

# & ; についてワイヤレス9800 WLCでのQoSのトラブルシューティング ( クイックリファレンス )

## 内容

---

### [はじめに](#)

### [前提条件](#)

#### [要件](#)

#### [使用するコンポーネント](#)

### [背景説明](#)

#### [IEEE 802.11e規格とWi-Fi Multimedia\(WMM\)の簡単な説明](#)

#### [WMMキューおよび拡張分散チャネルアクセス\(EDCA\)](#)

### [QoS 実装](#)

#### [レイヤ2「802.1p」CoS \( サービスクラス \)](#)

#### [レイヤ3 DSCP\(Differentiated Services Code Point\)](#)

#### [デフォルトのDSCP-to-UPマッピング](#)

### [パケットフローとQoSの信頼性](#)

#### [中央スイッチング-ダウンストリームの信頼](#)

#### [中央スイッチング: アップストリームの信頼](#)

#### [Flexconnectローカルスイッチングの信頼](#)

### [アップストリームトラフィックに関する一般的な問題](#)

#### [例#1: クライアントがUP値が「2」のトラフィックを送信するとき](#)

#### [例#2:DSCPからUPへのマッピングにおける既知のMicrosoft Windowsクライアントの問題](#)

### [DSCPとCOSのどちらのプロトコルを信頼するか？](#)

### [ワイヤレスLANコントローラQoSのベストプラクティス](#)

#### [メタルQoSプロファイル](#)

#### [片通話について](#)

#### [音声のとぎれや不自然な音声について](#)

#### [ローミング時の音声のギャップと欠落について](#)

#### [参考資料](#)

---

## はじめに

このドキュメントでは、9800ワイヤレスLANコントローラ(WLC)のQoSについて説明します。

## 前提条件

### 要件

このドキュメントでは、アップストリームとダウンストリームの両方でトラフィックに優先順位を付けてタグを付ける方法について説明します。また、ワイヤレスLANコントローラ(WLC)での音声トラフィックのベストプラクティス設定と、一般的な音声関連の問題のトラブルシューティングテクニックについて説明します。

## 使用するコンポーネント

### 17.12 Cisco IOS® XEリリースに基づく9800 WLC

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

### IEEE 802.11e規格とWi-Fi Multimedia(WMM)の簡単な説明

WMMは、IEEE 802.11e標準に基づくWi-Fi Allianceです。WMMは、拡張分散チャネルアクセス(EDCA)方式に基づいて、音声、ビデオ、ベストエフォート、およびバックグラウンドの4つのアクセスカテゴリに従ってトラフィックを優先順位付けすることで、Quality of Service(QoS)機能を提供します。

WMMを有効にすることは、Wi-Fiネットワーク、特に高帯域幅で低遅延のアプリケーションが広く普及している環境で最適なパフォーマンスを実現するために不可欠です。たとえば、802.11nネットワークでは、WMMはこの高速Wi-Fi標準の機能を完全に活用する必要があります。

### WMMキューおよび拡張分散チャネルアクセス(EDCA)

一般に、どのステーションもメディアをリッスンして、フレームを送信する前にメディアがアイドル状態かどうかを確認する必要があります。フレームが送信されると、ステーションはメディアをリッスンして、コリジョンが発生したかどうかを確認します。

ワイヤレスクライアントがコリジョンを検出できない。このために、CSMA/CA(Carrier Sense Multiple Access with Collision Avoidance)が使用されます。固定およびランダムタイマー(CWmin、CWmax)を使用し、衝突がなく、すべてのクライアントがトラフィックを送信できることを確認するために、送信されるすべてのフレームに確認応答が必要です。

前述したように、4つのアクセスカテゴリ(キュー)があり、各キューは異なるタイマーを使用します。プライオリティの高いフレームは統計的に早く送信され、プライオリティの低いフレームには統計的に後で送信されるようにバックオフパラメータが設定されます。

要約すると、4つのキューが存在するだけでは、Quality of Service(QoS)は保証されません。本当に重要なのは、各キュー内のトラフィックがどのように効果的に管理されているかということです。

# QoS 実装

デフォルトでは、Quality of Service(QoS)が設定されていない場合、ネットワークトラフィックはベストエフォート型配信モデルで同等に扱われます。つまり、すべてのトラフィックは、そのタイプや重要性に関係なく、任意の時点で同じ優先順位と配信される可能性を持ちます。ただし、QoS機能を有効にして適切に設定すると、音声やビデオなどの特定の種類のネットワークトラフィックに優先順位を割り当てることができます。

QoSの設定には、分類とマーキングという2つの主要コンポーネントが含まれます。

分類：

分類には、アプリケーションのタイプ、送信元/宛先IPアドレス、プロトコル、ポート番号などの特定の基準に基づいて、ネットワークトラフィックを識別して分類することが含まれます。トラフィックは次のクラスまたはキューに分割されます。

1. 音声：AC\_VO
2. ビデオ：AC\_VI
3. ベストエフォート：AC\_BE
4. バックグラウンド：AC\_BK

マーキング：

トラフィックがキューマーキングに分類されると、パケットにQoSマーキングまたはタグが割り当てられ、プライオリティレベルが示されます。

トラフィックをマーキングする方法はいくつかあります。主な2つの標準は、レイヤ2 802.1p CoS ( サービスクラス ) とレイヤ3 DSCP(Differentiated Services Code Point)です。

## レイヤ2「802.1p」 CoS ( サービスクラス )

802.1p標準では、7つのレベルのCoSがあり、それぞれが0 ~ 7の範囲の値を取ることができる3ビットフィールドで表されます。これらの値はトラフィックのプライオリティを示し、0が最低のプライオリティ、7が最高のプライオリティです。

