

# 컨버지드 액세스 컨트롤러 및 경량 AP의 QoS 컨피그레이션 예

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[L3 QoS 패킷 표시 개선 사항](#)

[MQC를 사용하여 QoS를 위한 무선 네트워크 구성](#)

[기본 하드코딩된 정책](#)

[플래티넘](#)

[골드](#)

[실버](#)

[브론즈](#)

[수동으로 구성](#)

[1단계: 음성 트래픽 식별 및 표시](#)

[2단계: 포트 레벨의 대역폭 및 우선순위 관리](#)

[3단계: SSID 레벨의 대역폭 및 우선순위 관리](#)

[4단계: CAC로 통화 제한](#)

[다음을 확인합니다.](#)

[show class-map](#)

[정책 맵 표시](#)

[wlan 표시](#)

[show policy-map 인터페이스](#)

[플랫폼 qos 정책 표시](#)

[show wireless client mac-address <mac> service policy](#)

[문제 해결](#)

## 소개

이 문서에서는 LAP(Lightweight Access Point)와 Cisco Catalyst 3850 스위치 또는 Cisco 5760 WLC(Wireless LAN Controller)를 사용하여 Cisco 통합 액세스 네트워크에서 QoS를 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

## 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- LAP 및 Cisco 통합 액세스 컨트롤러를 구성하는 방법에 대한 기본적인 지식
- 유선 네트워크에서 기본 라우팅 및 QoS를 구성하는 방법에 대한 지식

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS를 실행하는 Cisco Catalyst 3850 스위치입니까? XE 소프트웨어 릴리스 3.2.2(SE)
- Cisco IOS XE Software 릴리스 3.2.2(SE)를 실행하는 Cisco 5760 Wireless LAN Controller
- Cisco 3600 Series Lightweight 액세스 포인트

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

## 배경 정보

QoS는 네트워크에서 사용자 또는 애플리케이션 세트에 더 우수하거나 특별한 서비스를 제공하여 다른 사용자 또는 애플리케이션에 피해를 주는 기능을 의미합니다.

QoS를 사용하면 무선 LAN(WLAN) 및 WAN을 포함하는 LAN을 통해 대역폭을 보다 효율적으로 관리할 수 있습니다. QoS는 다음과 같은 서비스를 통해 안정적이고 향상된 네트워크 서비스를 제공합니다.

- 중요 사용자 및 애플리케이션을 위한 전용 대역폭을 지원합니다.
- 실시간 트래픽에 필요한 지터 및 레이턴시를 제어합니다.
- 네트워크 혼잡을 관리하고 최소화합니다.
- 트래픽 흐름을 원활하게 하기 위해 네트워크 트래픽을 셰이핑합니다.
- 네트워크 트래픽 우선순위를 설정합니다.

과거에는 WLAN이 주로 저대역폭 데이터 애플리케이션 트래픽을 전송하는 데 사용되었습니다. WLAN이 수직(소매, 금융, 교육 등) 및 엔터프라이즈 환경으로 확장됨에 따라 WLAN은 시간에 민감한 멀티미디어 애플리케이션과 함께 고대역폭 데이터 애플리케이션을 전송하는 데 사용됩니다. 이러한 요구 사항으로 인해 무선 QoS가 필요하게 되었습니다.

IEEE 802.11 표준 위원회 내의 IEEE 802.11e 작업 그룹은 표준 정의를 완료했으며, Wi-Fi Alliance는 WMM(Wi-Fi Multimedia) 인증을 생성했지만 802.11e 표준의 채택은 아직 제한적입니다. 802.11n 및 802.11ac 인증에는 WMM 인증이 필요하므로 대부분의 디바이스는 WMM 인증을 받았습니다. 많은 무선 디바이스는 데이터 링크 레이어로 전송된 패킷에 서로 다른 QoS 레벨을 할당하지 않으므로, 이러한 디바이스는 QoS 마킹 없이 상대 우선순위 지정 없이 대부분의 트래픽을 전송합니다. 그러나 대부분의 802.11 VoWLAN(Voice over Wireless LAN) IP 전화에서는 음성 트래픽을 표시하고 우선 순위를 지정합니다. 이 문서에서는 음성 트래픽을 표시하는 VoWLAN IP 전화 및 비디오 지원 wi-fi 디바이스에 대한 QoS 컨피그레이션에 대해 중점적으로 설명합니다.

**참고:** 내부 마킹을 수행하지 않는 장치의 QoS 구성이 이 문서의 범위를 벗어납니다.

802.11e 수정은 8개의 UP(User Priority) 레벨을 정의하며, 2를 4개의 QoS 레벨(액세스 범주)로 그룹화합니다.

- Platinum/Voice(UP 7 및 6) - PoS(Voice over Wireless)를 위한 고품질 서비스를 보장합니다.
- Gold/Video(UP 5 및 4) - 고품질 비디오 애플리케이션을 지원합니다.
- Silver/Best Effort(UP 3 및 0) - 클라이언트에 일반적인 대역폭을 지원합니다.이것이 기본 설정입니다.
- Bronze/Background(UP 2 및 1) - 게스트 서비스에 가장 낮은 대역폭을 제공합니다.

Platinum은 일반적으로 VoIP 클라이언트 및 비디오 클라이언트 Gold에 사용됩니다.이 문서에서는 컨트롤러에서 QoS를 구성하고 VoWLAN 및 비디오 클라이언트용 QoS로 구성된 유선 네트워크와 통신하는 방법을 설명하는 컨피그레이션 예를 제공합니다.

## L3 QoS 패킷 표시 개선 사항

Cisco 통합 액세스 컨트롤러는 WLC 및 LAP에서 보낸 패킷의 레이어 3(L3) IP DSCP(Differentiated Services Code Point) 표시를 지원합니다.이 기능은 AP(액세스 포인트)가 이 L3 정보를 사용하여 패킷이 AP에서 무선 클라이언트로 올바른 무선 우선 순위를 받도록 하는 방법을 개선합니다.

Catalyst 3850 스위치를 무선 컨트롤러로 사용하는 통합 액세스 WLAN 아키텍처에서 AP는 스위치에 직접 연결됩니다.5760 컨트롤러를 사용하는 통합 액세스 WLAN 아키텍처에서 WLAN 데이터는 CAPWAP(Control and Provisioning of Wireless Access Points) 프로토콜을 통해 AP와 WLC 간에 터널링됩니다.이 터널에서 원래 QoS 분류를 유지하려면 캡슐화된 데이터 패킷의 QoS 설정이 외부 터널 패킷의 레이어 2(L2)(802.1p) 및 L3(IP DSCP) 필드에 적절하게 매핑되어야 합니다.

VoWLAN 및 비디오에 대한 QoS를 구성할 때 무선 클라이언트에 대한 QoS 정책 및 WLAN에 관련된 정책 또는 둘 모두를 구성할 수 있습니다.특히 Catalyst 3850 스위치를 사용하여 AP를 연결하는 포트별 컨피그레이션으로 설정을 보완할 수도 있습니다.이 컨피그레이션 예에서는 무선 클라이언트, WLAN 및 AP에 대한 포트에 중점을 둡니다.VoWLAN 및 비디오 애플리케이션에 대한 QoS 컨피그레이션의 주요 목표는 다음과 같습니다.

- 업스트림 및 다운스트림 모두에서 음성 및 비디오 트래픽(트래픽 분류 및 표시)을 인식합니다.
- 음성 및 비디오 트래픽을 음성 우선 순위 수준으로 표시: 802.11e UP 6, 802.1p 5, DSCP 46 for voice802.11e UP 5, DSCP 34(비디오용)
- 음성 트래픽, 음성 신호 처리 및 비디오 트래픽에 대역폭을 할당합니다.

## MQC를 사용하여 QoS를 위한 무선 네트워크 구성

QoS를 구성하기 전에 기본 작동을 위해 Catalyst 3850 스위치 또는 Cisco 5760 WLC의 WCM(Wireless Controller Module) 기능을 구성하고 LAP를 WCM에 등록해야 합니다.이 문서에서는 WCM이 기본 작업을 위해 구성되었으며 LAP가 WCM에 등록되었다고 가정합니다.

통합 액세스 솔루션은 MQC(Modular QoS) CLI(Command Line Interface)를 사용합니다. Catalyst 3850 스위치에서 QoS 컨피그레이션에서 MQC를 사용하는 방법에 대한 자세한 내용은 [QoS 컨피그레이션 가이드, Cisco IOS XE Release 3SE\(Catalyst 3850 스위치\)](#)를 참조하십시오.

