9800 WLCでのワイヤレスQoSの検証およびトラブルシューティングの設定

内容

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)でワイヤレスQuality of Service(QoS)を設定、検証、およびトラブルシューティングする方法について説明します。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- WLC:17.12.03を実行するC9800-40-K9
- アクセスポイント(AP):C9120-AX-D
- スイッチ：17.03.05を実行するC9300-48P

- 有線およびワイヤレスクライアント：Windows 10

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

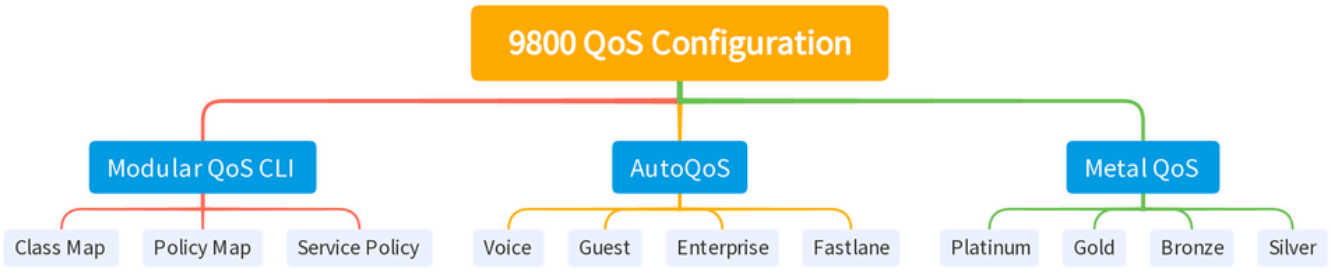
ワイヤレスQoSは、重要なアプリケーションが最適なパフォーマンスを得るために必要な帯域幅と低遅延を確実に受信するために不可欠です。このドキュメントでは、シスコワイヤレスネットワークでのQoSの設定、検証、およびトラブルシューティングに関する包括的なガイドを提供します。

この記事では、読者が無線と有線の両方のQoSの原則について基本的な知識を持っていることを前提としています。また、Cisco WLCとAPの設定および管理に習熟していることも期待されています。

コンフィギュレーション

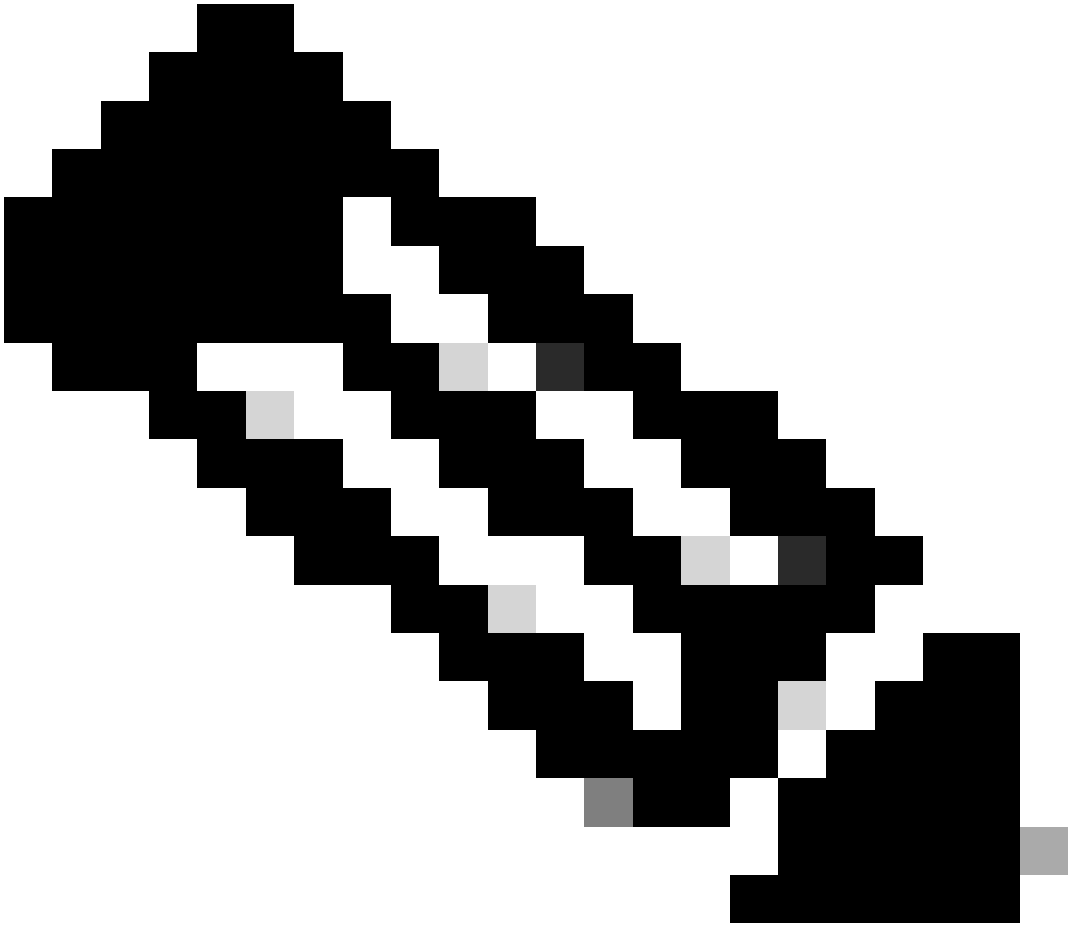
このセクションでは、9800ワイヤレスコントローラでのQoSの設定について詳しく説明します。これらの設定を活用することで、重要なアプリケーションが必要な帯域幅と低遅延を確実に受け取り、ネットワーク全体のパフォーマンスを最適化できます。

9800 WLCのQoS設定は、主に3つの大きなカテゴリに分けることができます。



9800 WLC QOS設定の概要

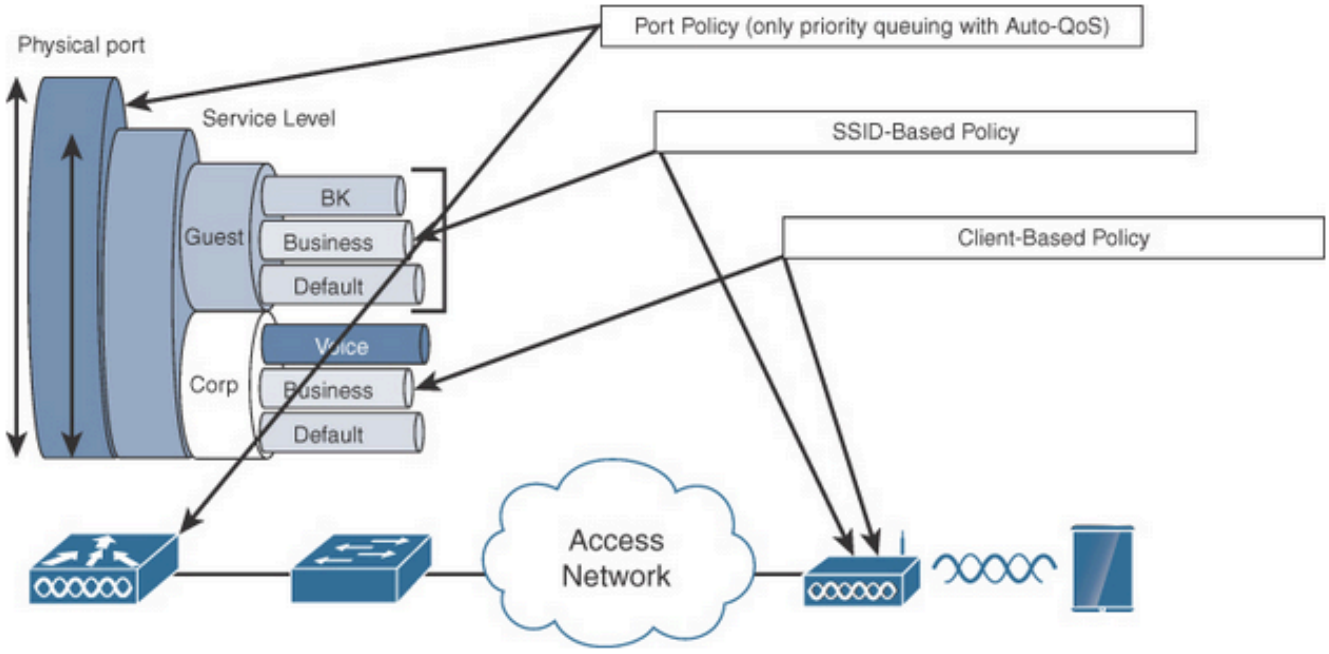
このドキュメントでは、以降のセクションで各セクションを1つずつ説明します。



注：この記事では、ローカルモードのAPに焦点を当てています。FlexConnectモードのAPについては説明しません。

QoSポリシーターゲット

ポリシーターゲットは、QoSポリシーを適用できる設定構成要素です。Catalyst 9800でのQoSの実装は、モジュール型で柔軟です。ユーザは、SSID、クライアント、ポートレベルの3つの異なるターゲットでポリシーを設定することを決定できます。



QoSポリシーターゲット

SSIDポリシーは、SSIDごとにAPごとに適用できます。SSIDでポリシングおよびマーキングポリシーを設定できます。

クライアントポリシーは、入力方向と出力方向で適用できます。クライアントにポリシングポリシーとマーキングポリシーを設定できます。AAAオーバーライドもサポートされています。

ポートベースのQoSポリシーは、物理ポートまたは論理ポートに適用できます。

自動 QoS

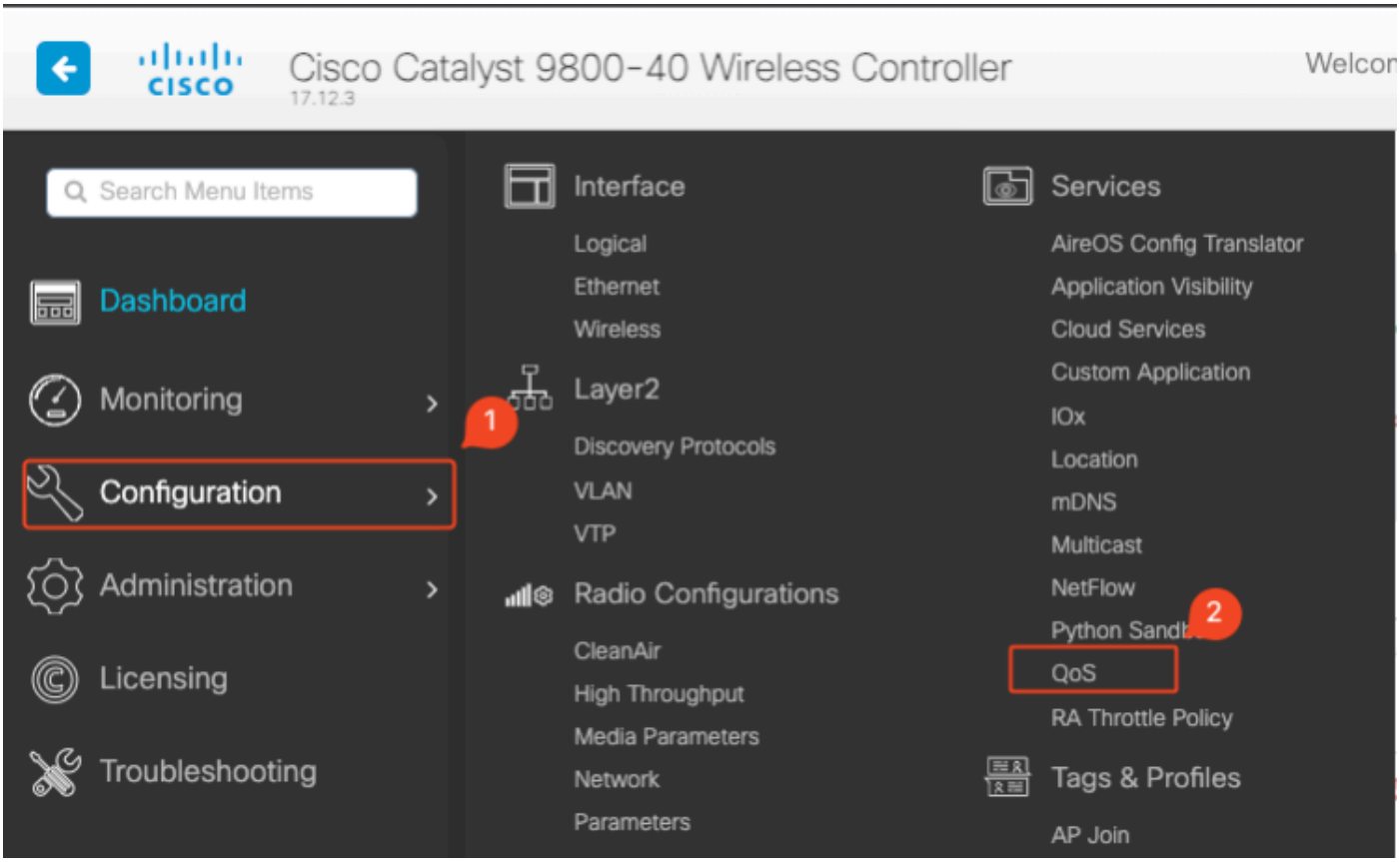
Wireless Auto QoSは、ワイヤレスQoS機能の導入を自動化します。また、事前定義された一連のプロファイルがあり、管理者はプロファイルをさらに変更して、さまざまなトラフィックフローに優先順位を付けることができます。Auto-QoSはトラフィックを照合し、一致した各パケットをQoSグループに割り当てます。これにより、出力ポリシーマップは特定のQoSグループをプライオリティキューなどの特定のキューに入れることができます。