注：802.1pは802.1q標準のサブセットであり、トランクポートなどにあるVLANタグがある場合にのみ表示されます。

表1:802.1PとWMMの分類

802.1P Priority	Access Category_WMM Designation	Access Category "AC"	QoS
1	AC_BK	Background	Bronze
2	AC_BK	Background	Bronze
0	AC_BE	Best Effort	Silver
3	AC_BE	Best Effort	Silver
4	AC_VI	Video	Gold
5	AC_VI	Video	Gold
6	AC_VO	Voice	Platinum
7	AC_VO	Voice	Platinum

### レイヤ3 DSCP(Differentiated Services Code Point)

DSCPはIPヘッダー上のレイヤ3タグで、6ビットを使用して64種類の値(0 ~ 63)を許可します。

表2:DSCPとWMMの分類

DSCP	Access Category_WMM Designation	Access Category "AC"	QoS
0-7	AC_BE	Best Effort	Silver
24-31	AC_BE	Best Effort	Silver
8-15	AC_BK	Background	Bronze
16-23	AC_BK	Background	Bronze
32-39	AC_VI	Video	Gold
40-47	AC_VI	Video	Gold
48-55	AC_VO	Voice	Platinum
56-63	AC_VO	Voice	Platinum

主なDSCP値は、音声で46(EF)、ビデオで34(AF41)、ベストエフォート用に0(BE)です。

### デフォルトのDSCP-to-UPマッピング

前に説明したように、イーサネットフレーム内のUPフィールドは3ビットですが、IPヘッダー内のDSCPは6ビットです。

レイヤ3 Differentiated Services Code Point(DSCP)値からレイヤ2ユーザプライオリティ(UP)値を計算するには、どうすればよいのですか。

現在、このマッピングに関する特定の標準はありませんが、一般的な方法が使用され、「デフォルトのDSCP-to-UPマッピング」として知られています。

DSCP-to-UPマッピング方式では、DSCPパケットの3msbからUP値を取得し、それを正しいアクセスカテゴリにマッピングします。

この方式は、Microsoft Windowsマシンが既知の問題に従うために使用されます。この問題については、「[例#2:DSCPからUPへのマッピングの既知のMicrosoft Windowsクライアントの問題](#)」で詳しく説明しています

表3：デフォルトのDSCPからUPへのマッピング

DSCP	DSCP (binary)	802.11e UP (binary)	802.11e UP (decimal)	Access Category Assignment
56-63	111000 - 111111	111	7	Voice
48-55	110000 - 110111	110	6	
40-47	101000 - 101111	101	5	Video
32-39	100000 - 100111	100	4	
24-31	011000 - 011111	011	3	Best Effort
0-7	000000 - 000101	000	0	
16-23	010000 - 010111	010	2	Background
8-15	001111 - 001111	001	1	

## パケットフローとQoSの信頼性

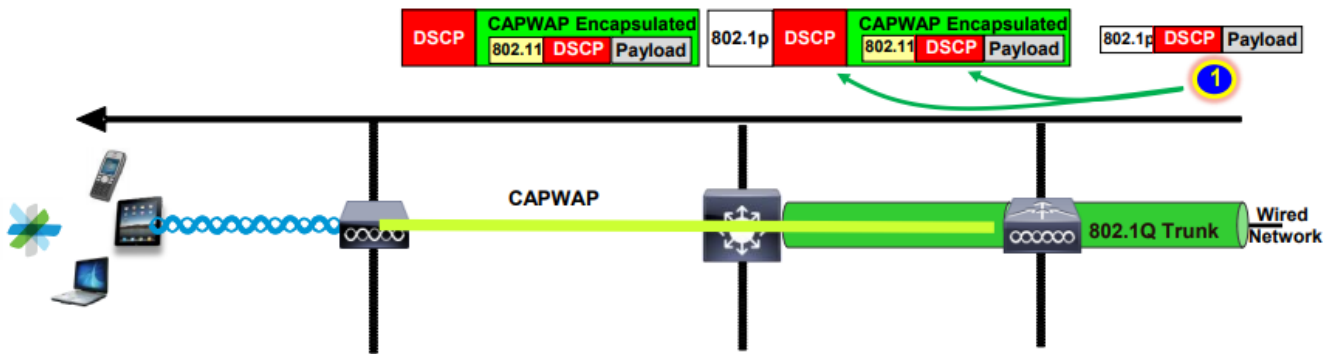
このセクションでは、次のさまざまなシナリオにおけるパケットフローとQoSの信頼性について説明します。