통합된 액세스 컨트롤러에서 MQC를 사용하는 QoS의 컨피그레이션은 다음 4가지 요소에 의존합니다.

- **클래스 맵**은 관심 트래픽을 인식하기 위해 사용됩니다.클래스 맵은 관심 있는 트래픽을 식별하기 위해 다양한 기술(예: 기존 QoS 마킹, 액세스 목록 또는 VLAN)을 사용할 수 있습니다.

- **정책 맵**은 관심 트래픽에 어떤 QoS 설정을 적용할지 결정하기 위해 사용됩니다. 정책 맵은 클래스 맵을 호출하고 각 클래스에 다양한 QoS 설정(예: 특정 표시, 우선순위 레벨, 대역폭 할당 등)을 적용합니다.
- **서비스 정책**은 네트워크의 전략적 지점에 정책 맵을 적용하기 위해 사용됩니다. 통합 액세스 솔루션에서 서비스 정책을 사용자, SSID(Service Set Identifier), AP 무선 장치 및 포트에 적용할 수 있습니다. 사용자가 포트, SSID 및 클라이언트 정책을 구성할 수 있습니다. 무선 정책은 무선 제어 모듈에 의해 제어됩니다. 포트, SSID, 클라이언트 및 무선에 대한 무선 QoS 정책은 스위치나 컨트롤러에서 무선 클라이언트로 트래픽이 이동할 때 다운스트림 방향으로 적용됩니다.
- **표 맵**은 수신 QoS 마킹을 검사하고 발신 QoS 표시를 결정하기 위해 사용됩니다. 테이블 맵은 SSID에 적용된 정책 맵에 배치됩니다. 표 맵을 사용하여 표시를 유지(복사)하거나 변경할 수 있습니다. 또한 테이블 맵을 사용하여 유무선 마킹 간에 매핑을 만들 수 있습니다. 유선 마킹은 DSCP(L3 QoS) 또는 802.1p(L2 QoS)를 사용합니다. 무선 표시에서는 UP(사용자 우선 순위)를 사용합니다. 테이블 맵은 관심 있는 각 UP에 어떤 DSCP 마킹을 사용해야 하는지, 관심 있는 각 DSCP 값에 어떤 UP를 사용해야 하는지를 결정하는 데 일반적으로 사용됩니다. DSCP와 UP 값 간에 직접 변환이 없기 때문에 표 맵은 통합된 액세스 QoS에 필수적입니다.

그러나 DSCP에서 UP 테이블 맵까지 복사 명령을 허용합니다. 이 경우 통합 액세스 솔루션은 DSCP에서 UP로 또는 UP에서 DSCP로 DSCP 변환을 결정하기 위해 AVVID(Cisco Architecture for Voice, Video, and Integrated Data) 매핑 테이블을 사용합니다.

레이블 인덱스	키 필드	수신 값	외부 DSCP	CoS	위로
0	N.A.	선택되지 않음	0	0	0
1-10	DSCP	0-7	0-7	0	0
11-18	DSCP	8-15	8-15	1	2
19-26	DSCP	16-23	16-23	2	3
27-34	DSCP	24-31	24-31	3	4
35-46	DSCP	32-39	32-39	4	5
47-48	DSCP	40-47	40-47	5	6
49-63	DSCP	48-55	48-55	6	7
64	DSCP	56-63	56-63	7	7
65	CoS	0	0	0	0
66	CoS	1	8	1	2
67	CoS	2	16	2	3
68	CoS	3	24	3	4
69	CoS	4	32	4	5
70	CoS	5	40	5	6
71	CoS	6	48	6	7
72	CoS	7	56	7	7
73	위로	0	0	0	0
74	위로	1	8	1	1
75	위로	2	16	1	2
76	위로	3	24	2	3
77	위로	4	34	3	4
78	위로	5	34	4	5
79	위로	6	46	5	6
80	위로	7	46	7	7

## 기본 하드코딩된 정책

통합 액세스 컨트롤러는 WLAN에 적용할 수 있는 하드코딩된 QoS 정책 프로파일을 채택합니다. 이러한 프로파일은 Cisco CUWN(Unified Wireless Networks) 컨트롤러 관리자에게 익숙한 금속 정책(플

래티넘, 골드 등)을 적용합니다. 음성 트래픽에 특정 대역폭을 할당하는 정책을 생성하지 않고 음성 트래픽이 적절한 QoS 마킹을 수신하도록 하는 것이 목표인 경우 하드코딩된 정책을 사용할 수 있습니다. 하드 코딩된 정책은 WLAN에 적용할 수 있으며 업스트림 및 다운스트림 방향에서 다를 수 있습니다.

## 참고:

이 [섹션](#)에 사용된 명령에 대한 자세한 내용을 보려면 [Command Lookup Tool](#)([등록된](#) 고객만 해당)을 사용합니다.

Output [Interpreter 도구](#)([등록된](#) 고객만 해당)는 특정 **show** 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

## 플래티넘

음성에 대한 하드코딩된 정책을 플래티넘이라고 합니다. 이름을 변경할 수 없습니다.

플래티넘 QoS 레벨에 대한 다운스트림 정책입니다.

```
Policy-map platinum
Class class-default
  set dscp dscp table plat-dscp2dscp
  set wlan user-priority dscp table plat-dscp2up
Table-map plat-dscp2dscp
  from 45 to 45
  from 46 to 46
  from 47 to 47
  default copy
Table-map plat-dscp2up
  from 34 to 4
  from 46 to 6
  default copy
```

Platinum QoS 레벨에 대한 업스트림 정책입니다.

```
Policy-map platinum-up
Class class-default
  set dscp wlan user-priority table plat-up2dscp
Table-map plat-up2dscp
  from 4 to 34
  from 5 to 34
  from 6 to 46
  from 7 to 8
  default copy
```

## 골드

비디오에 대한 하드코딩된 정책을 금이라고 합니다. 이름을 변경할 수 없습니다.

골드 QoS 레벨에 대한 다운스트림 정책입니다.

```
Policy Map gold
  Class class-default
    set dscp dscp table gold-dscp2dscp
    set wlan user-priority dscp table gold-dscp2u
```

```
Table Map gold-dscp2dscp
  from 45 to 34
  from 46 to 34
  from 47 to 34
  default copy
```

```
Table Map gold-dscp2up
  from 45 to 4
  from 46 to 4
  from 47 to 4
  default copy
```

**골드 QoS 레벨에 대한 업스트림 정책입니다.**

```
Policy Map gold-up
  Class class-default
    set dscp wlan user-priority table gold-up2dscp
```

```
Table Map gold-up2dscp
  from 6 to 34
  from 7 to 34
  default copy
```

## 실버

**최선의 노력을 위해 하드코딩된 정책을 은이라고 한다.이름을 변경할 수 없습니다.**

**은 QoS 레벨에 대한 다운스트림 정책입니다.**

```
Policy Map silver
  Class class-default
    set dscp dscp table silver-dscp2dscp
    set wlan user-priority dscp table silver-dscp2up
```

```
Table Map silver-dscp2dscp
  from 34 to 0
  from 45 to 0
  from 46 to 0
  from 47 to 0
  default copy
```

```
Table Map silver-dscp2up
  from 34 to 0
  from 45 to 0
  from 46 to 0
  from 47 to 0
  default copy
```

**은 QoS 레벨에 대한 업스트림 정책입니다.**

```
Policy Map silver-up
  Class class-default
    set dscp wlan user-priority table silver-up2dscp
```

```
Table Map silver-up2dscp
  from 4 to 0
  from 5 to 0
```

```
from 6 to 0
from 7 to 0
default copy
```

## 브론즈

백그라운드 트래픽에 대한 하드코딩된 정책을 bronze라고 합니다.이름을 변경할 수 없습니다.

