동하지 않습니다. 버그 설명을 참조하여 수정된 릴리스를 확인하십시오.

wave2 및 11ax 액세스 포인트의 경우 속도 제한은 17.6 이전에는 클라이언트당 또는 SSID당이 아니라 플로우 단위(5튜플) 레벨에서 발생합니다. 이는 EWc-AP(Embedded Wireless Controller on Access Point) 구축의 Flexconnect/Fabric에 있는 AP에 적용됩니다.

17.5부터 AAA 재정의를 활용하여 클라이언트당 속도 제한을 달성하기 위해 특성을 푸시할 수 있습니다.

17.6부터 Flex 로컬 스위칭 구성의 802.11ac Wave 2 및 11ax AP에서 클라이언트당 양방향 속도 제한이 지원됩니다.

 참고: Flex AP는 QoS 정책에서 ACL의 존재를 지원하지 않습니다. 또한 CLI를 통해 구성할 수 있지만 9800 웹 UI에서는 사용할 수 없고 9800에서는 지원되지 않는 BRR(대역폭 유지) 및 정책 우선순위를 지원하지 않습니다. Cisco 버그 ID CSCvx81067은 플렉스 AP에 대한 QoS 정책에서 ACL의 지원을 추적합니다.

설정

구성은 두 가지 예외를 제외하고 이 문서의 첫 번째 부분과 정확히 같습니다.

1. 정책 프로파일이 로컬 스위칭으로 설정됩니다. Flex 구축에서는 Bengaluru 17.4 릴리스까지 중앙 연결을 비활성화해야 합니다.

17.5부터 이 필드는 하드코딩되므로 사용자 컨피그레이션에 사용할 수 없습니다.

WLAN Switching Policy

Central Switching



Central Authentication



Central DHCP



Central Association



Flex NAT/PAT



2. 사이트 태그가 로컬 사이트가 아닌 것으로 설정됩니다.

Enable Local Site



Flexconnect/패브릭 문제 해결

AP는 QoS 정책을 적용하는 디바이스이므로 이러한 명령을 사용하면 적용되는 항목을 좁힐 수 있습니다.

dot11 qos 표시

정책 맵 표시

show rate-limit 클라이언트

show rate-limit bssid

속도 제한 wlan 표시

flexconnect 클라이언트 표시

<#root>

AP780C-F085-49E6#

show dot11 qos

Qos Policy Maps (UPSTREAM)

ratelimit targets:

Client: A8:DB:03:6F:7A:46

platinum-up targets:

VAP: 0 SSID:LAB-DNAS

VAP: 1 SSID:VlanAssign

VAP: 2 SSID:LAB-Qos

Qos Stats (UPSTREAM)

total packets: 29279

dropped packets: 0

marked packets: 0

shaped packets: 0

policed packets: 182

copied packets: 0

DSCP TO DOT1P (UPSTREAM)

Default dscp2dot1p Table Value:

[0]->0 [1]->2 [2]->10 [3]->18 [4]->26 [5]->34 [6]->46 [7]->48

Active dscp2dot1p Table Value:

[0]->0 [1]->2 [2]->10 [3]->18 [4]->26 [5]->34 [6]->46 [7]->48

Trust DSCP Upstream : Disabled

Qos Policy Maps (DOWNSTREAM)

ratelimit targets:

Client: A8:DB:03:6F:7A:46

Qos Stats (DOWNSTREAM)

total packets: 25673

dropped packets: 0

marked packets: 0

shaped packets: 0

policed packets: 150

copied packets: 0

DSCP TO DOT1P (DOWNSTREAM)

Default dscp2dot1p Table Value:

[0]->0 [1]->-1 [2]->1 [3]->-1 [4]->1 [5]->-1 [6]->1 [7]->-1

[8]->-1 [9]->-1 [10]->2 [11]->-1 [12]->2 [13]->-1 [14]->2 [15]->-1

[16]->-1 [17]->-1 [18]->3 [19]->-1 [20]->3 [21]->-1 [22]->3 [23]->-1

[24]->-1 [25]->-1 [26]->4 [27]->-1 [28]->-1 [29]->-1 [30]->-1 [31]->-1

[32]->-1 [33]->-1 [34]->5 [35]->-1 [36]->-1 [37]->-1 [38]->-1 [39]->-1

[40]->-1 [41]->-1 [42]->-1 [43]->-1 [44]->-1 [45]->-1 [46]->6 [47]->-1

[48]->7 [49]->-1 [50]->-1 [51]->-1 [52]->-1 [53]->-1 [54]->-1 [55]->-1

[56]->7 [57]->-1 [58]->-1 [59]->-1 [60]->-1 [61]->-1 [62]->-1 [63]->-1

Active dscp2dot1p Table Value:

[0]->0 [1]->0 [2]->1 [3]->0 [4]->1 [5]->0 [6]->1 [7]->0

[8]->1 [9]->1 [10]->2 [11]->1 [12]->2 [13]->1 [14]->2 [15]->1

[16]->2 [17]->2 [18]->3 [19]->2 [20]->3 [21]->2 [22]->3 [23]->2

[24]->3 [25]->3 [26]->4 [27]->3 [28]->3 [29]->3 [30]->3 [31]->3

[32]->4 [33]->4 [34]->5 [35]->4 [36]->4 [37]->4 [38]->4 [39]->4

[40]->5 [41]->5 [42]->5 [43]->5 [44]->5 [45]->5 [46]->6 [47]->5

[48]->7 [49]->6 [50]->6 [51]->6 [52]->6 [53]->6 [54]->6 [55]->6

[56]->7 [57]->7 [58]->7 [59]->7 [60]->7 [61]->7 [62]->7 [63]->7

Profinet packet recieved from

wired port:

0

wireless port:

?

AP780C-F085-49E6#

show policy-map

2 policymaps

Policy Map BWLimitAAAClients type:qos client:default

Class BWLimitAAAClients_AVC_UI_CLASS

drop

Class BWLimitAAAClients_ADV_UI_CLASS

set dscp af41 (34)

```
Class class-default
  police rate 5000000 bps (625000Bytes/s)
  conform-action
  exceed-action
```

```
Policy Map platinum-up          type:qos client:default
  Class cm-dscp-set1-for-up-4
    set dscp af41 (34)
```

```
Class cm-dscp-set2-for-up-4
  set dscp af41 (34)
```

```
Class cm-dscp-for-up-5
  set dscp af41 (34)
```

```
Class cm-dscp-for-up-6
  set dscp ef (46)
```

```
Class cm-dscp-for-up-7
  set dscp ef (46)
```

```
Class class-default
  no actions
```

AP780C-F085-49E6#

show rate-limit client

Config:

	mac	vap	rt_rate_out	rt_rate_in	rt_burst_out	rt_burst_in	nrt_rate_out	nrt_rate_in	nrt_burst_out	nrt_burst_in
A8:DB:03:6F:7A:46		2	0	0	0	0	0	0	0	0

Statistics:

	name	up	down
	Unshaped	0	0
	Client RT pass	0	0
	Client NRT pass	0	0
	Client RT drops	0	0
	Client NRT drops	0	38621
		9 54922	0

AP780C-F085-49E6#

AP780C-F085-49E6#

show flexconnect client

Flexconnect Clients:

	mac	radio	vap	aid	state	encr	aaa-vlan	aaa-ac1	aaa-ipv6-ac1	assoc	auth	switching
A8:DB:03:6F:7A:46		1	2	1	FWD	AES_CCM128	none	none	none	Local	Central	Local

AP780C-F085-49E6#

참조

[Catalyst 9000 16.12 QoS 가이드](#)

[9800 QoS 컨피그레이션 가이드](#)

[Catalyst 9800 컨피그레이션 모델](#)

[Cisco IOS® XE 17.6 릴리스 정보](#)

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.