1. 中央スイッチング：ダウンストリームの信頼。
2. 中央スイッチング：アップストリームの信頼。
3. FlexConnectローカルスイッチングの信頼。

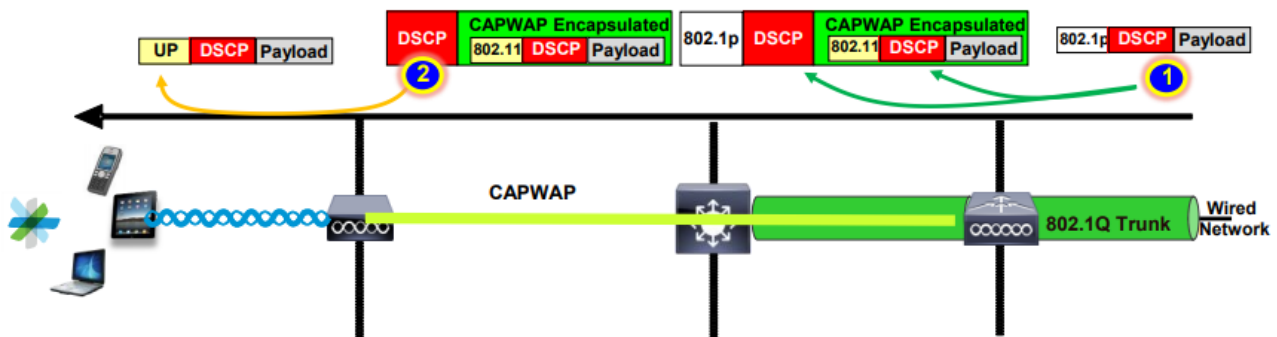
### 中央スイッチング – ダウンストリームの信頼

- ダウンストリーム：有線からワイヤレスへのトラフィック。
- ダウンストリームトラフィックはCAPWAPカプセル化されます。

1 - WLC 802.1qトランクポートでイーサネットフレームが受信されます。WLCは、有線ネットワークから送信された内部DSCP値を使用し、それをCAPWAPヘッダーの外部DSCPにマッピングし、WLCで設定されたQoSプロファイルに従って、外部DSCPを最大値にキャップします。



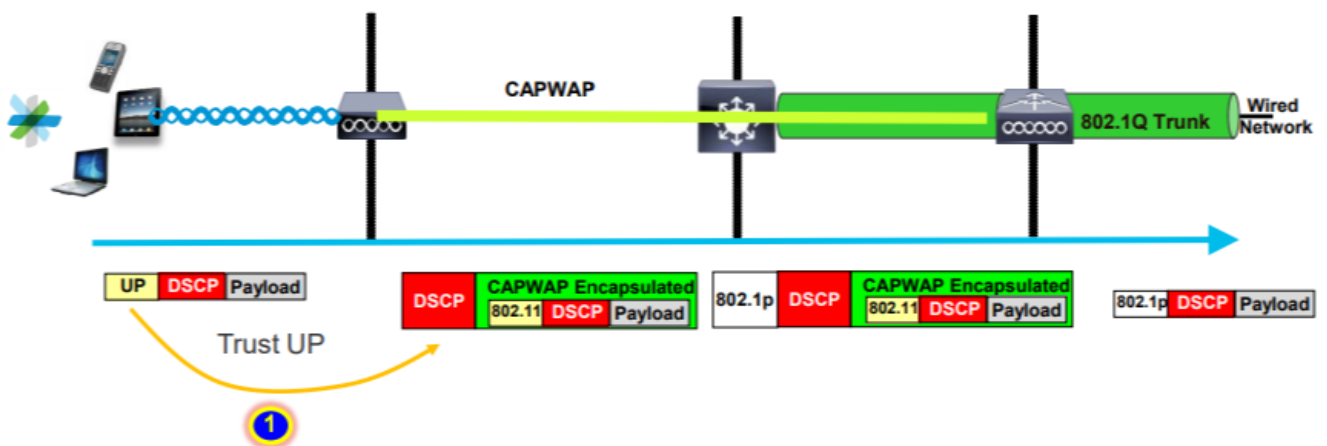
2- APがこのイーサネットフレームを受信すると、APは外部DSCP値をUP値にマッピングし、適切なACを使用してワイヤレスクライアントに送信します。