Bronze QoS 레벨에 대한 다운스트림 정책입니다.

```
Policy Map bronze
  Class class-default
    set dscp dscp table bronze-dscp2dscp
  set wlan user-priority dscp table bronze-dscp2up
```

```
Table Map bronze-dscp2dscp
  from 0 to 8
  from 34 to 8
  from 45 to 8
  from 46 to 8
  from 47 to 8
  default copy
```

```
Table Map bronze-dscp2up
  from 0 to 1
  from 34 to 1
  from 45 to 1
  from 46 to 1
  from 47 to 1
  default copy
```

브론즈 QoS 레벨에 대한 업스트림 정책입니다.

```
Policy Map bronze-up
  Class class-default
    set dscp wlan user-priority table bronze-up2dscp
```

```
Table Map bronze-up2dscp
  from 0 to 8
  from 1 to 8
  from 4 to 8
  from 5 to 8
  from 6 to 8
  from 7 to 8
  default copy
```

지정된 SSID에 대한 대상 트래픽과 가장 일치하는 테이블 맵을 결정했으면 일치하는 정책을 WLAN에 적용할 수 있습니다.이 예에서는 하나의 정책이 다운스트림 방향(출력, AP에서 무선 클라이언트로)에 적용되고 업스트림 방향(입력, 무선 클라이언트, AP를 통해 컨트롤러에 대한 입력)에 정책이 적용됩니다.

```
3850#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
3850(config)#wlan test1
3850(config-wlan)#service-policy output platinum
3850(config-wlan)#service-policy input platinum-up
3850(config-wlan)#end
3850#
```

WLAN에 어떤 정책이 적용되었는지 확인하려면 WLAN 컨피그레이션을 확인합니다.

3850#show wlan name test1

WLAN Profile Name : test1

```
=====
Identifier : 1
Network Name (SSID) : test1
Status : Disabled
Broadcast SSID : Enabled
Maximum number of Associated Clients : 0
AAA Policy Override : Disabled
Network Admission Control
  NAC-State : Disabled
Number of Active Clients : 0
Exclusionlist Timeout : 60
Session Timeout : 1800 seconds
CHD per WLAN : Enabled
Webauth DHCP exclusion : Disabled
Interface : default
Interface Status : Up
Multicast Interface : Unconfigured
WLAN IPv4 ACL : unconfigured
WLAN IPv6 ACL : unconfigured
DHCP Server : Default
DHCP Address Assignment Required : Disabled
DHCP Option 82 : Disabled
DHCP Option 82 Format : ap-mac
DHCP Option 82 Ascii Mode : Disabled
DHCP Option 82 Rid Mode : Disabled
QoS Service Policy - Input
  Policy Name : platinum-up
  Policy State : Validation Pending
QoS Service Policy - Output
  Policy Name : platinum
  Policy State : Validation Pending
QoS Client Service Policy
  Input Policy Name : unknown
  Output Policy Name : unknown
WMM : Allowed
Channel Scan Defer Priority:
  Priority (default) : 4
  Priority (default) : 5
  Priority (default) : 6
Scan Defer Time (msecs) : 100
Media Stream Multicast-direct : Disabled
CCX - AironetIe Support : Enabled
CCX - Gratuitous ProbeResponse (GPR) : Disabled
CCX - Diagnostics Channel Capability : Disabled
Dot11-Phone Mode (7920) : Invalid
Wired Protocol : None
Peer-to-Peer Blocking Action : Disabled
Radio Policy : All
DTIM period for 802.11a radio : 1
DTIM period for 802.11b radio : 1
Local EAP Authentication : Disabled
Mac Filter Authorization list name : Disabled
Accounting list name : Disabled
802.1x authentication list name : Disabled
Security
  802.11 Authentication : Open System
  Static WEP Keys : Disabled
  802.1X : Disabled
  Wi-Fi Protected Access (WPA/WPA2) : Enabled
    WPA (SSN IE) : Disabled
```

```

WPA2 (RSN IE) : Enabled
  TKIP Cipher : Disabled
  AES Cipher : Enabled
Auth Key Management
  802.1x : Enabled
  PSK : Disabled
  CCKM : Disabled
CKIP : Disabled
IP Security : Disabled
IP Security Passthru : Disabled
L2TP : Disabled
Web Based Authentication : Disabled
Conditional Web Redirect : Disabled
Splash-Page Web Redirect : Disabled
Auto Anchor : Disabled
Sticky Anchoring : Enabled
Cranite Passthru : Disabled
Fortress Passthru : Disabled
PPTP : Disabled
Infrastructure MFP protection : Enabled
Client MFP : Optional
Webauth On-mac-filter Failure : Disabled
Webauth Authentication List Name : Disabled
Webauth Parameter Map : Disabled
Tkip MIC Countermeasure Hold-down Timer : 60
Call Snooping : Disabled
Passive Client : Disabled
Non Cisco WGB : Disabled
Band Select : Disabled
Load Balancing : Disabled
IP Source Guard : Disabled

```

## 수동으로 구성

하드코딩된 정책은 기본 QoS 표시를 적용하지만 대역폭 할당은 적용하지 않습니다. 또한 하드 코딩된 정책은 트래픽이 이미 표시되어 있다고 가정합니다. 복잡한 환경에서는 정책 조합을 사용하여 음성 및 비디오 트래픽을 적절하게 인식 및 표시하고, 다운스트림 및 업스트림 방향의 대역폭 할당을 설정하고, 무선 셀에서 시작된 통화 수를 제한하기 위해 통화 허용 제어를 사용할 수 있습니다.

**참고:** 이 [섹션](#)에 사용된 명령에 대한 자세한 내용을 보려면 [Command Lookup Tool\(등록된 고객만 해당\)](#)을 사용합니다.

### 1단계: 음성 트래픽 식별 및 표시

첫 번째 단계는 음성 및 비디오 트래픽을 인식하는 것입니다. 음성 트래픽은 두 가지 범주로 분류할 수 있습니다.

- 음성 흐름 - 커뮤니케이션의 오디오 부분을 전달합니다.
- 음성 신호 - 음성 엔드포인트 간에 교환되는 통계 정보를 전달합니다.

음성 흐름은 일반적으로 16384 - 32767 범위의 RTP(Real-time Transport Protocol) 및 UDP(User Datagram Protocol) 대상 포트를 사용합니다. 범위는 다음과 같습니다. 실제 포트는 일반적으로 좁으며 구현에 따라 달라집니다.

여러 음성 신호 프로토콜이 있습니다. 이 컨피그레이션 예에서는 Jabber를 사용합니다. Jabber는 다

음과 같은 TCP 포트를 연결 및 디렉토리에 사용합니다.

- TCP 80(HTTP)
- 143(IMAP(Internet Message Access Protocol))
- 443(HTTPS)
- Cisco Unified MeetingPlace 또는 Cisco WebEx와 회의를 위한 서비스 및 음성 메일 기능을 위한 Cisco Unity 또는 Cisco Unity Connection과 같은 서비스에 대한 993(IMAP)
- TCP 389/636(연락처 검색을 위한 LDAP(Lightweight Directory Access Protocol) 서버)
- FTP(1080)
- 피어 또는 서버에서 파일 전송(컨피그레이션 파일 등)을 위한 TFTP(UDP 69)

이러한 서비스에는 특정 우선 순위가 필요하지 않을 수 있습니다.

Jabber는 음성 신호 처리를 위해 SIP(Session Initiation Protocol)(UDP/TCP 5060 및 5061)를 사용합니다.

비디오 트래픽은 구현에 따라 다른 포트 및 프로토콜을 사용합니다.이 컨피그레이션 예에서는 비디오 컨퍼런스에 Tandberg PrecisionHD 720p 카메라를 사용합니다.Tandberg PrecisionHD 720p 카메라는 여러 코덱을 사용할 수 있습니다.사용된 대역폭은 선택한 코덱에 따라 달라집니다.

- C20, C40 및 C60 코덱은 H.323/SIP를 사용하며 포인트 투 포인트 연결에서 최대 6Mbps의 대역폭을 사용할 수 있습니다.
- C90 코덱은 동일한 프로토콜을 사용하며 멀티 사이트 통신에서 최대 10Mbps의 대역폭을 사용할 수 있습니다.

H.323의 Tandberg 구현에서는 일반적으로 스트리밍 비디오에 UDP 970, 비디오 시그널링에 UDP 971, 스트리밍 오디오에 UDP 972, 오디오 시그널링에 UDP 973을 사용합니다.Tandberg 카메라는 다음과 같은 다른 포트도 사용합니다.

- UDP 161
- UDP 962(SNMP(Simple Network Management Protocol))
- TCP 963(netlog), TCP 964(FTP)
- TCP 965(가상 네트워크 컴퓨팅[VNC])
- UDP 974(SAP(Session Announcement Protocol))

이러한 추가 포트에는 특정 우선 순위가 필요하지 않을 수 있습니다.