モード	クライアント入力	クライアント出力	BSSID入力	BSSID出力	ポートの入力	ポートの出力	無線
音声	N/A	N/A	プラチナアップ	プラチナ	N/A	AutoQos-4.0-wlan – ポート – 出力 – ポリシー	ACMオン
ゲスト	N/A	N/A	自動Qos-4.0-wlan-	AutoQos-4.0-wlan-	N/A	AutoQos-4.0-	

			GT-SSID-Input-Policy	GT-SSID – 出力ポリシー		wlan – ポート – 出力 – ポリシー	
ファーストレーン	N/A	N/A	N/A	N/A	N/A	AutoQos-4.0-wlan – ポート – 出力 – ポリシー	EDCAパラメータFastLane
エンタープライズAVC	N/A	N/A	自動Qos-4.0-wlan-ET-SSID-Input-AVC-Policy	AutoQos-4.0-wlan-ET-SSID – 出力ポリシー	N/A	AutoQos-4.0-wlan – ポート – 出力 – ポリシー	

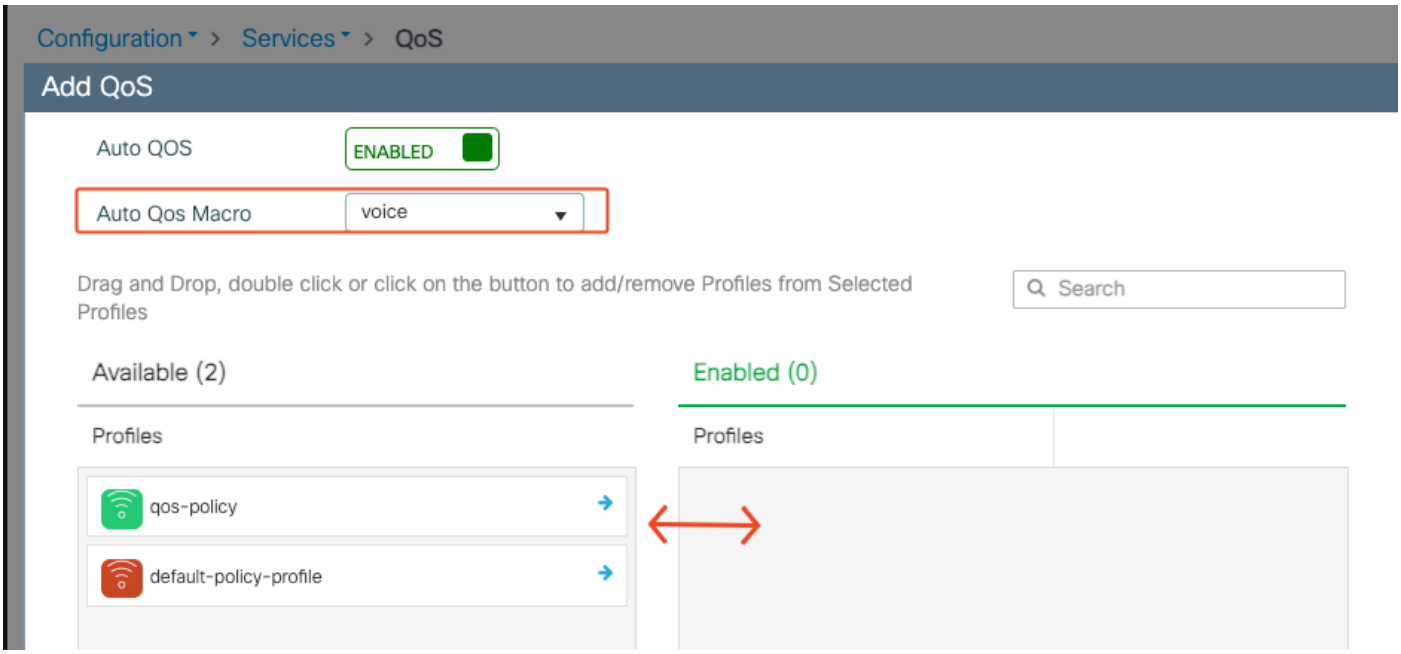
次の表に、自動QoSプロファイルが適用される際に発生する設定の変更を示します。

自動QoSを設定するには、Configuration > QoSの順に選択します。



QoSワークフロー

Addをクリックして、Auto QoSをenabledに設定します。リストから適切な自動QoSマクロを選択します。この例では、音声トラフィックに優先順位を付けるVoiceマクロが使用されます。



AutoQoS音声マッピング

マクロを有効にした後、ポリシーに適用するポリシーを選択します。

自動QoS CLI設定

```
# enable
# wireless autoqos policy-profile default-policy-profile mode voice
```

Auto QoSが有効になったので、発生した変更を確認できます。このセクションでは、音声の設定変更を一覧で示します。

```
class-map match-any AutoQos-4.0-Output-CAPWAP-C-Class
 match access-group name AutoQos-4.0-Output-Acl-CAPWAP-C
class-map match-any AutoQos-4.0-Output-Voice-Class
 match dscp ef
policy-map AutoQos-4.0-wlan-Port-Output-Policy
 class AutoQos-4.0-Output-CAPWAP-C-Class
  priority level 1
 class AutoQos-4.0-Output-Voice-Class
  priority level 2
 class class-default
interface TenGigabitEthernet0/0/0
 service-policy output AutoQos-4.0-wlan-Port-Output-Policy
interface TenGigabitEthernet0/0/1
 service-policy output AutoQos-4.0-wlan-Port-Output-Policy
interface TenGigabitEthernet0/0/2
 service-policy output AutoQos-4.0-wlan-Port-Output-Policy
interface TenGigabitEthernet0/0/3
 service-policy output AutoQos-4.0-wlan-Port-Output-Policy
ip access-list extended AutoQos-4.0-Output-Acl-CAPWAP-C
 10 permit udp any eq 5246 16666 any
wireless profile policy qos-policy
```

```
 autoqos mode voice
 service-policy input platinum-up
 service-policy output platinum
ap dot11 24ghz cac voice acm
ap dot11 5ghz cac voice acm
ap dot11 6ghz cac voice acm
```

モジュラQoS CLI

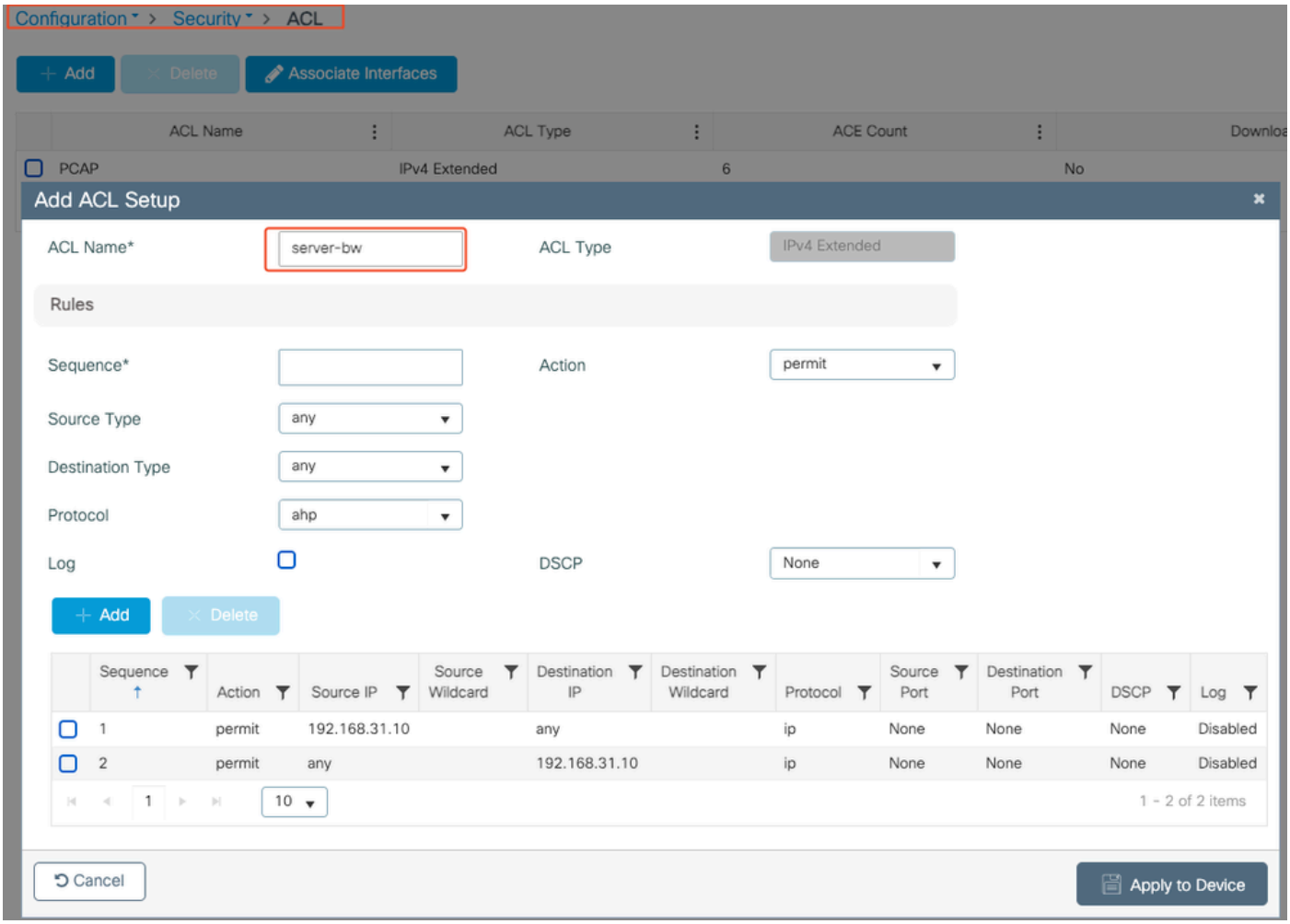
MQCを使用すると、トラフィッククラスを定義し、トラフィックポリシー（ポリシーマップ）を作成し、トラフィックポリシーをインターフェイスに割り当てることができます。トラフィックポリシーには、トラフィッククラスに適用されるQoS機能が含まれています。

MQS CLIワークフロー

この例では、アクセスコントロールリスト(ACL)を使用してトラフィックを分類し、帯域幅制限を適用する方法を示します。

管理する特定のトラフィックを識別および分類するACLを作成します。これは、IPアドレス、プロトコル、ポートなどの基準に基づいてトラフィックを照合するルールを定義することで実行できます。