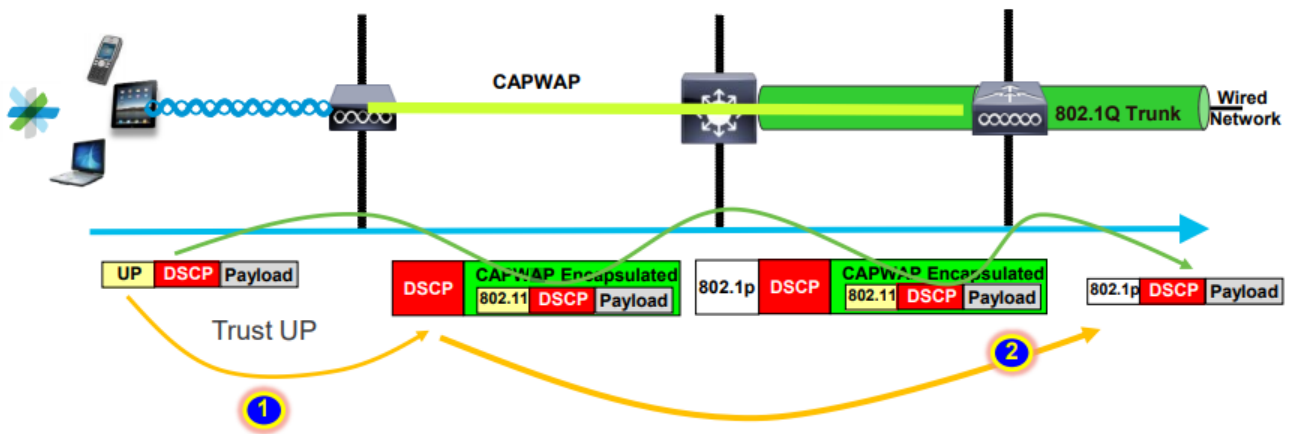
### 中央スイッチング：アップストリームの信頼

- アップストリーム：無線から有線へのトラフィック。

1. ワイヤレスクライアントが802.11e(WMM)フレームを送信し、APがこれを受信する。



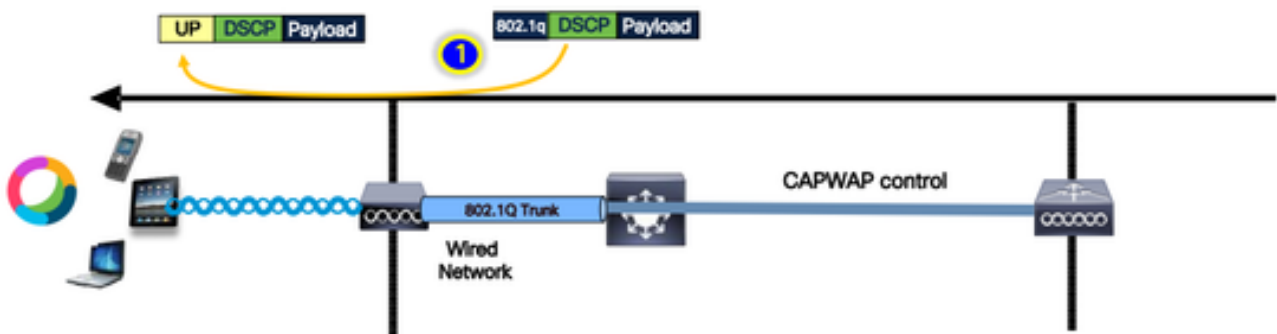
2- APは元の packets をCAPWAPヘッダーにカプセル化し、WLC上で設定されているQoSプロファイルでそのQoSレベルが許可されている限り、UPを外部DSCP値にマッピングします。パケットは、元のDSCP値で有線ネットワークに送信されます。



## Flexconnectローカルスイッチングの信頼

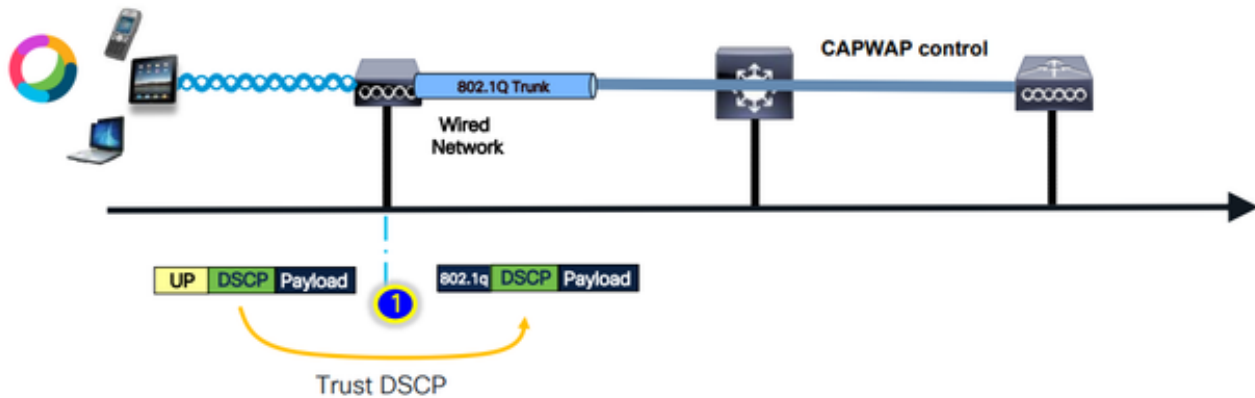
- Flexconnectローカルスイッチング：ダウンストリームの信頼

ローカルでスイッチされるVLANの場合、FlexConnect APはIPパケットのDSCP値を取得し、任意のQoSポリシー（AVCポリシーなど）を処理し、それをワイヤレスフレームの802.11e UP値にマッピングして、フレームをキューイングします（この例では、IPパケットはIPパケットのIPヘッダーにマッピングされます）。その後、クライアントに送信します。