트래픽을 식별하는 일반적인 방법은 관심 트래픽을 대상으로 하는 클래스 맵을 만드는 것입니다.각 클래스 맵은 음성 및 비디오 포트를 사용하는 모든 트래픽을 대상으로 하는 액세스 목록을 가리킬 수 있습니다.

```
ip access-list extended JabberVOIP
permit udp any any range 16384 32767
ip access-list extended JabberSIGNALING
permit tcp any any range 5060 5061
permit udp any any range 5060 5061
ip access-list extended H323Videostream
permit udp any any eq 970
ip access-list extended H323Audiostream
permit udp any any eq 972
ip access-list extended H323VideoSignaling
permit udp any any eq 971
ip access-list extended H323AudioSignaling
permit udp any any eq 973
```

그런 다음 각 트래픽 유형에 대해 하나의 클래스 맵을 만들 수 있습니다.각 클래스 맵은 관련 액세스

목록을 가리킵니다.

```
class-map RTPaudio
match access-group name JabberVOIP
match access-group name H323Audiostream
class-map H323realtimevideo
match access-group name H323Videostream
class-map signaling
match access-group name JabberSIGNALING
match access-group name H323VideoSignaling
match access-group name H323AudioSignaling
```

클래스 맵을 통해 음성 트래픽과 비디오 트래픽이 식별되면 트래픽이 올바르게 표시되는지 확인합니다. 이 작업은 테이블 맵을 통해 WLAN 레벨에서 수행할 수 있으며 클라이언트 정책 맵을 통해 수행할 수도 있습니다.

표 맵은 수신 트래픽의 QoS 마킹을 검사하고 발신 QoS 마킹을 결정합니다. 따라서 Table-map은 수신 트래픽에 이미 QoS 표시가 있는 경우 유용합니다. 테이블 맵은 SSID 레벨에서만 사용됩니다.

반면 정책 맵은 클래스 맵으로 식별되는 트래픽을 대상으로 할 수 있으며, 잠재적으로 태그가 지정되지 않은 트래픽에 더 잘 적용합니다. 이 컨피그레이션 예에서는 유선 측으로부터의 트래픽이 Catalyst 3850 스위치 또는 Cisco 5760 WLC로 들어가기 전에 이미 올바르게 표시되었다고 가정합니다. 그렇지 않은 경우 정책 맵을 사용하여 SSID 레벨에서 클라이언트 정책으로 적용할 수 있습니다. 무선 클라이언트의 트래픽이 표시되지 않았을 수 있으므로 음성 및 비디오 트래픽을 올바르게 표시해야 합니다.

- 실시간 음성은 DSCP 46(EF[Raped Forwarding])으로 표시되어야 합니다.
- 비디오는 DSCP 34로 표시되어야 합니다(Assured Forwarding Class 41 [AF41]).
- 음성 및 비디오에 대한 신호 처리는 DSCP 24(Class Selector Service 값 3[CS3])로 표시되어야 합니다.

이러한 표시를 적용하려면 다음 각 클래스를 호출하고 해당 트래픽을 표시하는 정책 맵을 만듭니다

```
policy-map taggingPolicy
class RTPaudio
set dscp ef

class H323realtimevideo
set dscp af41

class signaling
set dscp cs3
```

## 2단계:포트 레벨의 대역폭 및 우선순위 관리

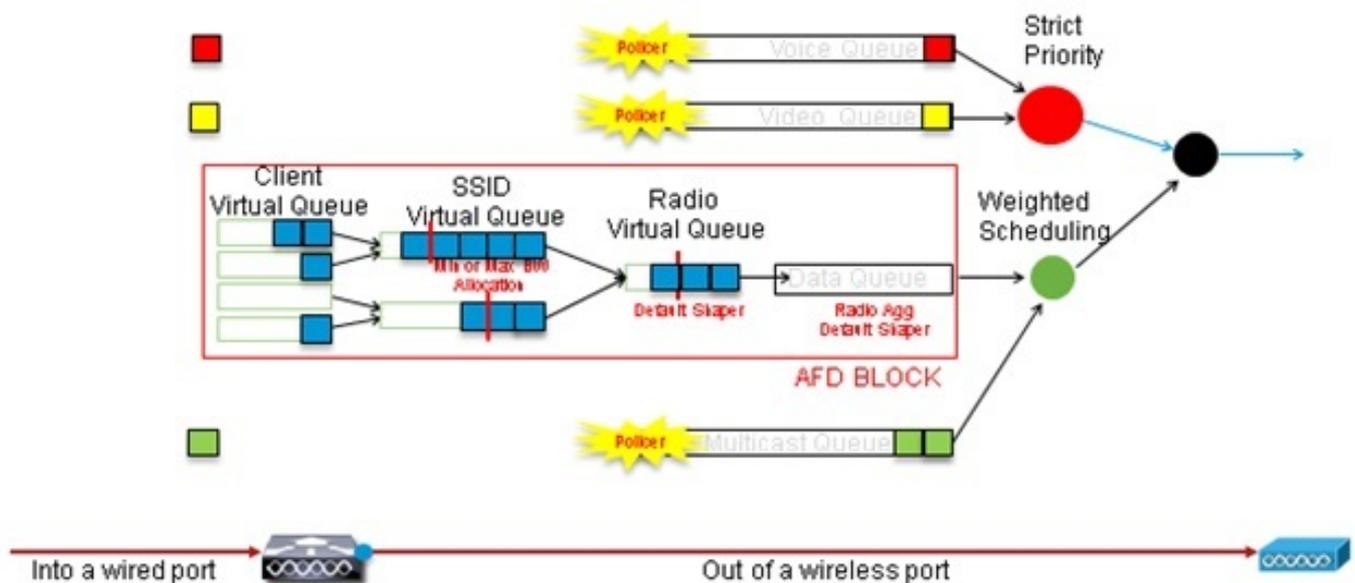
다음 단계는 AP로 이동하여 오는 포트에 대한 QoS 정책을 결정하는 것입니다. 이 단계는 주로 Catalyst 3850 스위치에 적용됩니다. Cisco 5760 컨트롤러에서 컨피그레이션을 수행한 경우 이 단계는 필수 단계가 아닙니다. Catalyst 3850 포트는 무선 클라이언트 및 AP를 오가는 음성 및 비디오 트래픽을 전달합니다. 이 컨텍스트의 QoS 컨피그레이션은 두 가지 요구 사항과 일치합니다.

1. **대역폭을 할당합니다.** 각 트래픽 유형에 할당되는 대역폭의 양을 결정할 수 있습니다. 이러한 대역폭 할당은 SSID 레벨에서도 수행할 수 있습니다. 대상 SSID를 제공하는 각 AP에서 수신할 수 있는 대역폭의 양을 구체화하려면 포트 대역폭 할당을 설정합니다. 이 대역폭은 대상

AP의 모든 SSID에 대해 설정되어야 합니다. 이 간소화된 컨피그레이션 예에서는 SSID와 AP가 하나만 있다고 가정합니다. 따라서 음성 및 비디오에 대한 포트 대역폭 할당은 SSID 레벨에서 음성 및 비디오에 대한 전역 대역폭 할당과 동일합니다. 각 트래픽 유형은 6Mbps에 할당되며 이 할당된 대역폭을 초과하지 않도록 폴리싱됩니다.

2. **트래픽의 우선 순위를 지정합니다.** 포트에는 4개의 대기열이 있습니다. 처음 두 개의 대기열은 우선 순위가 지정되고 실시간 트래픽(일반적으로 음성 및 비디오)용으로 예약됩니다. 네 번째 큐는 비실시간 멀티캐스트 트래픽용으로 예약되며, 세 번째 큐에는 다른 모든 트래픽이 포함됩니다. 통합된 액세스 대기열 로직을 사용하면 각 클라이언트에 대한 트래픽이 가상 대기열에 할당되며, 여기서 QoS를 구성할 수 있습니다. 클라이언트 QoS 정책의 결과는 SSID 가상 대기열에 삽입되며 QoS도 구성할 수 있습니다. 지정된 AP 라디오에 여러 SSID가 존재할 수 있으므로 AP 무선에 있는 각 SSID의 결과는 무선 용량을 기반으로 트래픽이 형성되는 AP 무선 가상 대기열에 삽입됩니다. AFD(Approximate Fair Drop)라는 QoS 메커니즘을 사용하여 이러한 단계에서 트래픽을 지연하거나 삭제할 수 있습니다. 그런 다음 이 정책의 결과는 AP 포트(무선 포트)로 전송되며, 여기에서 처음 두 개의 대기열(구성 가능한 대역폭까지)에 우선 순위가 지정되고, 이 단락의 앞부분에서 설명한 대로 세 번째와 네 번째 큐로 지정됩니다.