Configuration > Security > ACLの順に移動し、ACLを追加します。

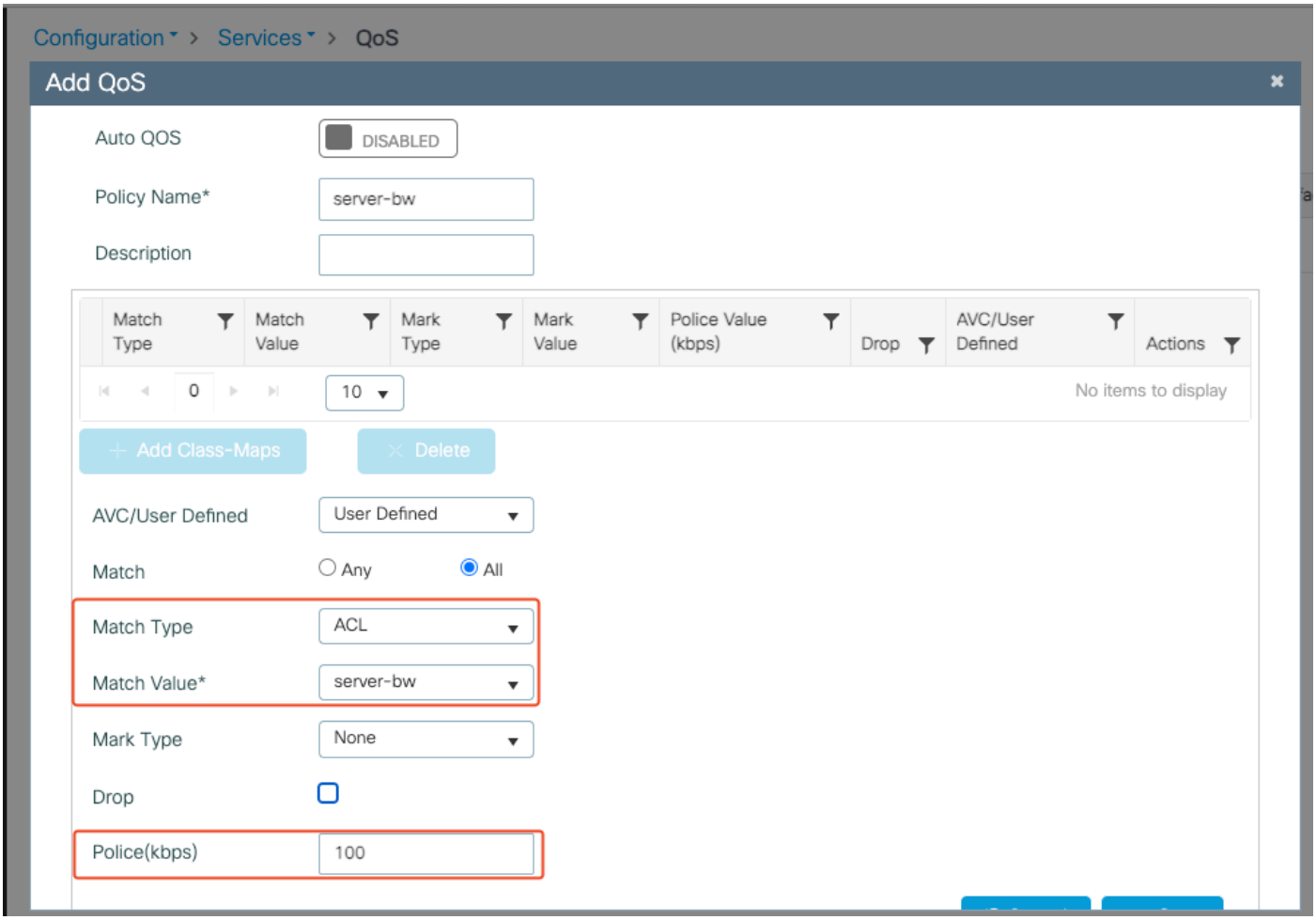


ACLの設定

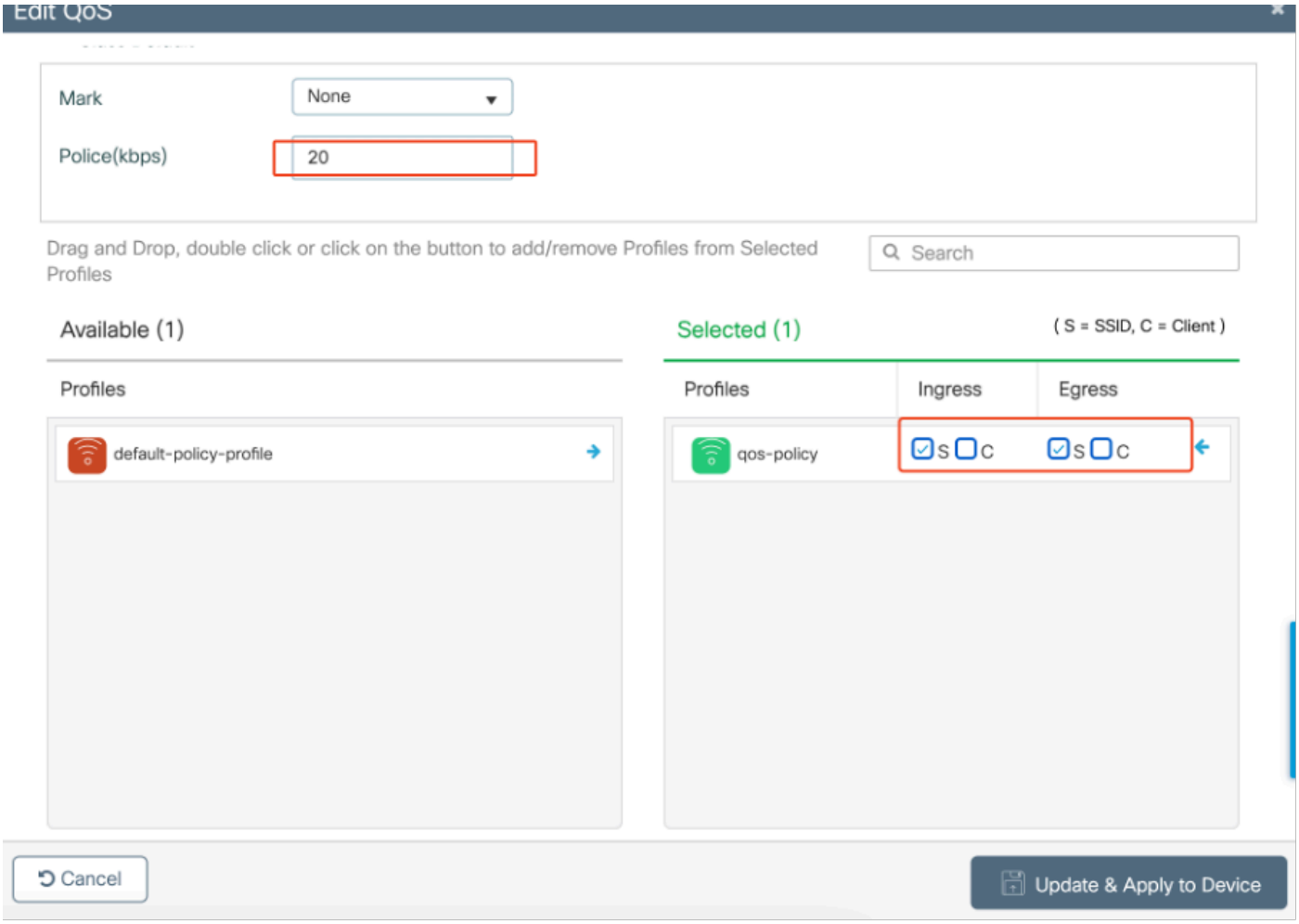
ACLを使用してトラフィックを分類したら、帯域幅の制限を設定して、このトラフィックに割り当てる帯域幅の量を制御します。

Configuration > Services > QoSの順に移動し、QoSポリシーを選択します。ポリシー内にACLを接続し、kbps単位でポリシングを適用します。

下にスクロールして、QoSを適用するポリシープロファイルを選択します。SSIDまたはクライアントの両方に対して、入力/出力方向のポリシーを選択できます。


Configuration
Services
QoS
Add QoS
Auto QOS
DISABLED
Policy Name*
server-bw
Description
Match Type
Match Value
Mark Type
Mark Value
Police Value (kbps)
Drop
AVC/User Defined
Actions
0
10
No items to display
Add Class-Maps
Delete
AVC/User Defined
User Defined
Match
Any
All
Match Type
ACL
Match Value*
server-bw
Mark Type
None
Drop
Police(kbps)
100

MQSポリシー



MQSプロファイル

MQS CLI設定

```
ip access-list extended server-bw
1 permit ip host 192.168.31.10  any
!
class-map match-any server-bw
match access-group name server-bw
!
policy-map server-bw
class server-bw
  police cir 100000
   conform-action transmit
   exceed-action drop
exit
class class-default
police cir 20000
conform-action transmit
exceed-action drop
exit
wireless profile policy default-policy-profile
service-policy input server-bw
service-policy output server-bw
exit
```

メタルQoS

これらのQoSプロファイルの主な目的は、ワイヤレスネットワークで許可されるDifferentiated Services Code Point(DSCP)の最大値を制限し、それによって802.11ユーザプライオリティ(UP)値を制御することです。

Cisco 9800ワイヤレスLANコントローラ(WLC)では、メタルQoSプロファイルが事前に定義されており、設定できません。ただし、これらのプロファイルを特定のSSIDまたはクライアントに適用して、QoSポリシーを適用できます。

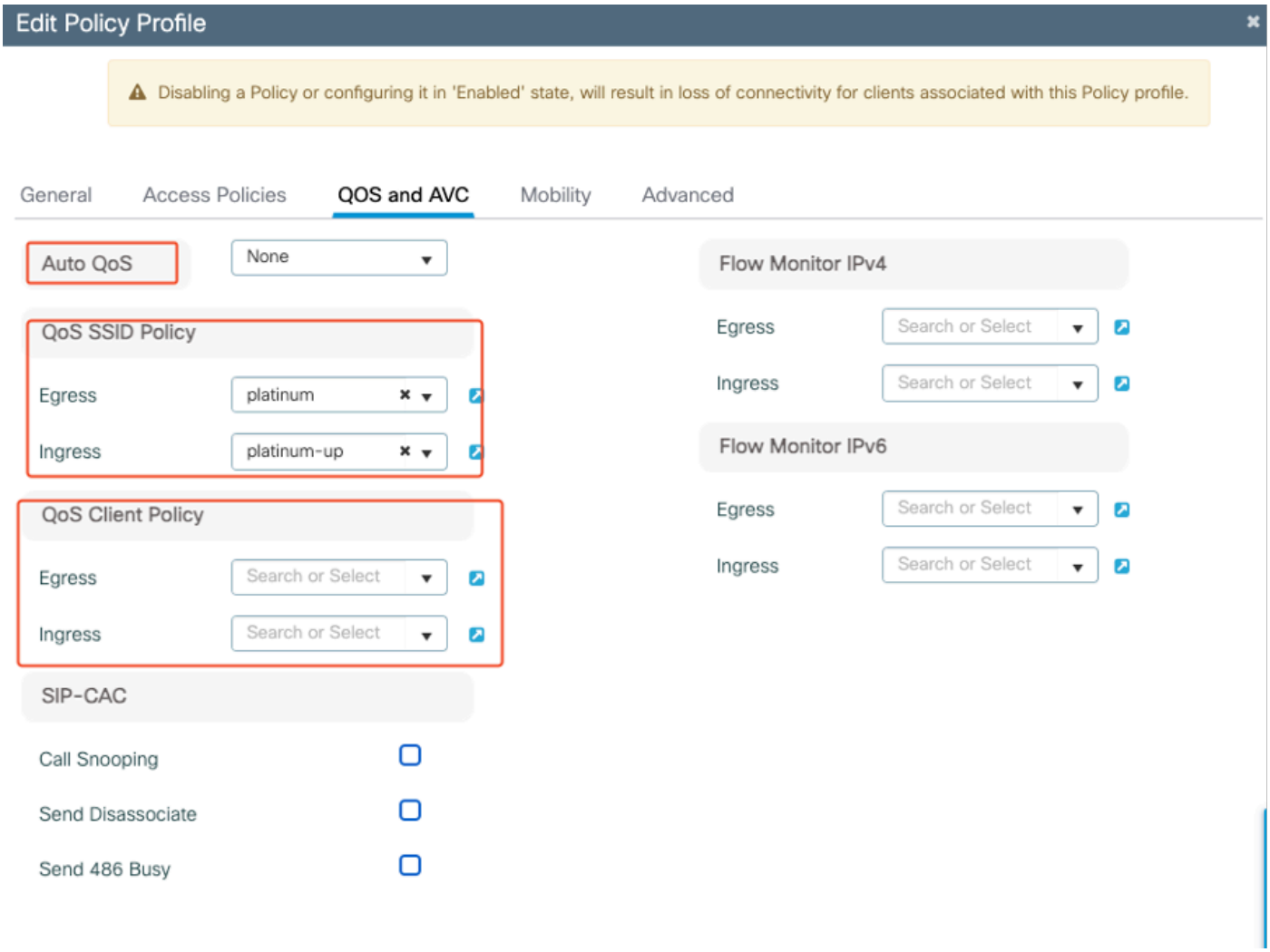
使用可能な4つのメタルQoSプロファイルがあります。

QoS プロファイル	最大DSCP
Bronze	8
シルバー	0
ゴールド	34
Platinum	46

Cisco 9800 WLCでメタルQoSを設定するには、次の手順を実行します。

Configuration > Policy > QoS & AVCの順に移動します。

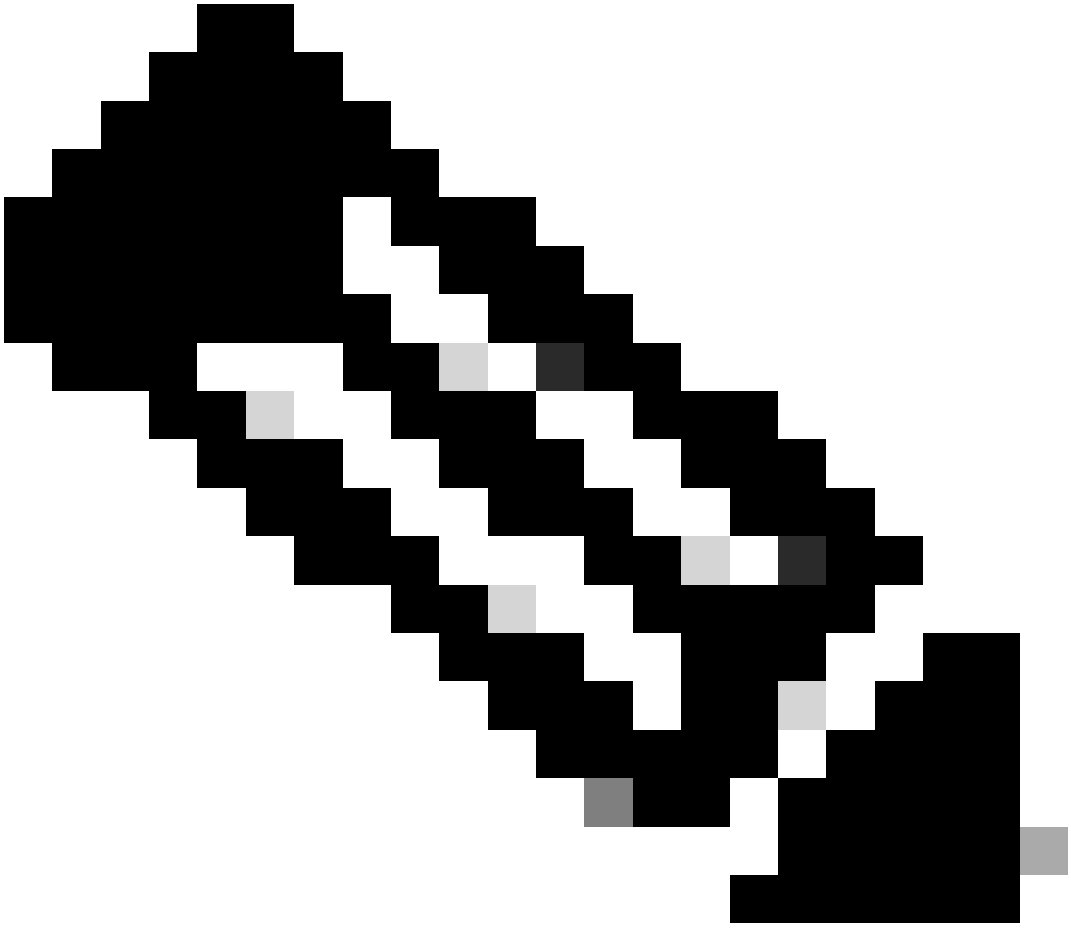
- 目的のMetal QoSプロファイル（Platinum、Gold、Silver、またはBronze）を選択します。
- 選択したプロファイルをターゲットSSIDまたはクライアントに適用します。