- Flexconnectローカルスイッチング：アップストリームの信頼

クライアントがフレームを送信し、APによって受信されます。APは、パケットを有線に送信する前に、元のパケットのDSCP値を参照してQoSポリシーを適用します。



## アップストリームトラフィックに関する一般的な問題

ワイヤレスクライアントとAP間のアップストリームシナリオのトラフィックは制御できません。つまり、クライアントから無線で送信されるQoSを制御できません。

正常に動作しているシナリオでは、クライアントは正しいUPおよびDSCP値を持つパケットを送信し、トラフィックが正しいアクセスカテゴリに入ることを想定しています。

クライアントが誤ったUP値を持つトラフィックを送信するとどうなりますか。

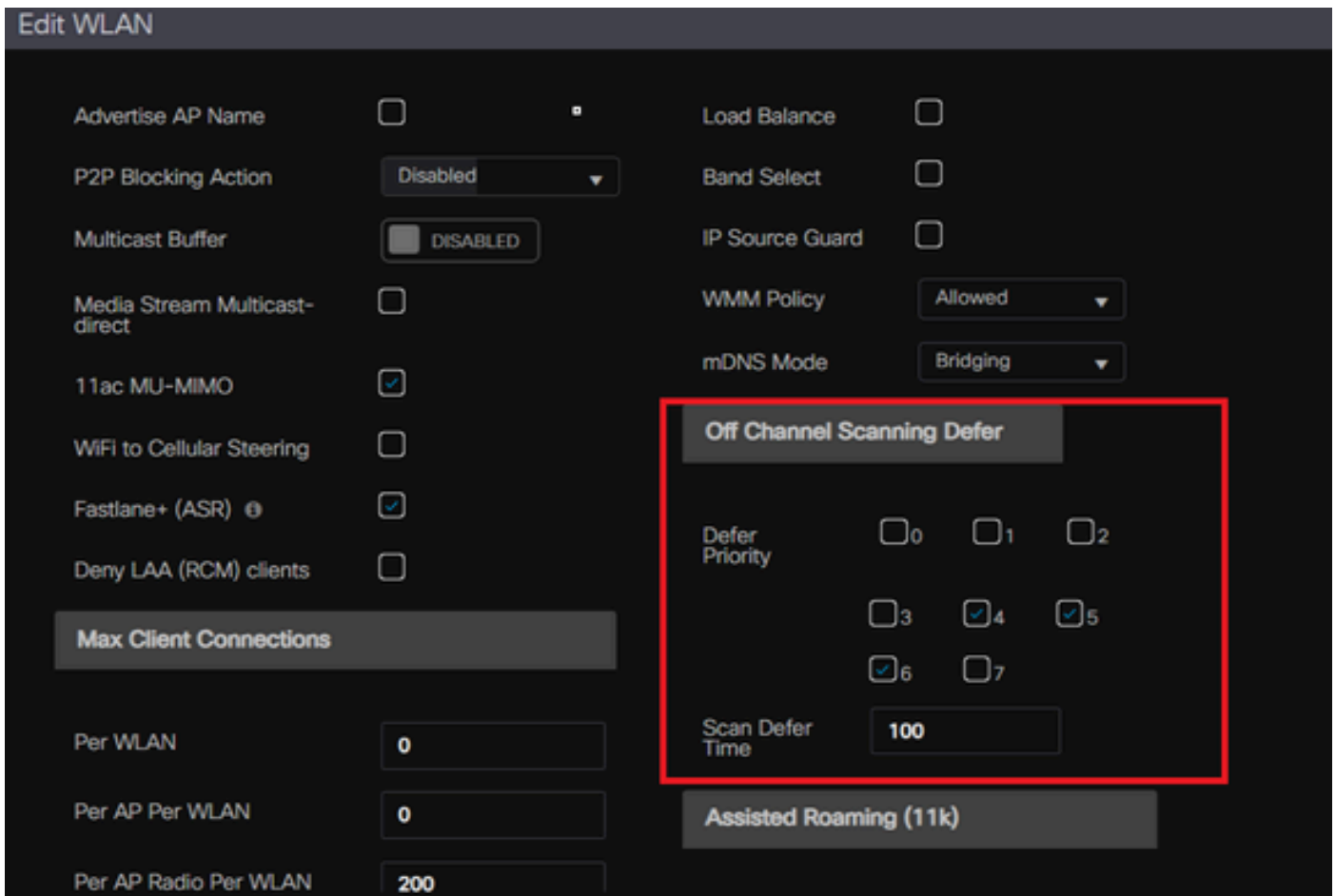
### 例#1：クライアントがUP値が「2」のトラフィックを送信するとき

注：RRMアルゴリズムに必要な情報を収集するために、APはオフチャネルでスキャンを行います。これは、音声やビデオなどの機密トラフィックに確実に影響します。

Off Channel Scanning DeferオプションがWLAN Advancedタブで設定されている。デフォルトでは、UPクラス4、5、および6で有効になっており、時間しきい値は100ミリ秒です。これは、機密トラフィック（音声またはビデオ）が検出された後、APが100ミリ秒間スキャンするためにオフチャネルにならないことを意味します。

ワイヤレスクライアントが音声アプリケーションを使用していると仮定すると、予期されるUP値は「6」ですが、クライアントは誤ったUP値「2」でパケットを送信しました。その後、APはオフチャネルスキャンを実行し、これはクライアントのパフォーマンスとエクスペリエンスに影響します。