## Approximate Fair Drop and Wireless Queueing



이 컨피그레이션 예에서는 **priority level** 명령을 사용하여 첫 번째 우선순위 큐와 비디오를 두 번째 우선순위 대기열에 넣습니다. 나머지 트래픽은 나머지 포트 대역폭에 할당됩니다.

ACL(Access Control List)을 기반으로 트래픽을 대상으로 하는 클래스 맵을 사용할 수 없습니다. 포트 레벨에서 적용된 정책은 클래스 맵을 기반으로 트래픽을 대상으로 할 수 있지만, 이러한 클래스 맵은 QoS 값으로 식별된 트래픽을 대상으로 해야 합니다. ACL을 기반으로 트래픽을 식별하고 클라이언트 SSID 레벨에서 이 트래픽을 올바르게 표시하면 포트 레벨에서 동일한 트래픽에 대한 두 번째 심층 검사를 수행하기 위해 이중화됩니다. 트래픽이 AP로 이동하는 포트에 도달하면 이미 올바르게 표시됩니다.

이 예에서는 SSID 정책에 대해 생성된 일반 클래스 맵을 재사용하고 음성 RTP 트래픽 및 비디오 실시간 트래픽을 직접 대상으로 합니다.

```
Class-map allvoice
match dscp ef
Class-map videoandsignaling
Match dscp af41
match dscp cs3
```

관심 트래픽을 식별한 후에는 적용할 정책을 결정할 수 있습니다. AP가 탐지되면 기본 정책 (parent\_port라고 함)이 각 포트에 자동으로 적용됩니다. 다음과 같이 설정된 이 기본값을 변경할 수 없습니다.

```
policy-map parent_port
class class-default
shape average 1000000000
service-policy port_child_policy
```

기본 parent\_port 정책은 port\_child\_policy를 호출하므로 한 가지 옵션은 port\_child\_policy를 편집하는 것입니다. (이름을 변경하면 안 됩니다.) 이 하위 정책은 각 큐에서 어떤 트래픽이 이동해야 하는지, 얼마나 대역폭을 할당해야 하는지 결정합니다. 첫 번째 큐의 우선 순위가 가장 높고, 두 번째 큐의 우선 순위가 두 번째로 높습니다. 이 두 대기열은 실시간 트래픽용으로 예약되어 있습니다. 네 번째 큐는 비실시간 멀티캐스트 트래픽에 사용됩니다. 세 번째 큐는 다른 모든 트래픽을 포함합니다.

이 예에서는 음성 트래픽을 첫 번째 대기열에 할당하고 비디오 트래픽을 두 번째 대기열에 할당하고 각 대기열 및 다른 모든 트래픽에 대역폭을 할당하기로 결정합니다.

```
Policy-map port_child_policy
Class allvoice
  Priority level 1
  police rate percent 10
  conform-action transmit
  exceed-action drop
class videoandsignaling
  priority level 2
  police rate percent 20
  conform-action transmit
  exceed-action drop
class non-client-nrt-class
  bandwidth remaining ratio 7
class class-default
  bandwidth remaining ratio 63
```

이 정책에서 'voice' 및 'videoandsignaling' 클래스와 연결된 우선순위 문을 사용하면 해당 트래픽을 관련 우선순위 대기열에 할당할 수 있습니다. 그러나 경찰 속도 퍼센트 문은 유니캐스트가 아닌 멀티캐스트에만 적용됩니다.

이 정책은 AP가 탐지되는 즉시 자동으로 적용되므로 포트 레벨에서 적용할 필요가 없습니다.

### 3단계: SSID 레벨의 대역폭 및 우선순위 관리

다음 단계는 SSID 레벨에서 QoS 정책을 처리하는 것입니다. 이 단계는 Catalyst 3850 스위치와 5760 컨트롤러 모두에 적용됩니다. 이 컨피그레이션에서는 class-map 및 access-list를 사용하여 음성 및 비디오 트래픽이 식별되고 올바르게 태그가 지정되었다고 가정합니다. 그러나 액세스 목록의 대상이 아닌 일부 수신 트래픽은 해당 QoS 마킹을 표시하지 않을 수 있습니다. 이 경우 이 트래픽을 기본값으로 표시할지 아니면 태그가 지정되지 않은 상태로 두어야 할지를 결정할 수 있습니다. 동일한 논리는 이미 표시되었지만 클래스 맵의 대상이 아닌 트래픽에 적용됩니다. 표 맵의 기본 copy 문을 사용하여 표시되지 않은 트래픽이 표시되지 않고 태그 처리된 트래픽이 태그를 유지하고 태그가

나타나지 않도록 합니다.

표 맵은 나가는 DSCP 값을 결정하지만 프레임 UP 값을 결정하기 위해 802.11 프레임을 만드는 데에도 사용됩니다.

이 예에서는 음성 QoS 레벨(DSCP 46)을 표시하는 수신 트래픽이 DSCP 값을 유지 관리하고, 해당 값은 상응하는 802.11 마킹(UP 6)에 매핑됩니다. 비디오 QoS 레벨(DSCP 34)을 표시하는 수신 트래픽은 DSCP 값을 유지하고, 이 값은 해당하는 802.11 마킹(UP 5)에 매핑됩니다. 마찬가지로 DSCP 24로 표시된 트래픽은 음성 신호일 수 있습니다. DSCP 값을 유지 관리하고 802.11 UP 3으로 변환해야 합니다.

```
Table-map dscp2dscp
```

```
Default copy
```

```
Table-map dscp2up
```

```
Map from 46 to 6
```

```
Map from 24 to 3
```

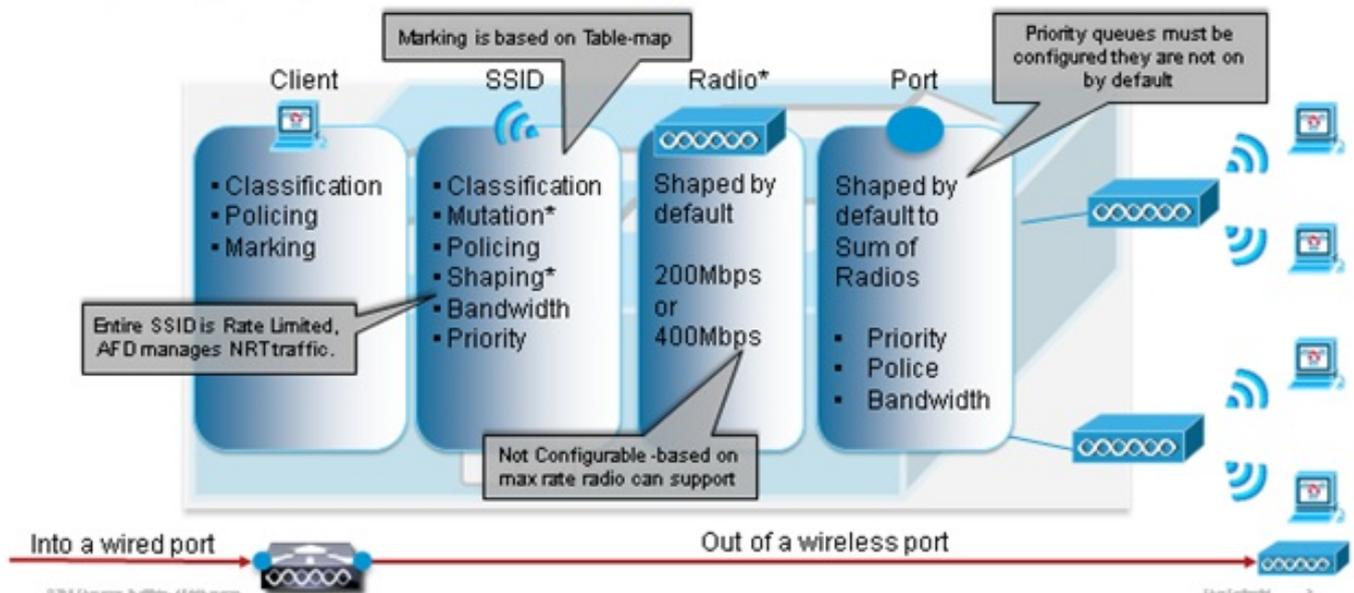
```
Map from 34 to 5
```

```
Default copy
```

수신 유선 포트 레벨에서도 마킹을 수행할 수 있습니다. 이 그림에는 유선에서 무선으로 트래픽을 전송할 때 수행할 수 있는 QoS 작업이 나와 있습니다.