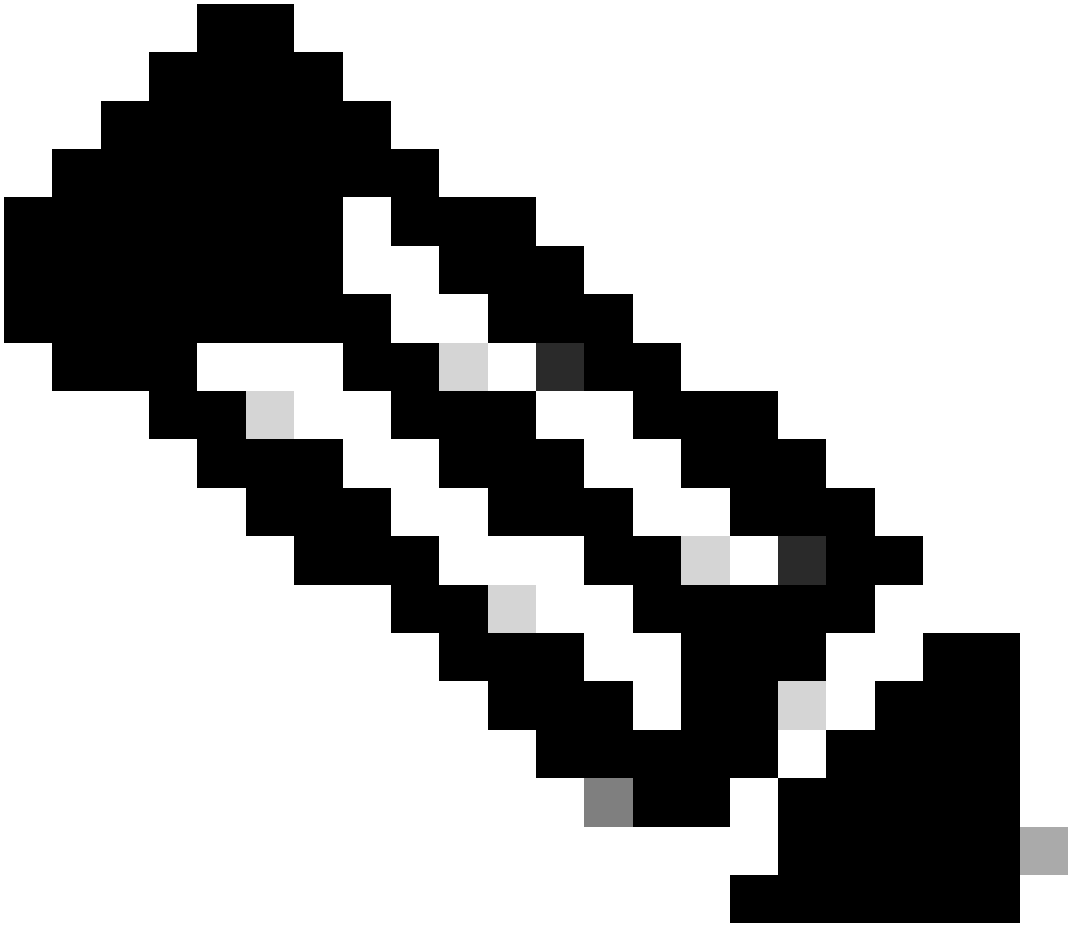
メタルQoSプロファイル

メタルQoS CLI設定

```
#configure terminal
#wireless profile policy qos-policy
 service-policy input platinum-up
 service-policy output platinum
```



注：ユーザ単位およびSSID単位の帯域幅契約は、Metal QoS上ではなく、QoSポリシーを通じて設定できます。9800では、一致しないトラフィックはデフォルトクラスに入ります。



注:GUIでは、SSIDごとにMetal QoSしか設定できません。CLIでは、クライアントターゲットで設定することもできます。

パケットキャプチャによるエンドツーエンドQoSの検証

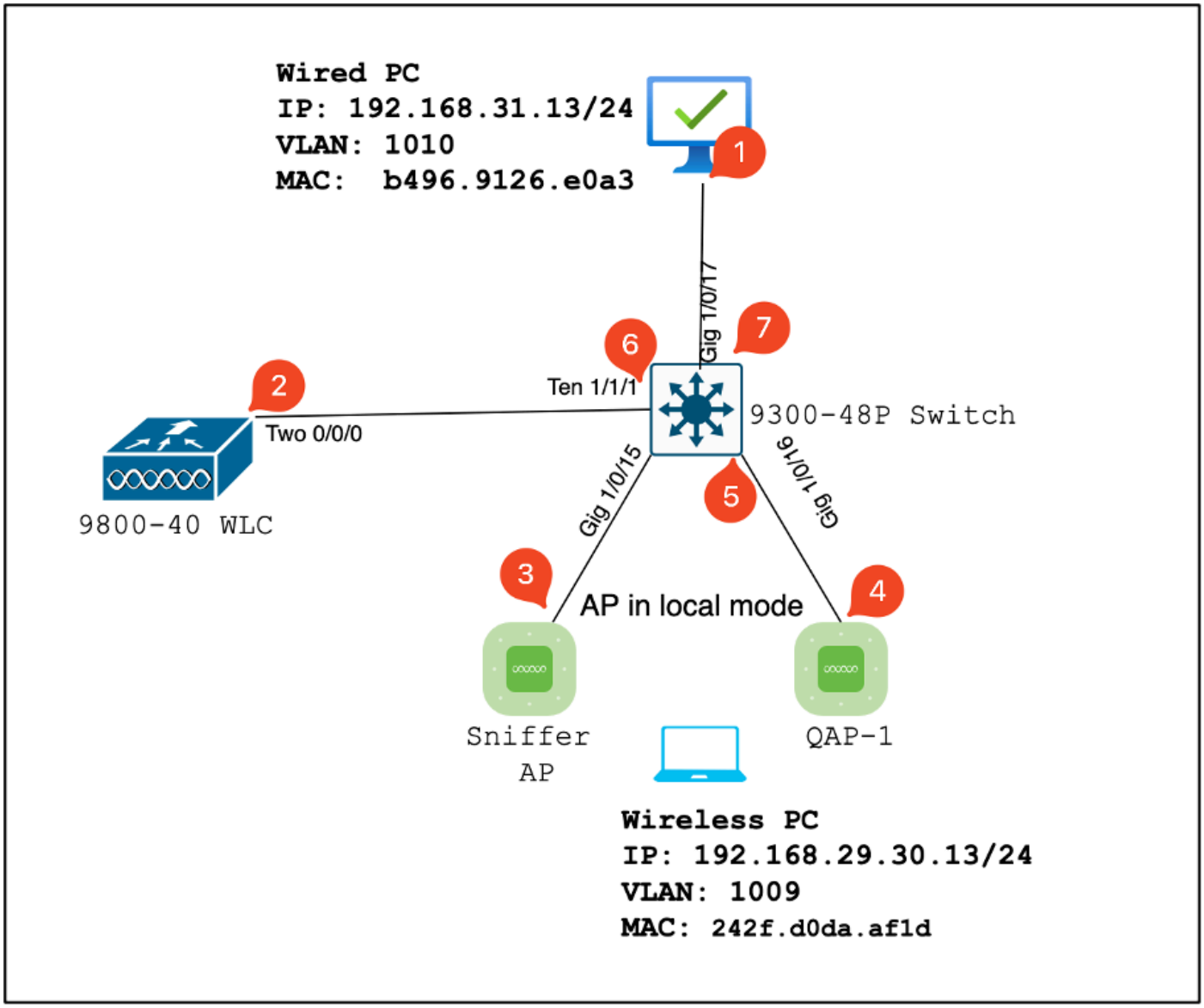
QoSの設定が完了したら、QoSパケットを調べ、QoSポリシーがエンドツーエンドで正しく機能していることを検証する必要があります。これは、パケットキャプチャと分析を通じて実現できます。

QoS設定を複製して検証するには、小規模なラボ環境を使用します。ラボには次のコンポーネントが含まれています。

- WLC
- AP
- OTAを取得するスニファAP
- 有線 PC
- 最大 300 のアクセス ポイント グループ

これらのコンポーネントはすべて、ラボ環境内の同じスイッチに接続されます。この図で強調表示されている数字は、トラフィックフローを監視および分析するためにパケットキャプチャが有効になっているポイントを示しています。

ネットワーク図



ラボのトポロジ

ラボのコンポーネントとパケットキャプチャポイント

次のステップを実行します。

- ワイヤレスネットワークのQoSポリシーと構成を管理します。
- パケットキャプチャポイント：WLC、AP、およびスイッチ間のトラフィックをキャプチャします。

AP：

- クライアントにワイヤレス接続を提供し、QoSポリシーを適用

- パケットキャプチャポイント：APとスイッチ間のトラフィックをキャプチャします。

スニファAP:

- ワイヤレストラフィックをキャプチャするための専用デバイスとして機能します。
- パケットキャプチャポイント：APとワイヤレスクライアント間のワイヤレストラフィックをキャプチャします。

有線PC:

- スイッチに接続して、有線トラフィックをシミュレートし、エンドツーエンドのQoSを検証します。
- パケットキャプチャポイント：有線リンクを介して送受信されるQoSパケットをキャプチャします。

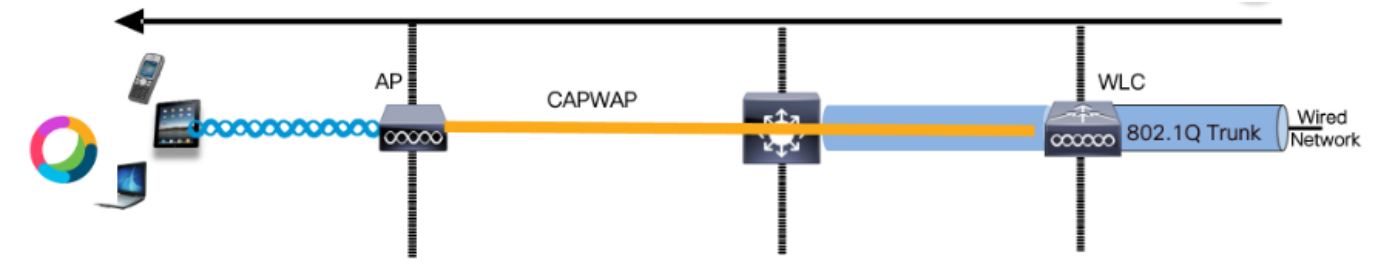
無線PC:

- WLANに接続して、ワイヤレストラフィックをシミュレートし、エンドツーエンドのQoSを検証する。
- パケットキャプチャポイント：ワイヤレスリンクを介して送受信されるQoSパケットをキャプチャします。

スイッチ：

- すべてのラボコンポーネントを相互接続し、トラフィックフローを容易にする中央デバイス。
- パケットキャプチャポイント：さまざまなスイッチポートでトラフィックをキャプチャし、適切なQoS適用を検証します。

論理的には、ラボトポロジは次のように作成できます。



論理ラボトポロジ

QoS設定をテストおよび検証するために、iPerfを使用してクライアントとサーバ間のトラフィックを生成します。これらのコマンドは、QoSテストの方向に基づいてサーバとクライアントの役割が相互に変更されるiPerf通信を促進するために使用されます。

テストシナリオ1：ダウンストリームQoSの検証

目的は、ダウンストリームQoS設定を検証することです。設定には、DSCP 46でパケットを無線PCに送信する有線PCが含まれます。
ワイヤレスLANコントローラ(WLC)には、ダウンストリーム方向とアップストリーム方向の両方

に対してメタルの「Platinum QoS」ポリシーが設定されています。

テストの設定：

- トラフィック フロー:

  出典：有線PC

  宛先：無線PC

  トラフィックタイプ：DSCPが46のUDPパケット

- WLCでのQoSポリシー設定：

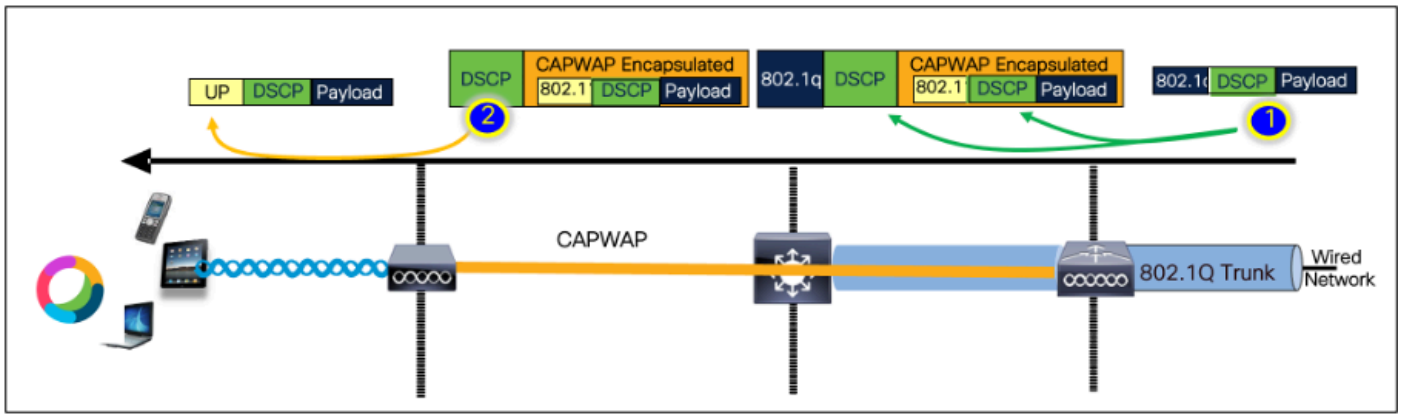
  QoSプロファイル：Metal QoS - Platinum QoS

  方向：ダウンストリームとアップストリームの両方

- メタルQoS設定コマンド：

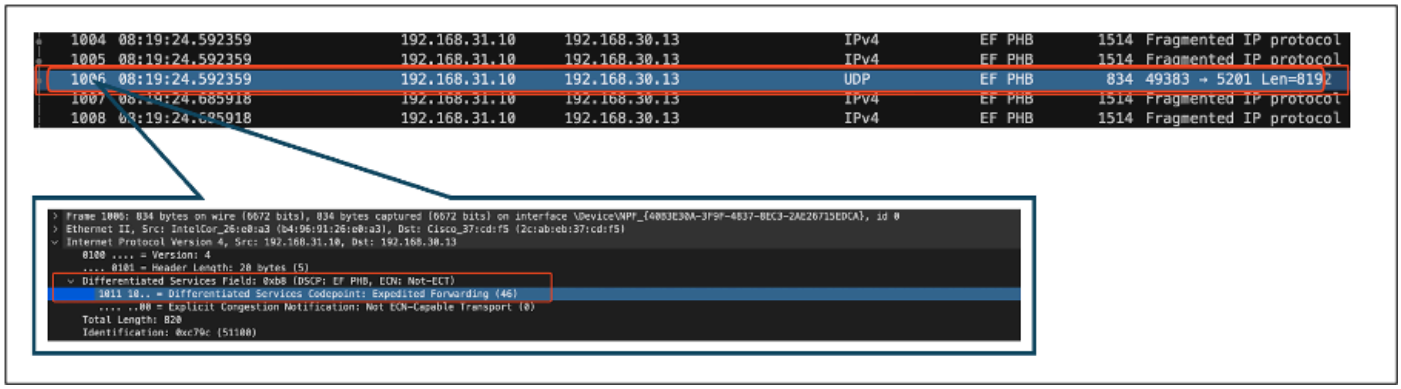
```
wireless profile policy qos-policy
service-policy input platinum-up
service-policy output platinum
```

論理トポロジとダウンストリーム方向のDSCPカンバセーション



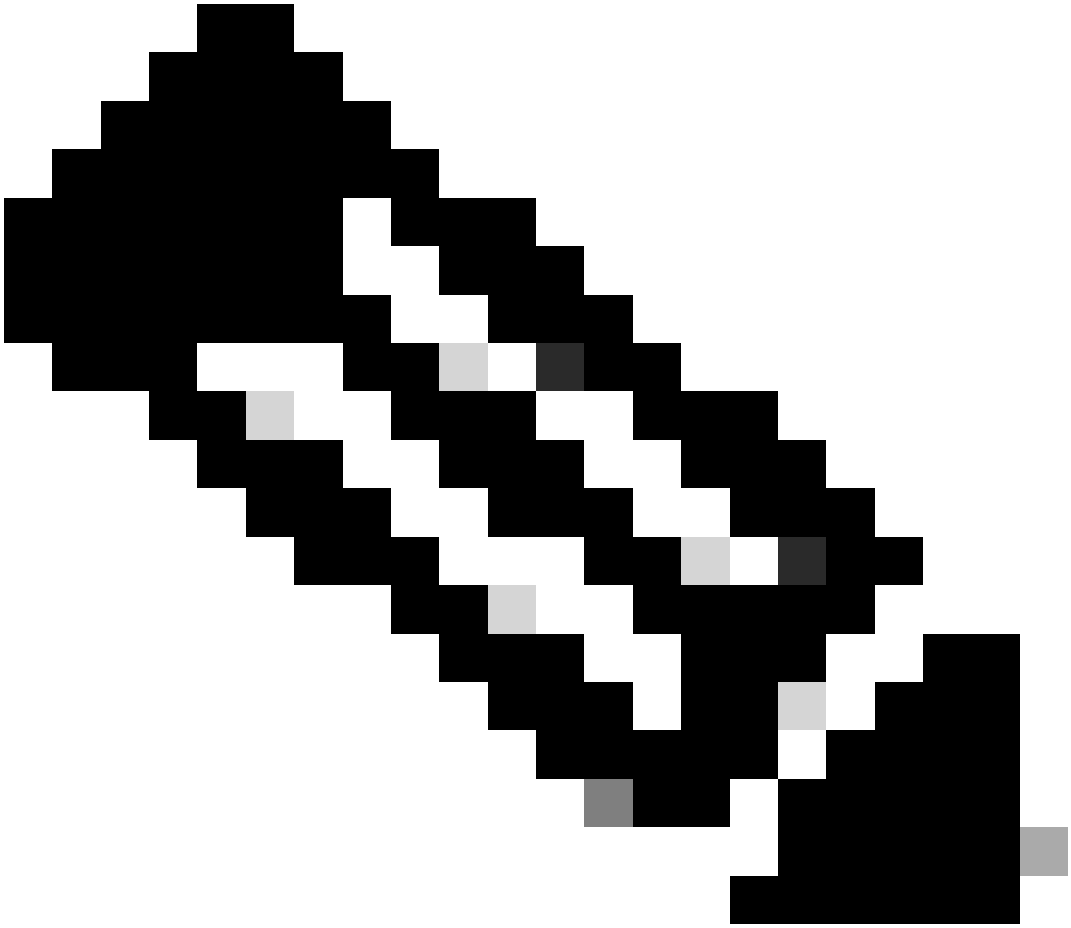
DSCPカンバセーションポイント

有線PCで取得されたパケットキャプチャ。これにより、有線PCが正しいDSCPマーキング46を使用して、指定された宛先IP 192.168.10.13にUDPパケットを送信していることを確認できます。

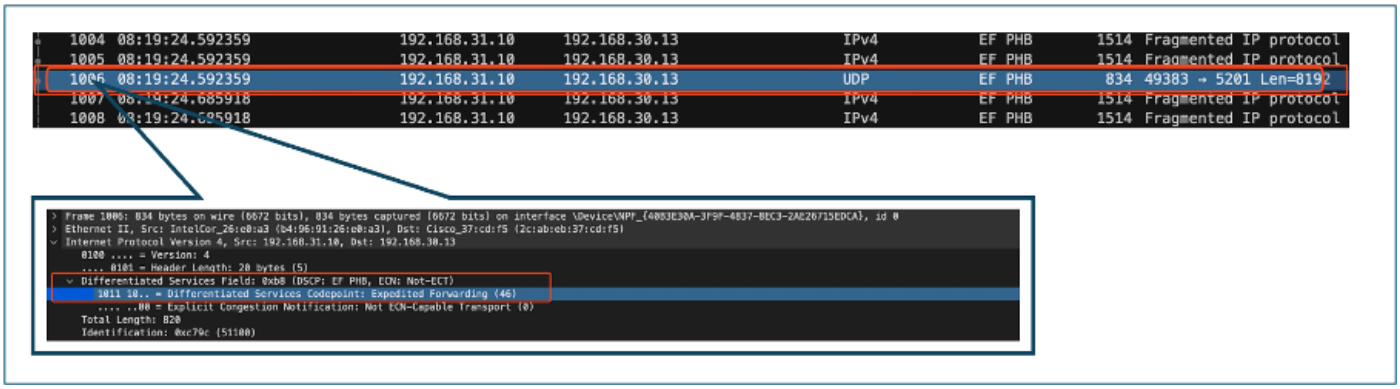


有線PCキャプチャ – ダウンストリーム方向

次に、有線PCに接続されたアップリンクスイッチでキャプチャされたパケットを調べます。スイッチはDSCPタグを信頼し、DSCP値は46のまま変わりません。

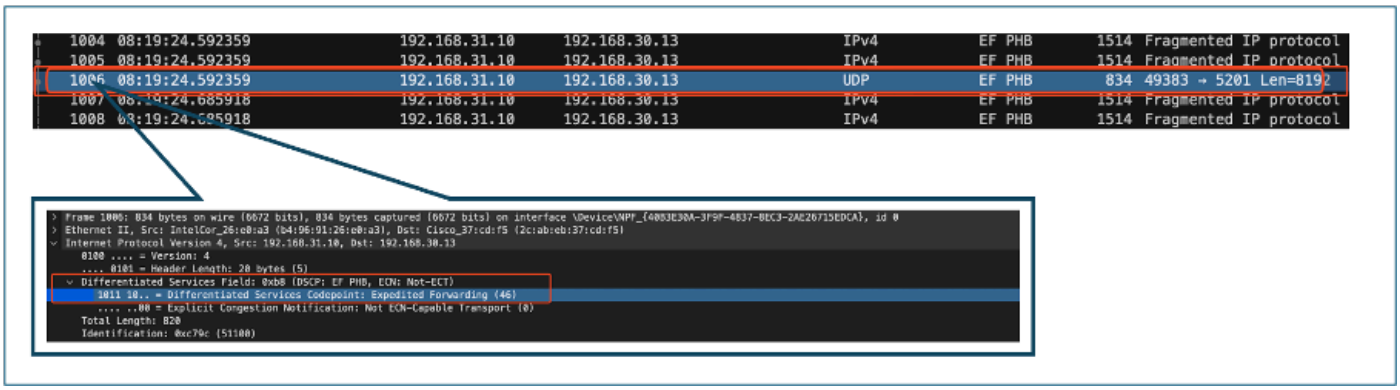


注：Catalyst 9000シリーズのスイッチポートは、デフォルトでtrusted状態になっています。



有線PCアップリンクインターフェイスのキャプチャ

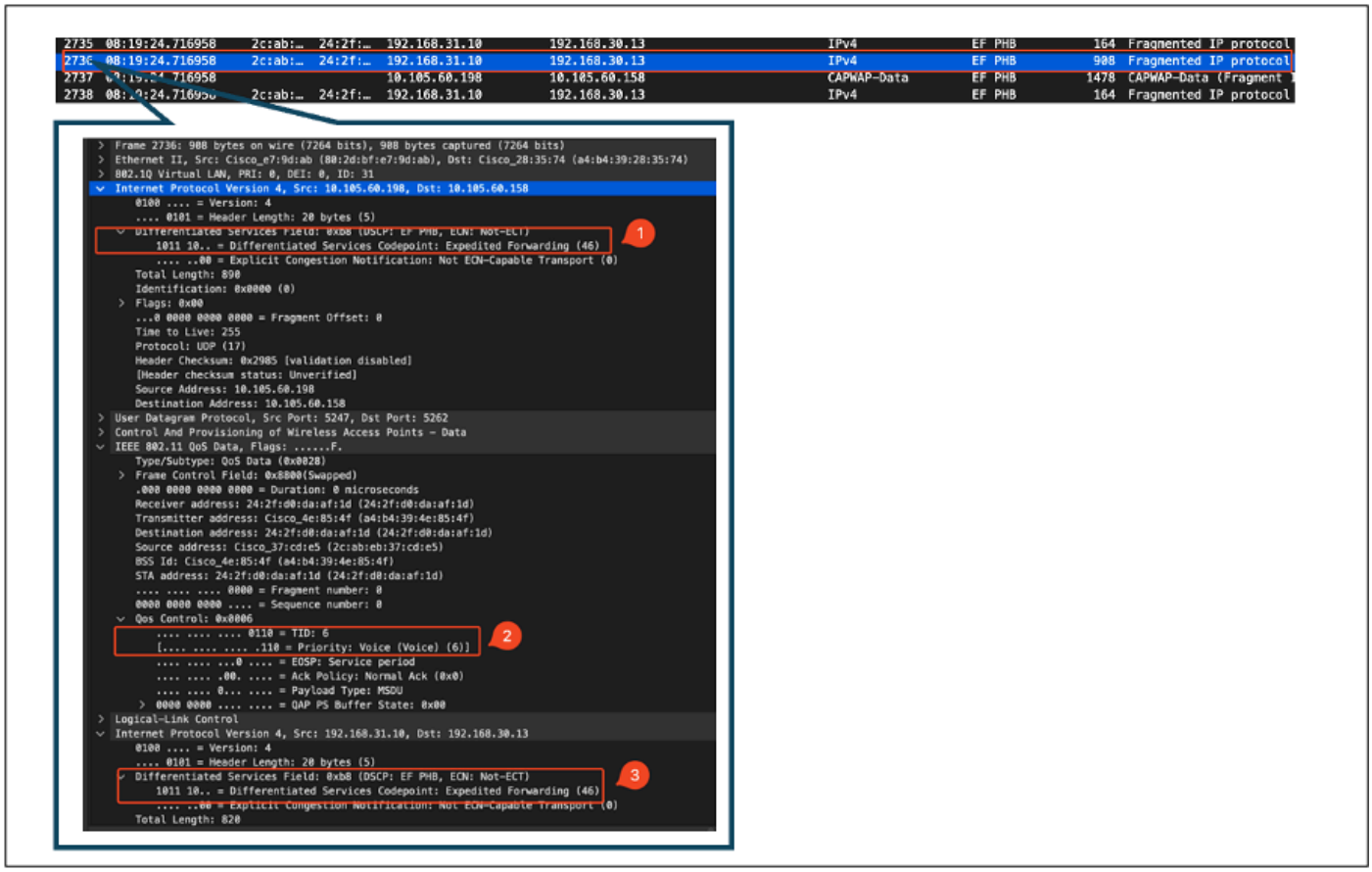
EPCを使用して取得したWLC上のパケットキャプチャを調べると、パケットはアップリンクスイッチから同じDSCPタグ46で到着します。 これにより、パケットがWLCに到達する際にDSCPマーキングが保持されていることを確認できます。