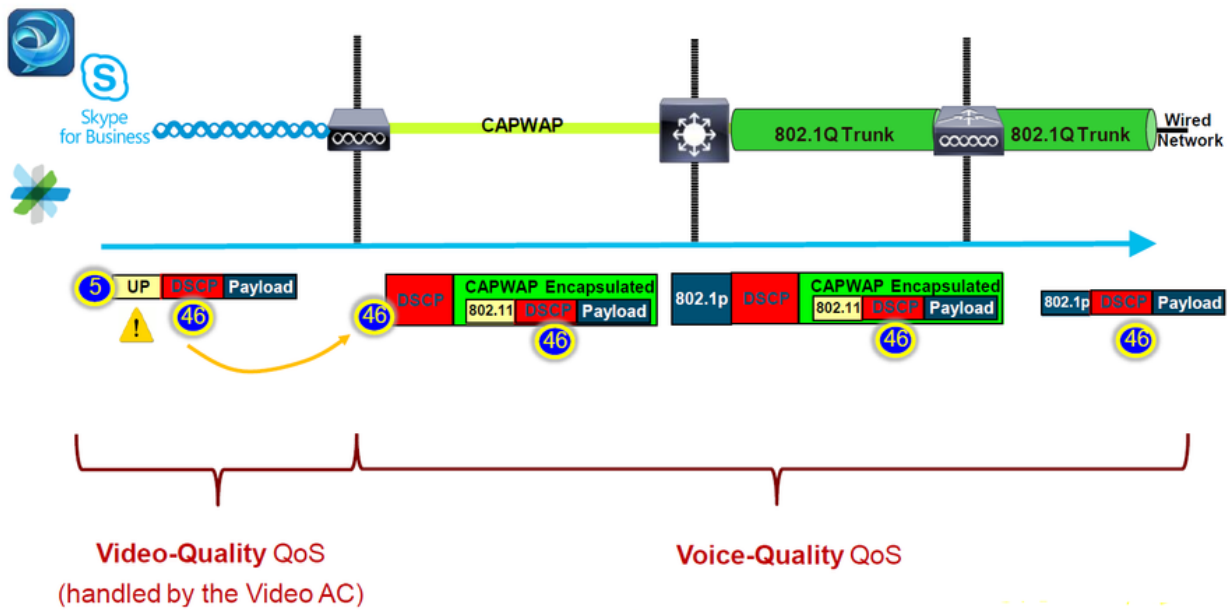
低いUPプライオリティに対してDefer Scanningを有効にできますか。

答えは「はい」です。低いUPプライオリティトラフィックに対してDefer Scanningを有効にすると、アクセスポイントがオフチャネルスキャンを実行することを効果的に防止できるため、RRMと不正検出アルゴリズムの動作に影響を与えます。この課題に対処するには、チャンネルのスキャンを容易にしながら、重要なトラフィックに優先順位を付ける別のアプローチが必要です。

## 例#2:DSCPからUPへのマッピングにおける既知のMicrosoft Windowsクライアントの問題

MS Windowsマシンでよく見られる問題は、DHCPとUP値の間のデフォルトマッピングが使用されている場合に発生します。このマッピングでは、Differentiated Services Code Point(DSCP)値の上位3ビット(msb)からユーザプライオリティ(UP)が決定されます。たとえば、DSCP値がEF(101110)の音声トラフィックの場合は、UP 5(101)にマッピングされます。

デフォルトでは、アップストリームのAPはUP値を信頼します。このため、音声トラフィックは、意図されたDSCP値46の音声アクセスカテゴリ(AC\_VO)ではなく、DSCP値34のビデオアクセスカテゴリ(AC\_VI)で処理されます。このため、音声フレームの待ち時間が長くなり、再試行の可能性が高くなります。

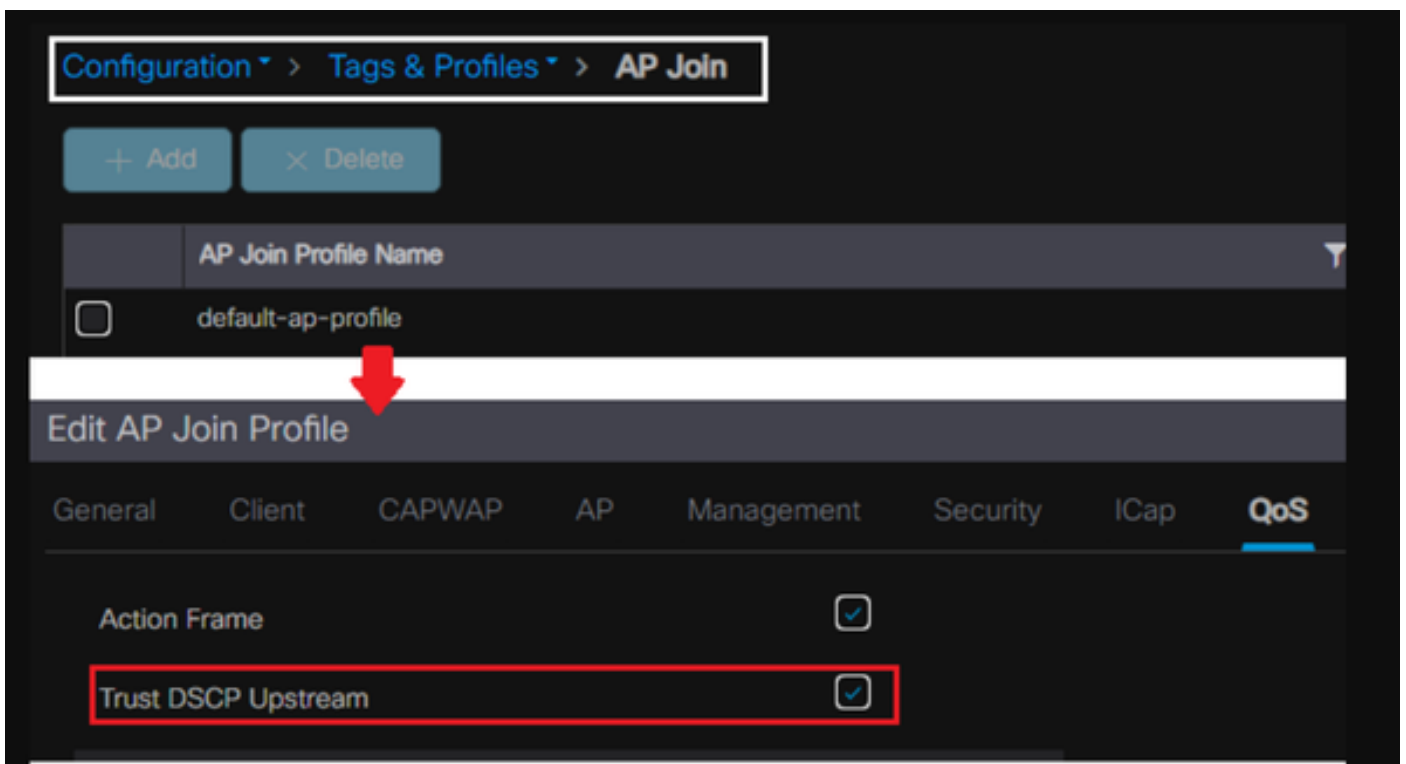


これを修正する方法はありますか。

MS Windowsマシンが正しいDSCP値で音声トラフィックを送信する場合、答えは「はい」です。

それはどのように修正できますか？

WLCで「trust DSCP Upstream」オプションを使用する。このオプションにより、APはUPではなくアップストリームの内部DSCPを信頼するようになります。