## QoS Touch points

Port, Radio, SSID, Client - What features apply at each level - Downstream



이 컨피그레이션 예에서는 QoS 컨피그레이션의 무선 측면에 중점을 두고 무선 클라이언트 레벨에서 트래픽을 표시합니다. 마킹 부분이 완료되면 대역폭을 할당해야 합니다. 여기에서 6Mbps의 대역폭이 음성 트래픽 흐름에 할당됩니다. (음성에 대한 전체 대역폭 할당이지만, 각 통화에는 128kbps와 같이 더 적게 소비됩니다.) 이 대역폭은 **police** 명령에 할당되어 대역폭을 예약하고 초과 트래픽을 삭제합니다.

비디오 트래픽도 6Mbps에 할당되고 폴링됩니다. 이 컨피그레이션 예에서는 비디오 흐름이 하나만 있다고 가정합니다.

비디오 및 음성 트래픽의 신호 부분도 대역폭을 할당해야 합니다. 두 가지 방법이 있다.

- 초과 트래픽을 버퍼링하고 나중에 전송할 수 있도록 **shape average** 명령을 사용합니다. 이러한 흐름에는 일관된 지연 및 지터가 필요하므로 음성 또는 비디오 흐름 자체에서 이 로직은 효율적이지 않습니다. 그러나 신호 처리가 통화 품질에 영향을 주지 않고 약간 지연될 수 있으므로 신호 처리가 효율적일 수 있습니다. 컨버지드 액세스 솔루션에서 shape 명령은 할당된 대역폭을 초과하는 트래픽의 버퍼링을 결정하는 "버킷 컨피그레이션"이라는 것을 허용하지 않습니다. 따라서 버킷 크기가 0임을 지정하려면 두 번째 명령인 **queue-buffers ratio 0**을 추가해야 합니다. 나머지 트래픽에 시그널링을 포함하고 shape 명령을 사용하는 경우 혼잡이 발생할 때 신호 처리 트래픽이 삭제될 수 있습니다. 두 쪽 끝에 통신이 더 이상 발생하지 않는 것으로 확인되므로 결과적으로 통화가 삭제될 수 있습니다.
- 통화 끊김 위험을 방지하려면 우선 순위 대기열 중 하나에 신호 처리를 포함할 수 있습니다. 이 컨피그레이션 예에서는 우선 순위 큐를 음성 및 비디오로 정의했고 이제 비디오 큐에 시그널링을 추가합니다.

정책은 음성 흐름에 CAC(Call Admission Control)를 사용합니다. CAC는 무선 트래픽을 대상으로 하며 특정 UP를 매칭합니다(이 컨피그레이션 예에서는 UP 6 및 7). 그런 다음 CAC는 이 트래픽이 사용해야 하는 최대 대역폭 양을 결정합니다. 음성 트래픽을 감시하는 컨피그레이션에서 CAC는 음성 흐름에 할당된 전체 대역폭의 하위 집합을 할당해야 합니다. 예를 들어, 음성이 6Mbps로 폴리싱된 경우 CAC는 6Mbps를 초과할 수 없습니다. CAC는 기본 다운스트림 정책 맵(상위 정책이라고 함)에 통합된 정책 맵(하위 정책이라고 함)에서 구성됩니다. CAC는 **accept cac wmm-tspec** 명령과 함께 대상 트래픽에 할당된 대상 UP와 대역폭이 함께 도입되었습니다.

각 통화는 음성 흐름에 할당된 모든 대역폭을 소비하지 않습니다. 예를 들어, 각 통화는 각 방식으로 64kbps를 소비할 수 있으며, 이로 인해 128kbps의 효과적인 양방향 대역폭 소비가 발생합니다. 속도 명령은 각 통화 대역폭 소비를 결정하며, police 문은 음성 트래픽에 할당된 전체 대역폭을 결정합니다. 셀 내에서 발생하는 모든 통화가 최대 허용 대역폭에 근접하여 사용되면 셀 내에서 시작되어 소비된 대역폭이 음성 흐름에 허용된 최대 대역폭을 초과하게 되는 모든 새 통화가 거부됩니다. [4단계](#)에서 설명한 대로 대역 레벨에서 CAC 컨피그레이션을 통해 이 프로세스를 세부적으로 조정할 수 있습니다. [CAC의 통화 제한](#).

따라서 기본 다운스트림 정책에 통합된 CAC 지침이 포함된 하위 정책을 구성해야 합니다. CAC가 업스트림 정책 맵에 구성되지 않았습니다. CAC는 셀에서 시작된 음성 통화에 적용되지만, 이러한 통화에 대한 응답이므로 CAC는 다운스트림 정책 맵으로만 설정됩니다. 업스트림 정책 맵은 다릅니다. 이전에 생성한 클래스 맵은 ACL을 기반으로 트래픽을 대상으로 하므로 사용할 수 없습니다. SSID 정책에 삽입된 트래픽은 이미 클라이언트 정책을 통과했으므로 패킷에 대한 심층 검사를 두 번 수행하지 않아야 합니다. 대신 클라이언트 정책의 결과를 QoS 마킹으로 대상 트래픽을 지정합니다.

기본 클래스에 시그널링을 남겨두지 않으려면 시그널링의 우선 순위를 지정해야 합니다.

이 예에서 신호 및 비디오는 동일한 클래스에 있으며 신호 부분을 수용하기 위해 해당 클래스에 더 많은 대역폭이 할당됩니다. 6Mbps는 비디오 트래픽에 할당되며(Tandberg 카메라 포인트 투 포인트 흐름 1개), 모든 음성 통화 및 비디오 흐름에 대한 신호 전송에 1Mbps가 할당됩니다.

```
Class-map allvoice
match dscp ef
Class-map videoandsignaling
Match dscp af41
Match dscp cs3
```

다운스트림 하위 정책은 다음과 같습니다.

```
Policy-map SSIDout_child_policy
```

```

class allvoice
priority level 1
police 6000000
admit cac wmm-tspec
rate 128
wlan-up 6 7
class videoandsignaling
priority level 2
police 1000000

```

다운스트림 상위 정책은 다음과 같습니다.

```

policy-map SSIDout
class class-default
set dscp dscp table dscp2dscp
set wlan user-priority dscp table dscp2up
shape average 30000000
queue-buffers ratio 0
service-policy SSIDout_child_policy

```

업스트림 트래픽은 무선 클라이언트에서 오는 트래픽이며, 트래픽이 유선 포트에서 전송되거나 다른 SSID로 전송되기 전에 WCM으로 전송됩니다. 두 경우 모두 각 트래픽 유형에 할당된 대역폭을 정의하는 정책 맵을 구성할 수 있습니다. 트래픽이 유선 포트에서 전송되는지 또는 다른 SSID로 전송되는지에 따라 정책이 다를 수 있습니다.

업스트림 방향에서 가장 중요한 문제는 대역폭이 아니라 우선순위를 결정하는 것입니다. 다시 말해, 업스트림 정책 맵은 각 트래픽 유형에 대역폭을 할당하지 않습니다. 트래픽이 이미 AP에 있고 반이 중 무선 공간에 의해 형성된 Bottle-Neck를 이미 통과했기 때문에 Catalyst 3850 스위치 또는 Cisco 5760 WLC의 컨트롤러 기능에 이 트래픽을 전달하여 추가 처리를 하는 것이 목표입니다. AP 레벨에서 트래픽을 수집할 때, 컨트롤러에 전송되는 트래픽 플로우의 우선 순위를 지정하기 위해 잠재적인 기존 QoS 마킹을 신뢰해야 할지 여부를 결정할 수 있습니다. 이 예에서는 기존 DSCP 값을 신뢰할 수 있습니다.

```

Policy-map SSIDin
Class class-default
set dscp dscp table dscp2dscp

```

정책이 생성되면 WLAN에 정책 맵을 적용합니다. 이 예에서는 WLAN에 연결하는 모든 장치가 WMM을 지원해야 하므로 WMM이 필요합니다.

```

wlan test1
wmm require
service-policy client input taggingPolicy
service-policy input SSIDin
service-policy output SSIDout

```

## 4단계: CAC로 통화 제한

마지막 단계는 CAC를 특정 상황에 맞게 조정하는 것입니다. [3단계](#)에 설명된 CAC 컨피그레이션에서 [SSID 레벨의 대역폭 및 우선순위 관리](#)에서 AP는 할당된 대역폭을 초과하는 모든 음성 패킷을 삭제합니다.