WLC EPCダウンストリーム方向

WLCがCAPWAPトンネル内のAPにパケットを送信する場合、これはWLCが設定に基づいてDSCPを変更できる重要な交差点です。わかりやすくするために、番号の付いたポイントで強調表示されているパケットキャプチャを分類します。

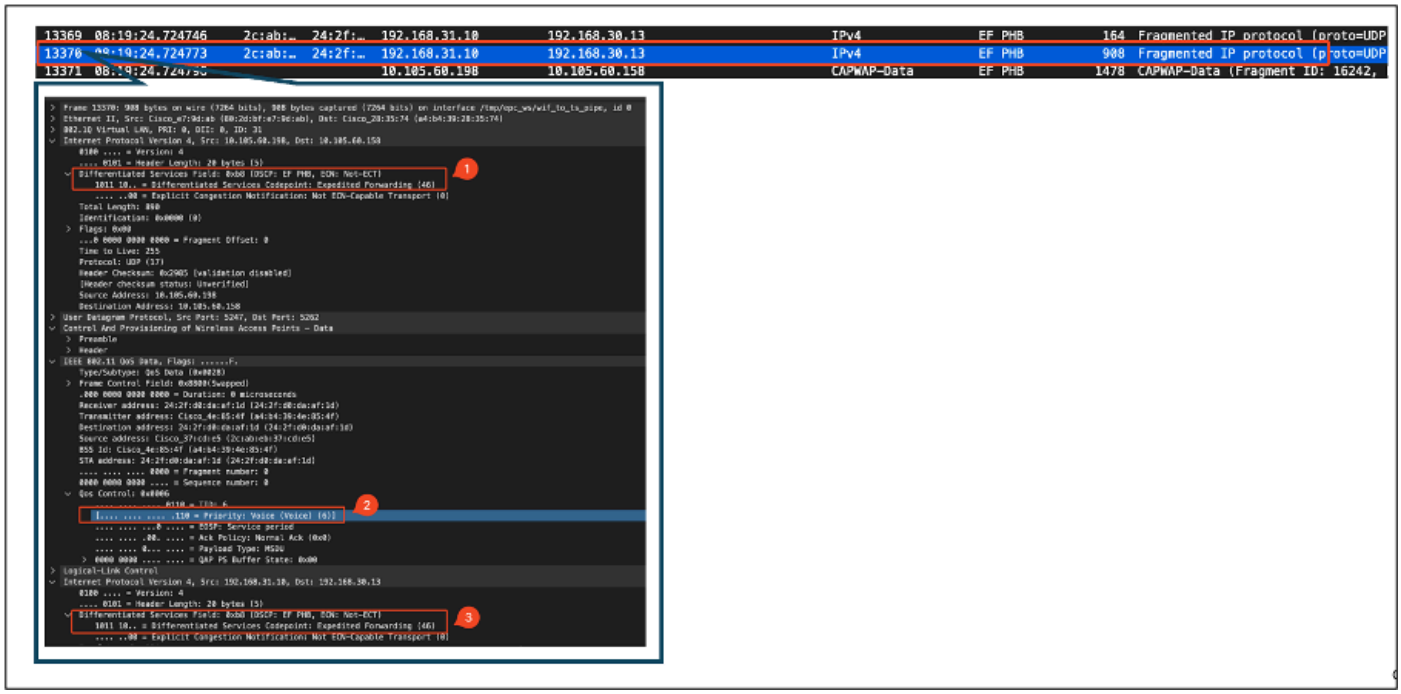
- CAPWAP外部層：CAPWAPトンネルの外部層では、DSCPタグが46として表示されます。これは、スイッチの端から受信した値です。
- CAPWAP内の802.11 UP値：CAPWAPトンネル内のWLCは、DSCP 46を音声トラフィックに対応する802.11ユーザプライオリティ(UP)6にマッピングします。
- CAPWAP内部のDSCP値：Cisco 9800 WLCはtrust DSCPモデルで動作するため、CAPWAPトンネル内部のDSCP値は外部のDSCPレイヤと同じく46に維持されます。



CAPWAP DSCPマーキング

次に、APアップリンクスイッチポートで同じパケットを確認します。

外部CAPWAPレイヤのDSCP値は46のままです。説明の便宜上、タギングを示すために内部CAPWAPトラフィックが強調表示されています。

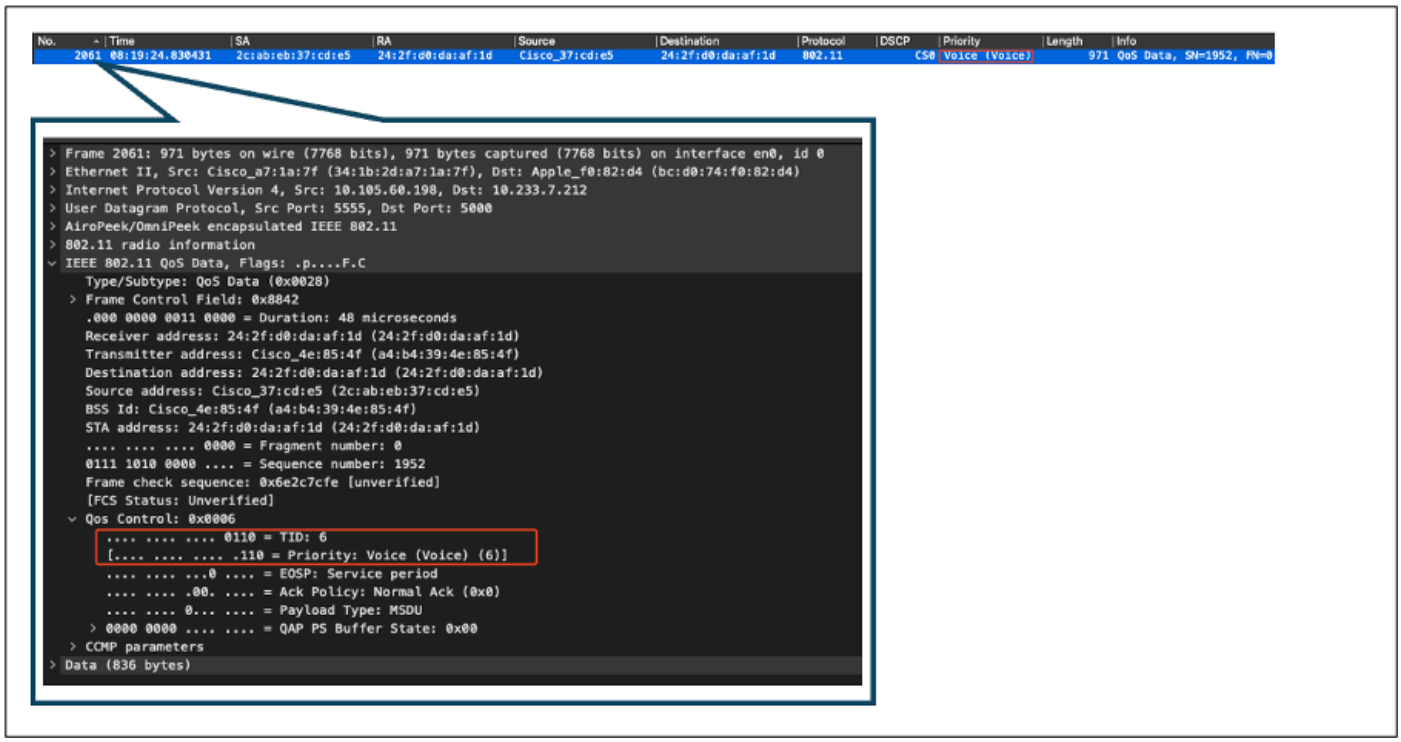


APアップリンクスイッチインターフェイスのキャプチャ

APはパケットを受信すると、そのパケットを無線で送信します。ユーザプライオリティ(UP)タギ

ングを確認するには、スニファAPで取得したOver-the-Air(OTA)キャプチャを使用します。

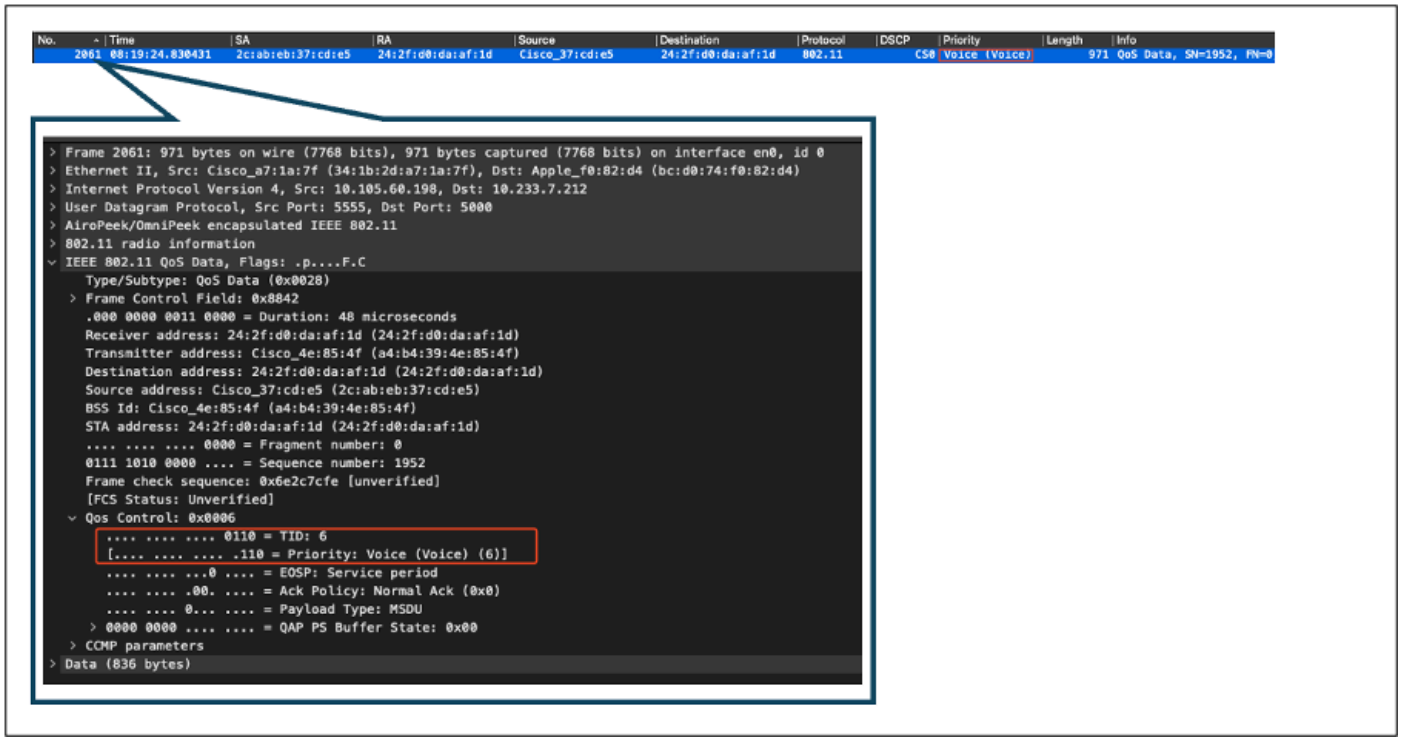
APはUP値6でフレームを転送しました。これにより、APがDSCP値を適切な802.11 UP値(6)に正しくマッピングしていることが確認されます。この値は音声トラフィックに対応しています。



APからクライアントへのOTAキャプチャ

最終段階では、無線PCがパケットを受信します。無線PCは、DSCP値が46のフレームを受信します。

これは、DSCPマーキングが有線PCから無線PCまでの伝送路全体で保持されることを示します。一貫したDSCP値の46は、QoSポリシーがダウンストリーム方向で正しく適用および維持されていることを確認します。



ワイヤレスPCキャプチャ

テストシナリオ2：アップストリームQoSの検証

このテストシナリオの目的は、アップストリームQoS設定を検証することです。設定には、DSCP 46のUDPパケットを有線PCに送信する無線PCが含まれます。WLCには、アップストリーム方向とダウンストリーム方向の両方に対してメタルの「Platinum QoS」ポリシーが設定されています。

- トラフィック フロー:

出典：Wireless PC

宛先：有線PC

トラフィックタイプ：DSCPが46のUDPパケット

- WLCでのQoSポリシー設定：

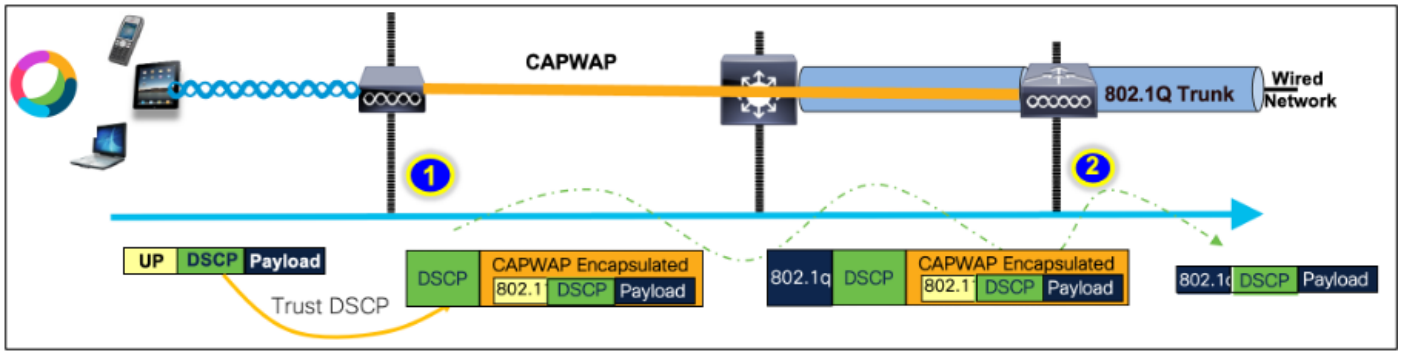
QoSプロファイル：Platinum QoS

方向：アップストリームとダウンストリームの両方

- メタルQoS設定コマンド：

```
wireless profile policy qos-policy
service-policy input platinum-up
service-policy output platinum
```