トラフィックを上書きするか、またはタグ付けするようにWindowsマシンを設定する詳細な手順

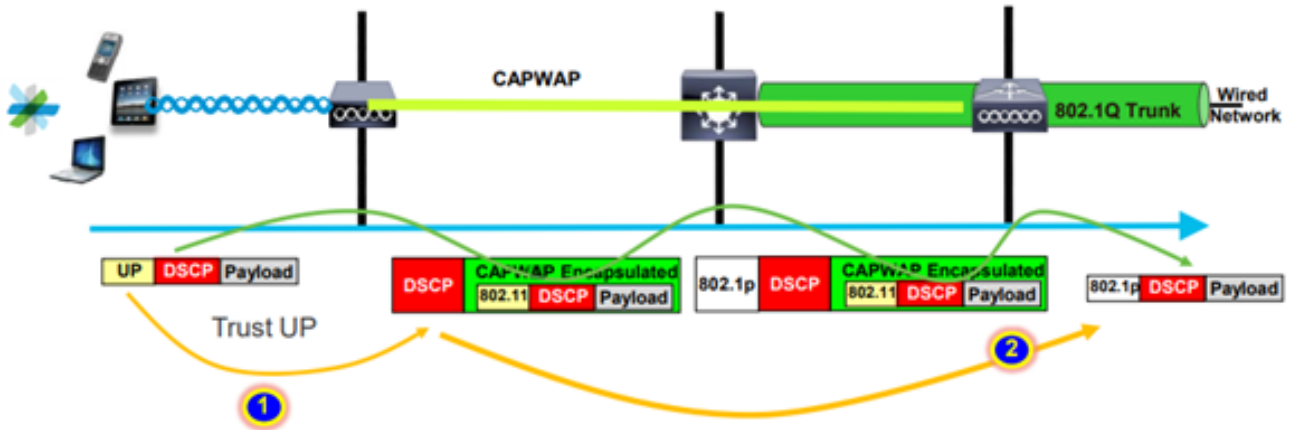
については、「[WindowsマシンでDSCPタギングを有効にする方法](#)」を参照してください。

## DSCPとCOSのどちらのプロトコルを信頼するか？

WLCスイッチポートに選択する信頼タイプはどれか？

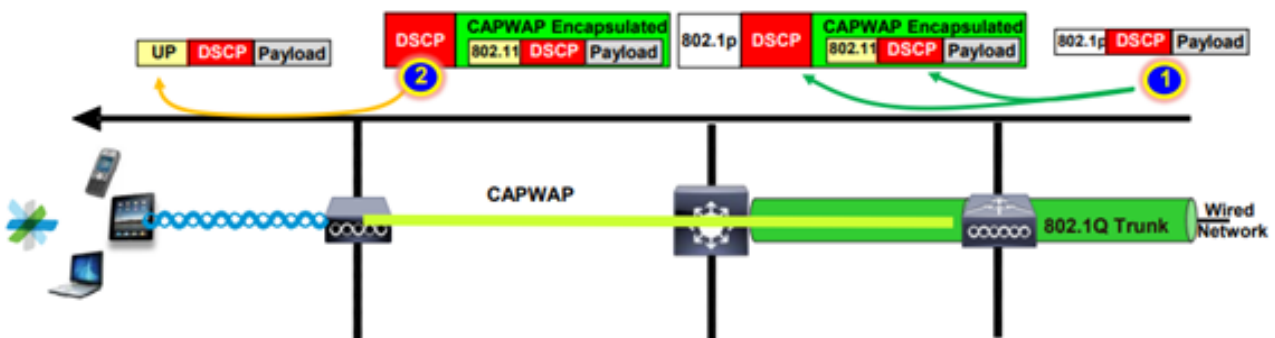
実際には、任意の信頼オプションを選択できます。ただし、CoSを信頼することを選択した場合は、アップストリームのシナリオに対して、スイッチに設定されたCoS-DSCPマッピングテーブルに基づいて外部DSCP値が書き換えられることに注意する必要があります。

ただし、DSCPを信頼するように選択すると、スイッチは着信の内部DSCPを信頼するため、外部DSCP値を書き換えません。



ダウンストリームシナリオでは、WLCが接続されているスイッチは、設定されているDSCP-CoSマッピングテーブルに基づいて802.1p値を追加します。CoSを信頼することを選択した場合、外部DSCP値は着信802.1p値に基づいて変更されます。

ただし、DSCPを信頼するように選択した場合、スイッチは外部DSCP値を書き換えません。



上記の例では、ワイヤレスクライアントはネイティブVLANの管理インターフェイスにマッピングされたSSIDに接続されています。

WLCスイッチポートでCoSを信頼する場合はどうなりますか。

クライアントトラフィックはタグなしのネイティブVLANであるため、トランクポートに到達しても802.1qにタグ付けされません。

これを修正するには、どうすればよいですか。

CoSの代わりにDSCP信頼オプションを使用できます。これは一般的に推奨される方法です。

## ワイヤレスLANコントローラQoSのベストプラクティス

### メタルQoSプロファイル

WLCでは、4つの主要なQoSプロファイル(Platinum、Gold、Silver、Bronze)を設定できます。

- Platinum/Voice:Voice over Wirelessの高品質なサービスを保証します。
- ゴールド/ビデオ：高品質ビデオアプリケーションをサポートします。
- シルバー/ベストエフォート：クライアントの通常の帯域幅をサポートします。これがデフォルト設定です。
- ブロンズ/バックグラウンド：ゲストサービスに最低帯域幅を提供します。