대역폭 최대값을 방지하려면 발신된 통화와 대역폭을 초과할 통화를 인식하도록 WCM을 구성해야 합니다. 일부 전화기는 WMM TSPEC(Traffic Specification)을 지원하며, 예상 통화가 소비될 대역폭을 무선 인프라에 알립니다. 그런 다음 WCM은 통화를 걸기 전에 통화를 거부할 수 있습니다.

일부 SIP 전화기는 TSPEC을 지원하지 않지만 WCM과 AP를 설정하여 SIP 포트에 전송된 통화 시작 패킷을 인식할 수 있으며 SIP 통화가 연결되려고 함을 설정하기 위해 이 정보를 사용할 수 있습니다. SIP 전화기는 통화에 사용할 대역폭을 지정하지 않으므로 관리자는 코덱과 샘플링 시간 등을 기준으로 예상 대역폭을 결정해야 합니다.

CAC는 각 AP 레벨에서 사용된 대역폭을 계산합니다. CAC는 계산(정적 CAC)에서 클라이언트 대역폭 소비만 사용하도록 설정하거나, 동일한 채널(로드 기반 CAC)에서 인접 AP와 디바이스를 고려하도록 설정할 수 있습니다. SIP 전화에는 고정 CAC를, TSPEC 전화기에는 로드 기반 CAC를 사용하는 것이 좋습니다.

마지막으로 CAC는 대역 단위로 활성화됩니다.

이 예에서는 전화기가 세션 시작을 위해 TSPEC 대신 SIP를 사용하고, 각 통화는 각 스트림 방향에 64kbps를 사용하며, 정적 CAC가 활성화된 경우 로드 기반 CAC가 비활성화되고, 각 AP 대역폭 최대값의 75%가 음성 트래픽에 할당됩니다.

```
ap dot11 5ghz shutdown
ap dot11 5ghz cac voice acm
no ap dot11 5ghz cac voice load-based
ap dot11 5ghz cac voice max-bandwidth 75
ap dot11 5ghz cac voice sip bandwidth 64
no ap dot11 5ghz shutdown
```

2.4GHz 대역에서 동일한 컨피그레이션을 반복할 수 있습니다.

```
ap dot11 24ghz shutdown
ap dot11 24ghz cac voice acm
no ap dot11 24ghz cac voice load-based
ap dot11 24ghz cac voice max-bandwidth 75
ap dot11 24ghz cac voice sip bandwidth 64
no ap dot11 24ghz shutdown
```

각 밴드에 대해 CAC가 적용되면 WLAN 레벨에서 SIP CAC를 적용해야 합니다. 이 프로세스를 통해 AP는 SIP 통화 시도를 나타내는 UDP 5060으로 전송된 쿼리를 식별하기 위해 무선 클라이언트 트래픽의 레이어 4(L4) 정보를 검토할 수 있습니다. TSPEC는 802.11 레벨에서 작동하며 AP에서 기본적으로 탐지됩니다. SIP 전화기는 TSPEC를 사용하지 않으므로 SIP 트래픽을 식별하기 위해 AP에서 심층 패킷 검사를 수행해야 합니다. AP가 모든 SSID에서 이 검사를 수행하지 않도록 하기 때문에 어떤 SSID가 SIP 트래픽을 예상하는지 확인해야 합니다. 그런 다음 해당 SSID에서 통화 스누핑을 활성화하여 음성 통화를 검색할 수 있습니다. SIP 호출을 거부해야 하는 경우 수행할 작업을 결정할 수도 있습니다. SIP 클라이언트의 연결을 해제하거나 SIP 통화 중 메시지를 보낼 수도 있습니다.

이 예에서는 통화 스누핑이 활성화되고 SIP 통화를 거부해야 하는 경우 통화 중 메시지가 전송됩니다. [3단계](#)에서 QoS 정책을 추가하면 [SSID 레벨의 대역폭 및 우선순위 관리](#)는 WLAN 예제의 SSID 컨피그레이션입니다.

```
wlan test1
wmm require
service-policy client input taggingPolicy
service-policy input SSIDin
service-policy output SSIDout
call-snoop
sip-cac send-486busy
```

**다음을 확인합니다.**

QoS 컨피그레이션이 제대로 작동하는지 확인하려면 다음 명령을 사용합니다.

## 참고:

이 [섹션](#)에 사용된 명령에 대한 자세한 내용을 보려면 [Command Lookup Tool](#)([등록된 고객만 해당](#))을 사용합니다.

Output [Interpreter 도구](#)([등록된 고객만 해당](#))는 특정 **show** 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 [출력 인터프리터 도구]를 사용합니다.

## show class-map

이 명령은 플랫폼에 구성된 클래스 맵을 표시합니다.

```
3850#show class-map
Class Map match-any H323realtimeaudio (id 6)
  Match access-group name H323Audiostream
Class Map match-any H323realtimevideo (id 7)
  Match access-group name H323Videostream
Class Map match-any allvideo (id 10)
  Match dscp af41 (34)
Class Map match-any jabberaudiosignaling (id 11)
  Match access-group name JabberSIGNALING
Class Map match-any allvoice (id 12)
  Match dscp ef (46)
Class Map match-any RTPaudio (id 19)
  Match access-group name JabberVOIP
  Match access-group name H323Audiostream
Class Map match-any class-default (id 0)
  Match any
Class Map match-any jabberRTPaudio (id 14)
  Match access-group name JabberVOIP
Class Map match-any non-client-nrt-class (id 1)
  Match non-client-nrt
Class Map match-any H323audiosignaling (id 17)
  Match access-group name H323AudioSignaling
Class Map match-any H323videosignaling (id 18)
  Match access-group name H323VideoSignaling
Class Map match-any signaling (id 20)
  Match access-group name JabberSIGNALING
  Match access-group name H323VideoSignaling
  Match access-group name H323AudioSignaling
```

## 정책 맵 표시

이 명령은 플랫폼에 구성된 정책 맵을 표시합니다.

```
3850 #show policy-map
show policy-map
Policy Map port_child_policy
  Class non-client-nrt-class
    bandwidth remaining ratio 7
  Class allvoice
    priority level 1
```

```

    police rate percent 10
      conform-action transmit
      exceed-action drop
Class allvideo
  priority level 2
  police rate percent 20
    conform-action transmit
    exceed-action drop
Class class-default
  bandwidth remaining ratio 63
Policy Map SSIDin
  Class class-default
    set dscp dscp table dscp2dscp
Policy Map SSIDout_child_policy
  Class allvoice
    priority level 1
    police cir 6000000 bc 187500
      conform-action transmit
      exceed-action drop
    admit cac wmm-tspec
      rate 6000 (kbps)
      wlan-up 6
  Class allvideo
    priority level 2
    police cir 6000000 bc 187500
      conform-action transmit
      exceed-action drop
    admit cac wmm-tspec
      rate 6000 (kbps)
      wlan-up 4 5
Policy Map taggingPolicy
  Class RTPaudio
    set dscp ef
  Class H323realtimevideo
    set dscp af41
  Class signaling
    set dscp cs3
Policy Map SSIDout
  Class class-default
    set dscp dscp table dscp2dscp
    set wlan user-priority dscp table dscp2up
    shape average 30000000 (bits/sec)
    queue-buffers ratio 0
    service-policy SSIDout_child_policy
Policy Map parent_port
  Class class-default
    shape average 1000000000 (bits/sec) op

```

## wlan 표시

이 명령은 WLAN 컨피그레이션 및 서비스 정책 매개변수를 표시합니다.

```

3850# show wlan name test1 | include Policy
AAA Policy Override                : Disabled
QoS Service Policy - Input
  Policy Name                       : SSIDin
  Policy State                       : Validated
QoS Service Policy - Output
  Policy Name                       : SSIDout
  Policy State                       : Validated
QoS Client Service Policy

```

```
Input Policy Name      : taggingPolicy
Output Policy Name     : taggingPolicy
Radio Policy           : All
```