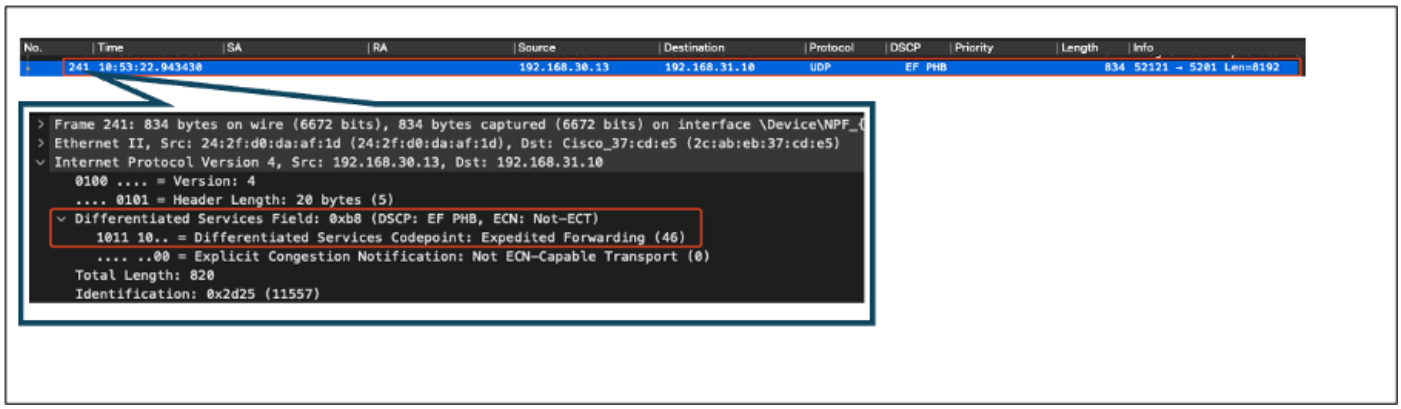
アップストリーム方向の論理トポロジとDSCP変換：



論理トポロジとDSCP変換 – アップストリーム

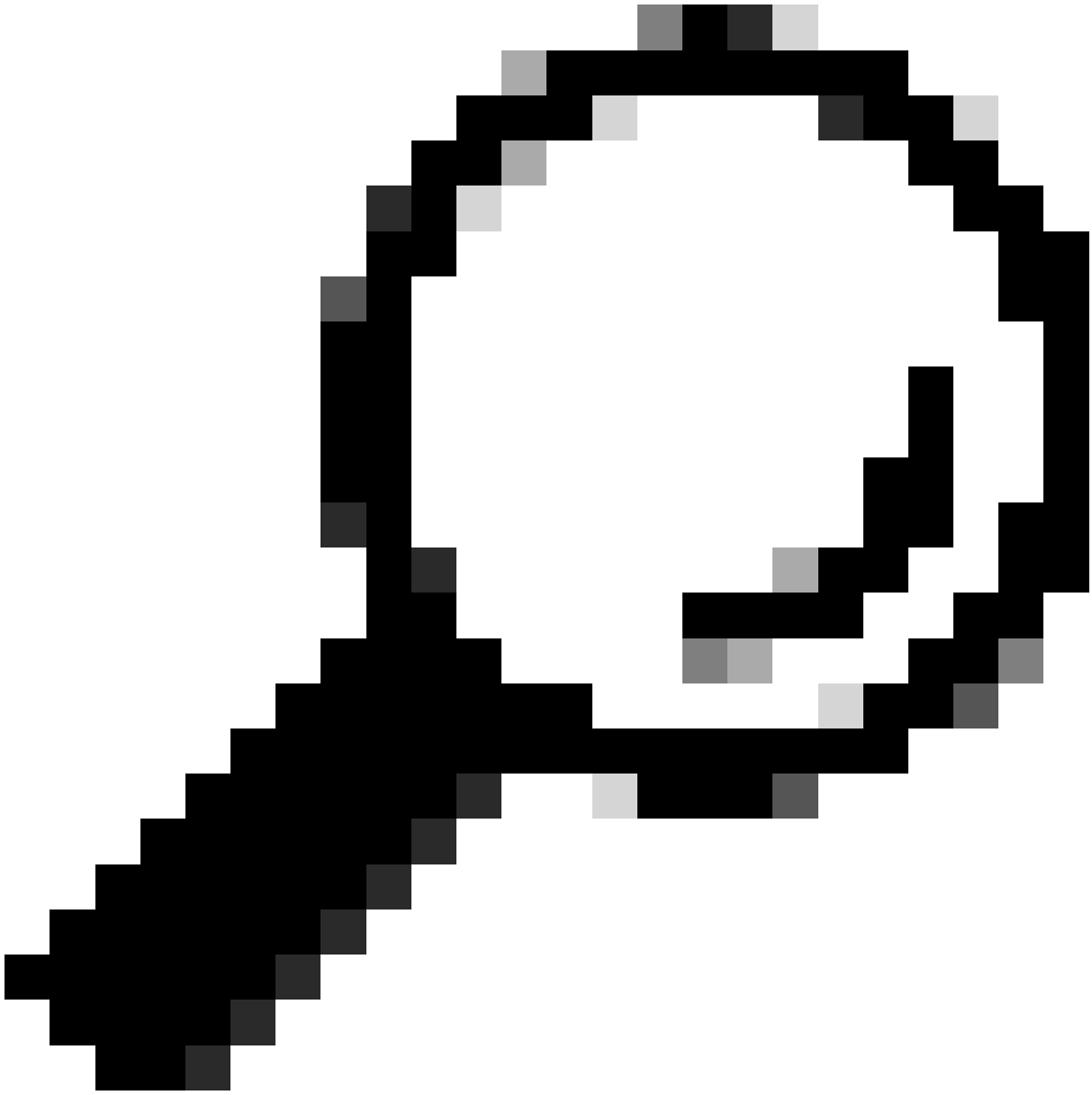
無線PCから有線PCに送信されるパケット。このキャプチャは無線PCで取得したものです。

無線PCはDSCP 46でUDPパケットを送信します。

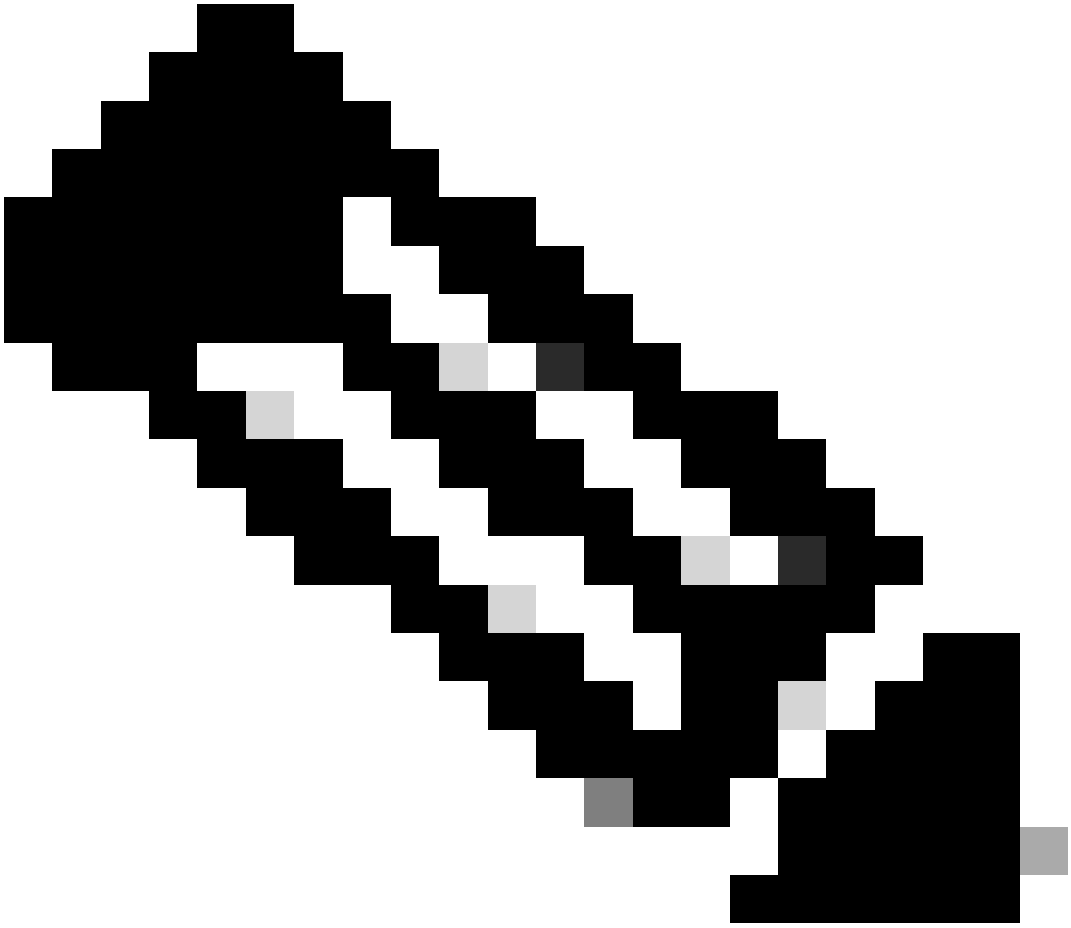


アップストリーム方向でのワイヤレスPCキャプチャ

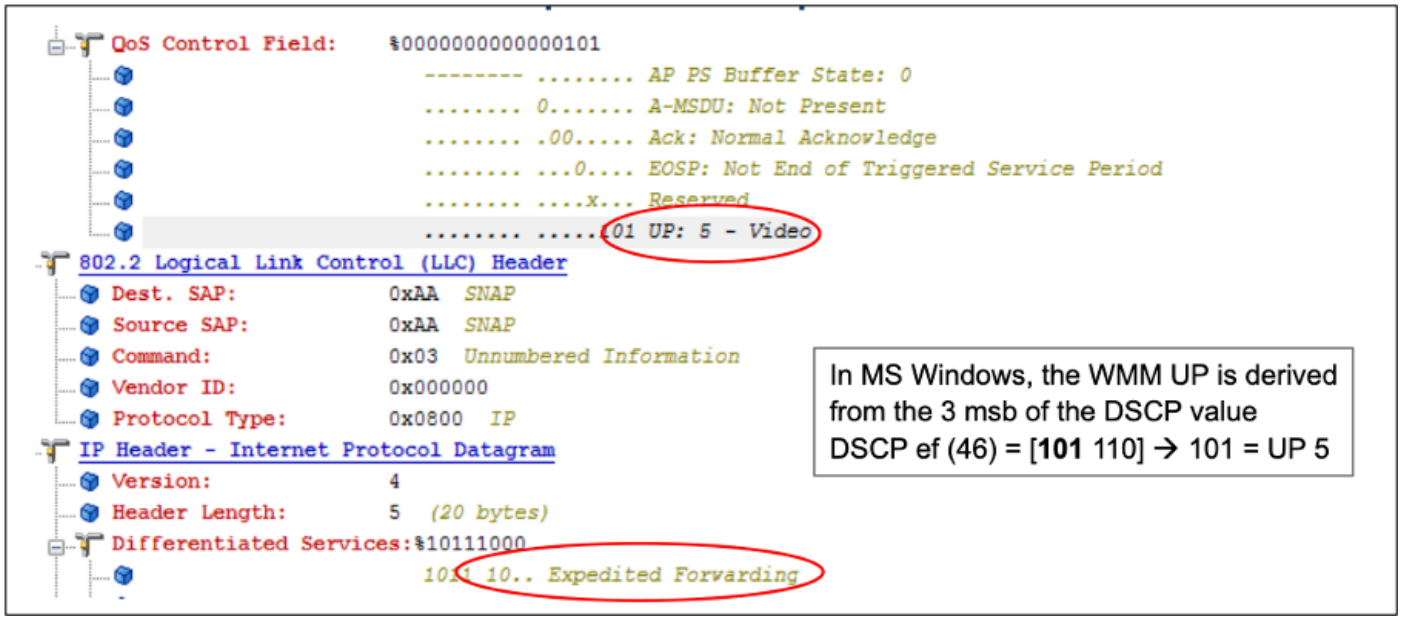
次に、クライアントからAPへのOTAキャプチャを見てみましょう。



ヒント: WindowsワイヤレスPCを使用してDSCP 46でパケットを送信する場合、WindowsはDSCP 46をユーザープライオリティ(UP)値5（ビデオ）にマップします。その結果、OTAキャプチャはパケットをビデオトラフィック(UP 5)として示します。ただし、パケットを復号化しても、DSCP値は46のままです。