これらのQoSプロファイルの主な目的は、内部DSCPに影響を与えずに、アップストリームとダウンストリームの両方でCAPWAPヘッダーの最大外部DSCP値を制限することです。

注：内部DSCP値はAVCによって変更されます。

ローカルでスイッチされるトラフィックの場合、QoSプロファイルはUP値に基づいてダウンストリームトラフィックに適用されます。この値がデフォルトのWLAN値よりも大きい場合、デフォルトのWLAN値が使用されます。

アップストリームトラフィックの場合、クライアントがデフォルトのWLAN値よりも高いUP値を送信すると、デフォルトのWLAN値が使用されます。

9800 WLCのベストプラクティス設定ガイドの詳細については、『[Catalyst 9800ワイヤレスコントローラのワイヤレスQoS](#)』

トラブルシューティングの手順：

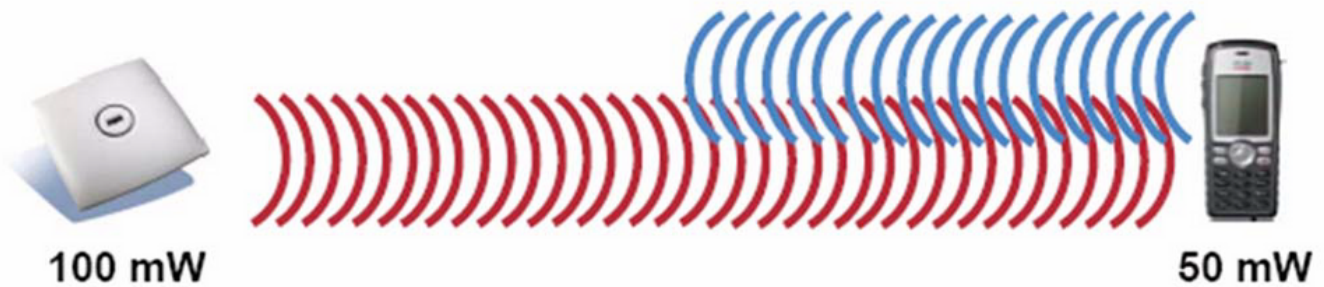
1. 問題を理解する。
2. 堅実なアクションプランを作成します。
  - トラブルシューティングに関する質問とネットワークトポロジダイアグラムを作成する。
  - ログとデバッグを収集します。
  - PIヒートマップを要求します。
3. [WLC設定をチェックします。](#)
4. デバッグの分析

5. VoWLAN[チェックリスト](#)を使用して、ベストプラクティスに従っているかどうかを確認します。

## 片通話について

この問題は主に、クライアントとAPの間に非対称電力がある場合に発生します。

APは最大電力で送信できますが、Ciscoの電話などのワイヤレスデバイスはより少ない電力で送信するため、Ciscoの電話はAPからのダウンストリームフレームを受信しますが、APは電話からのアップストリームのフレームを受信しません。



APのTX電力を、ワイヤレスデバイスでサポートされている最大のTX電力よりも高く設定しないことを推奨します。

- アクションプラン：
  - クライアント接続をチェックし、安定していて、切断されていないことを確認します。
  - RF環境 ( APの電力、信号強度など ) を確認します。
  - 音声トラフィックを確認するためにOTAキャプチャを収集します。単方向のトラフィックが見られます。
- ベストプラクティス：
  - DTPCの有効化：CCXクライアントがAPの電力に合わせて送信電力を調整するのに役立ちます。
  - クライアントデバイスのボリューム設定を確認します。

## 音声のとぎれや不自然な音声について

「途切れる」音声と「ロボットのよう」な音声は、パケット損失が大きい場合や、パケットの遅延が発生している場合に発生します。

Choppy Voice ( 途切れる音声 ) とは、音声の途切れや遅延を意味します。これらは、[choppy](#)および[robotic](#)レコードの例です。

- アクションプラン：
  - クライアント接続をチェックし、接続が安定していて、切断されていないことを確認します。
  - RF環境をチェックする ( チャンネル使用率が高い、ノイズ、干渉デバイスなど ) 。
  - パスを通じてキャプチャを収集し、パケットドロップを確認します。

- ベスト プラクティス:
  - [WLCのQoS設定をチェックします。](#)
  - 有線側でQoSが設定されていることを確認します。

## ローミング時の音声のギャップと欠落について

ある場所から別の場所にローミングしているときに、ユーザから音声の途切れや接続断が報告されることがあります。

- アクションプラン：
  - RF環境をチェックして、AP間のカバレッジセルが良好であることを確認します。
  - PIヒートマップを取得します。
  - パスを通じてキャプチャを収集し、パケットドロップを確認します。
- ベスト プラクティス:
  - クライアント接続をチェックし、安定していて、切断されていないことを確認します
  - 
  - 宛先APのRSSI値を-67以上にする

## 参考資料

### ワイヤレスQoSの推奨事項

[https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-9/config-guide/b\\_wl\\_17\\_9\\_cg/m\\_wireless\\_qos\\_cg\\_vewlc1\\_from\\_17\\_3\\_1\\_onwards.html](https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/17-9/config-guide/b_wl_17_9_cg/m_wireless_qos_cg_vewlc1_from_17_3_1_onwards.html)

『Application Visibility and Control Deployment Guide for Cisco Catalyst 9800 Series Wireless Controller』

<https://www.cisco.com/c/dam/en/us/td/docs/wireless/controller/9800/17-1/deployment-guide/c9800-avc-deployment-guide-rel-17-1.pdf>

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。