## show policy-map 인터페이스

이 명령은 특정 인터페이스에 대해 설치된 정책 맵을 표시합니다.

```
3850#show policy-map interface wireless ssid name test1
```

```
Remote SSID test1 iifid: 0x01023F4000000033.0x00F2E98000000003.0x00C2EB000000001F
```

```
Service-policy input: SSIDin
  Class-map: class-default (match-any)
    Match: any
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp dscp table dscp2dscp
```

```
Remote SSID test1 iifid: 0x01023F4000000033.0x00C8384000000004.0x00D0D08000000021
```

```
Service-policy input: SSIDin
  Class-map: class-default (match-any)
    Match: any
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp dscp table dscp2dscp
```

```
SSID test1 iifid: 0x01023F4000000033.0x00F2E98000000003.0x00EC3E800000001E
```

```
Service-policy input: SSIDin
  Class-map: class-default (match-any)
    Match: any
      0 packets, 0 bytes
      30 second rate 0 bps
    QoS Set
      dscp dscp table dscp2dscp
```

```
Service-policy output: SSIDout
```

```
Class-map: class-default (match-any)
  Match: any
    0 packets, 0 bytes
    30 second rate 0 bps
  QoS Set
    dscp dscp table dscp2dscp
    wlan user-priority dscp table dscp2up
  shape (average) cir 30000000, bc 120000, be 120000
  target shape rate 30000000
  queue-buffers ratio 0
```

```
Service-policy : SSIDout_child_policy
```

```
Class-map: allvoice (match-any)
  Match: dscp ef (46)
    0 packets, 0 bytes
    30 second rate 0 bps
  Priority: Strict,
```

```
Priority Level: 1
police:
  cir 6000000 bps, bc 187500 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    drop
  conformed 0000 bps, exceed 0000 bps
  cac wmm-tspec rate 6000 kbps
```

```
Class-map: allvideo (match-any)
Match: dscp af41 (34)
  0 packets, 0 bytes
  30 second rate 0 bps
Priority: Strict,
```

```
Priority Level: 2
police:
  cir 6000000 bps, bc 187500 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    drop
  conformed 0000 bps, exceed 0000 bps
  cac wmm-tspec rate 6000 kbps
```

```
Class-map: class-default (match-any)
Match: any
  0 packets, 0 bytes
  30 second rate 0 bps
```

SSID test1 iifid: 0x01023F40000000033.0x00C83840000000004.0x00DB5680000000020

Service-policy input: SSIDin

```
Class-map: class-default (match-any)
Match: any
  0 packets, 0 bytes
  30 second rate 0 bps
QoS Set
  dscp dscp table dscp2dscp
```

Service-policy output: SSIDout

```
Class-map: class-default (match-any)
Match: any
  0 packets, 0 bytes
  30 second rate 0 bps
QoS Set
  dscp dscp table dscp2dscp
  wlan user-priority dscp table dscp2up
shape (average) cir 30000000, bc 120000, be 120000
target shape rate 30000000
queue-buffers ratio 0
```

Service-policy : SSIDout\_child\_policy

```
Class-map: allvoice (match-any)
Match: dscp ef (46)
  0 packets, 0 bytes
  30 second rate 0 bps
Priority: Strict,
```

```
Priority Level: 1
police:
  cir 6000000 bps, bc 187500 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    drop
  conformed 0000 bps, exceed 0000 bps
  cac wmm-tspec rate 6000 kbps
```

```
Class-map: allvideo (match-any)
Match: dscp af41 (34)
  0 packets, 0 bytes
  30 second rate 0 bps
Priority: Strict,
```

```
Priority Level: 2
police:
  cir 6000000 bps, bc 187500 bytes
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    drop
  conformed 0000 bps, exceed 0000 bps
  cac wmm-tspec rate 6000 kbps
```

```
Class-map: class-default (match-any)
Match: any
  0 packets, 0 bytes
  30 second rate 0 bps
```

3850#**show policy-map interface wireless client**

Client 8853.2EDC.68EC iifid:

0x01023F4000000033.0x00F2E98000000003.0x00EC3E800000001E.0x00E0D04000000022

Service-policy input: taggingPolicy

```
Class-map: RTPaudio (match-any)
Match: access-group name JabberVOIP
  0 packets, 0 bytes
  30 second rate 0 bps
Match: access-group name H323Audiostream
  0 packets, 0 bytes
  30 second rate 0 bps
QoS Set
  dscp ef
```

```
Class-map: H323realtimevideo (match-any)
Match: access-group name H323Videostream
  0 packets, 0 bytes
  30 second rate 0 bps
QoS Set
  dscp af41
```

```
Class-map: signaling (match-any)
Match: access-group name JabberSIGNALING
  0 packets, 0 bytes
  30 second rate 0 bps
Match: access-group name H323VideoSignaling
  0 packets, 0 bytes
  30 second rate 0 bps
Match: access-group name H323AudioSignaling
  0 packets, 0 bytes
  30 second rate 0 bps
```

```

QoS Set
  dscp cs3
Class-map: class-default (match-any)
  Match: any
    0 packets, 0 bytes
    30 second rate 0 bps

Service-policy output: taggingPolicy

Class-map: RTPaudio (match-any)
  Match: access-group name JabberVOIP
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: access-group name H323Audiostream
    0 packets, 0 bytes
    30 second rate 0 bps
  QoS Set
    dscp ef

Class-map: H323realtimevideo (match-any)
  Match: access-group name H323Videostream
    0 packets, 0 bytes
    30 second rate 0 bps
  QoS Set
    dscp af41

Class-map: signaling (match-any)
  Match: access-group name JabberSIGNALING
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: access-group name H323VideoSignaling
    0 packets, 0 bytes
    30 second rate 0 bps
  Match: access-group name H323AudioSignaling
    0 packets, 0 bytes
    30 second rate 0 bps
  QoS Set
    dscp cs3
Class-map: class-default (match-any)
  Match: any
    0 packets, 0 bytes
    30 second rate 0 bps

```

## 플랫폼 qos 정책 표시

이 명령은 포트, AP 무선, SSID 및 클라이언트에 대해 설치된 QoS 정책을 표시합니다. 라디오 정책을 확인할 수 있지만 변경할 수는 없습니다.

```

3850#show platform qos policies PORT
Loc Interface          IIF-ID                Dir Policy             State
-----
L:0 Gi1/0/20          0x01023f4000000033  OUT defportangn       INSTALLED IN HW
L:0 Gi1/0/20          0x01023f4000000033  OUT port_child_policy INSTALLED IN HW

3850#show platform qos policies RADIO
Loc Interface          IIF-ID                Dir Policy             State
-----
L:0 R56356842871193604 0x00c8384000000004  OUT def-11an          INSTALLED IN HW
L:0 R68373680329064451 0x00f2e98000000003  OUT def-11gn          INSTALLED IN HW
3850#show platform qos policies SSID
Loc Interface          IIF-ID                Dir Policy             State
-----

```

```

-----
L:0 S70706569125298203 0x00fb33400000001b OUT SSIDout_child_policyINSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 OUT SSIDout_child_policyINSTALLED IN HW
L:0 S70706569125298203 0x00fb33400000001b OUT SSIDout INSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 OUT SSIDout INSTALLED IN HW
L:0 S70706569125298203 0x00fb33400000001b IN SSIDin INSTALLED IN HW
L:0 S69318160817324057 0x00f6448000000019 IN SSIDin INSTALLED IN HW

```

3850#**show platform qos policies CLIENT**

Loc	Interface	IIF-ID	Dir	Policy	State
L:0	8853.2edc.68ec	0x00e0d04000000022	IN	taggingPolicy	NOT INSTALLED IN HW
L:0	8853.2edc.68ec	0x00e0d04000000022	OUT	taggingPolicy	NOT INSTALLED IN HW

## show wireless client mac-address <mac> service policy

이 명령은 클라이언트 레벨에서 적용된 정책 맵을 표시합니다.

3850#**show wireless client mac-address 8853.2EDC.68EC service-policy output**

Wireless Client QoS Service Policy

Policy Name : taggingPolicy

Policy State : Installed

3850#**sh wireless client mac-address 8853.2EDC.68EC service-policy in**

3850#**sh wireless client mac-address 8853.2EDC.68EC service-policy input**

Wireless Client QoS Service Policy

Policy Name : taggingPolicy

Policy State : Installed

## 문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.