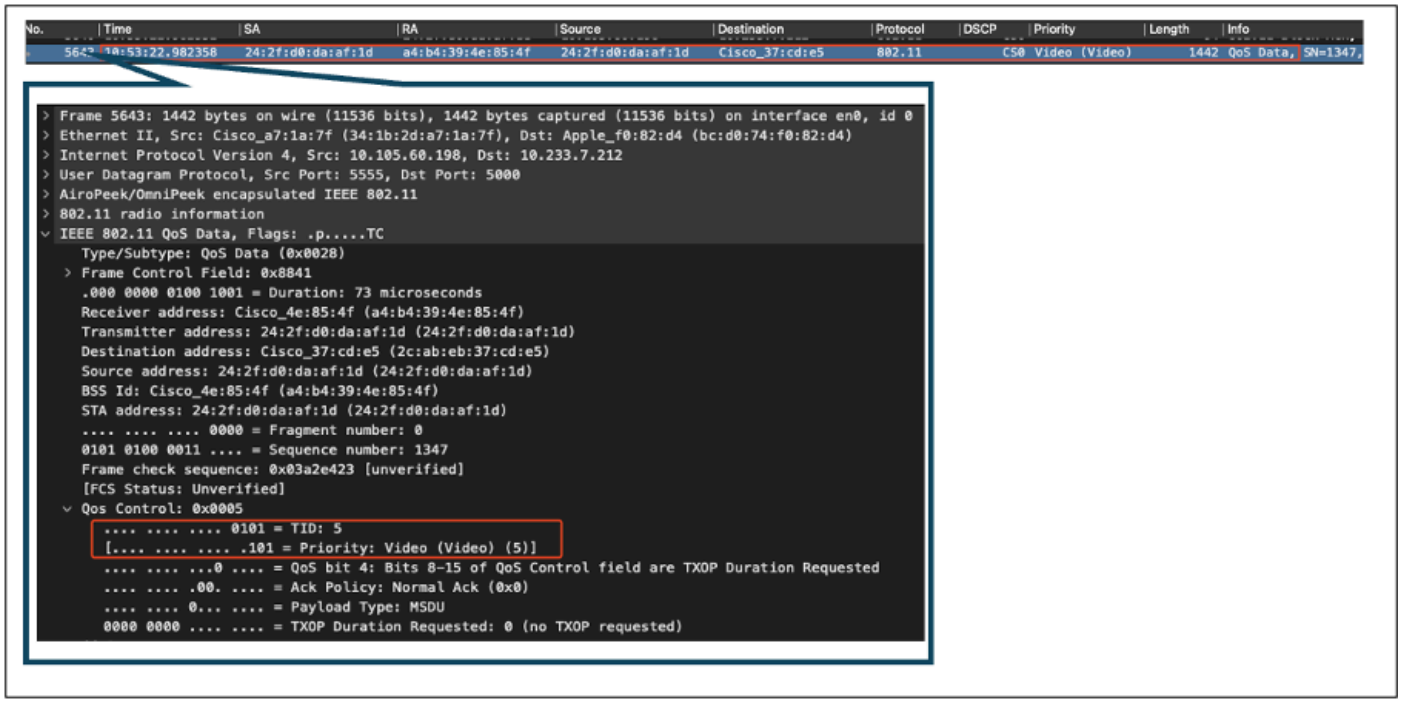
注：バージョン17.4以降のCisco 9800 WLCのデフォルト動作では、AP加入プロファイルのDSCP値を信頼します。これにより、DSCP値46がWLCによって保持および信頼され、WindowsのDSCPからUPへのマッピング動作に関連する問題が回避されます。



WindowsのUPからDSCPへのマッピング

ラボセットアップから取得した暗号化されたOver-the-Air(OTA)キャプチャが分析され、アップストリームQoS設定が検証されます。

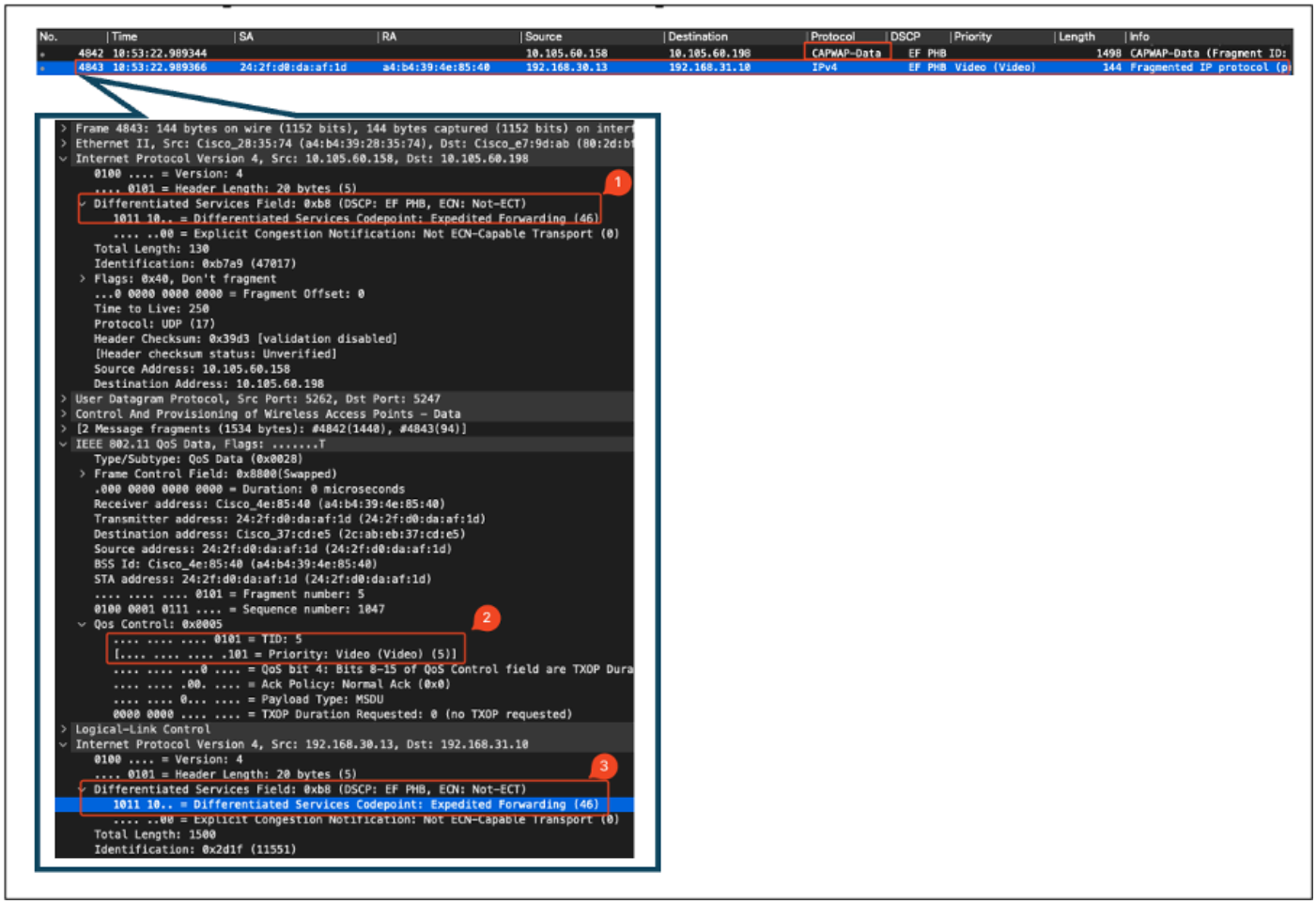
OTAキャプチャは、ユーザプライオリティ(UP)値が5（ビデオ）のパケットを示します。OTAキャプチャではUP 5と表示されていますが、暗号化パケット内のDSCP値は46のままです。



ラボでアップストリーム方向にOTAを設定

次に、APアップリンクポートでのパケットキャプチャが分析され、パケットがAPからWLCに移動する際にDSCP値が維持されることが確認されます。

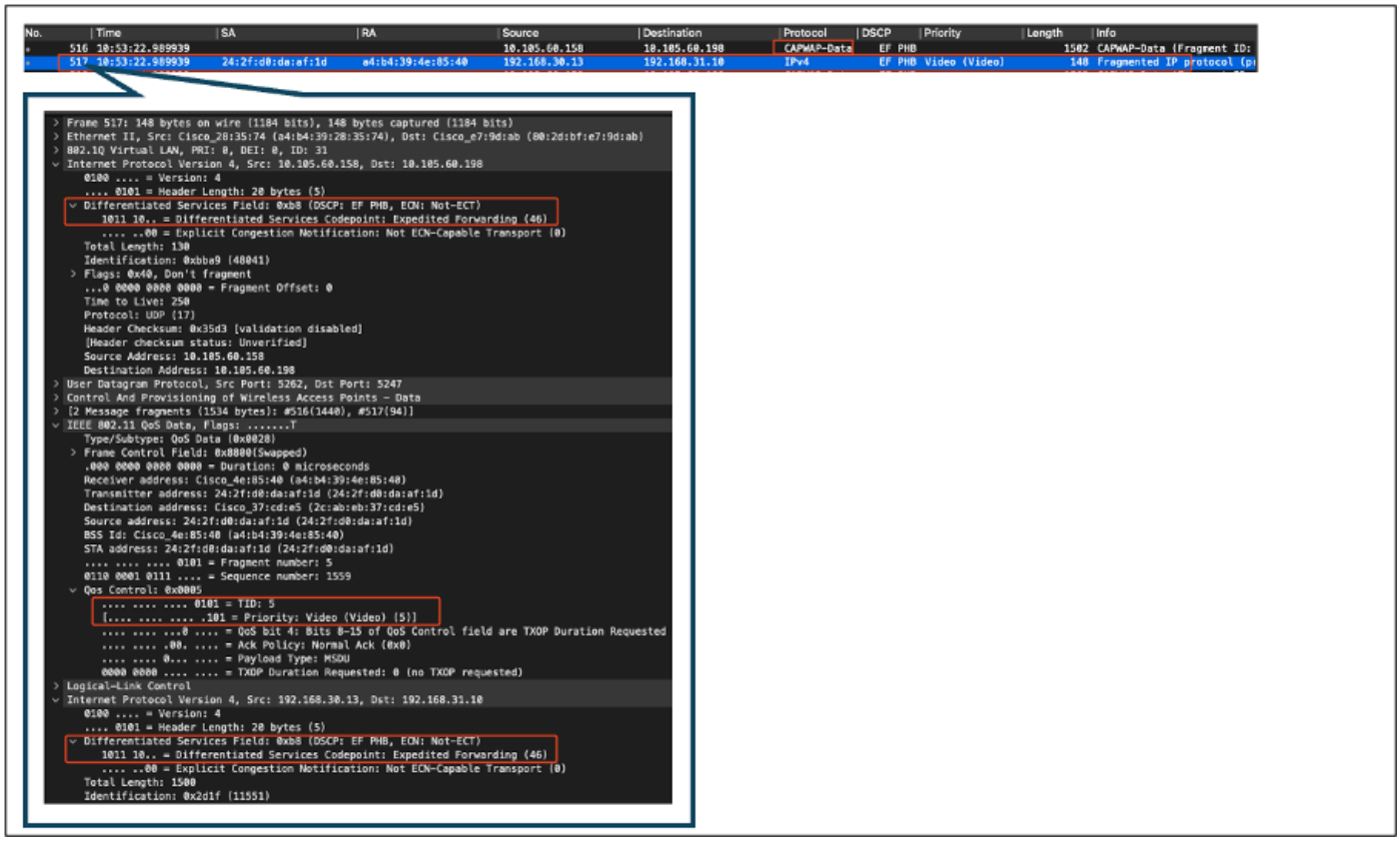
- 外部CAPWAPレイヤのDSCP値は46に維持される
- CAPWAPトンネル内では、DSCP値も46に維持されます。



アップストリーム方向のAPアップリンクキャプチャ

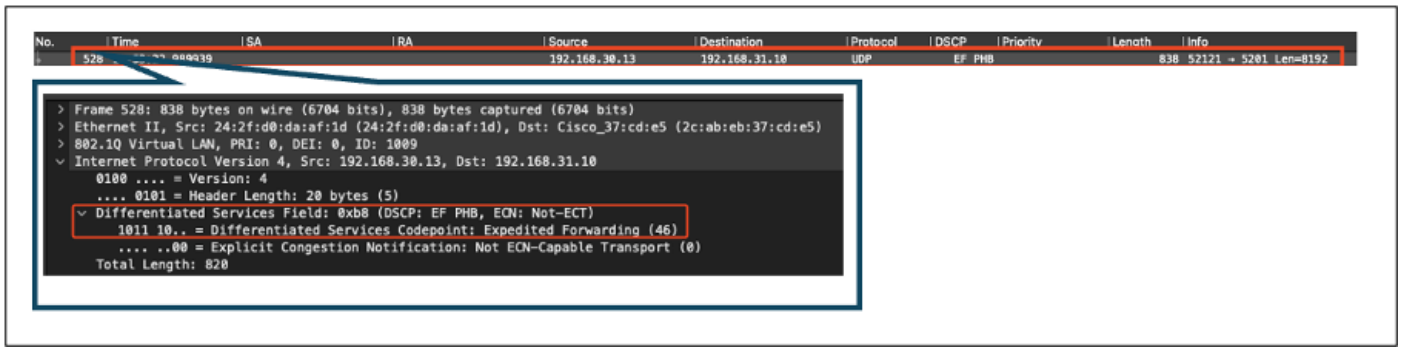
キャプチャは、パケットがスイッチから到着したときにWLCで取得されます。

- パケットは、外部CAPWAPレイヤのDSCP値46でWLCに到達します。
- CAPWAPトンネル内では、DSCP値は46に維持されます。



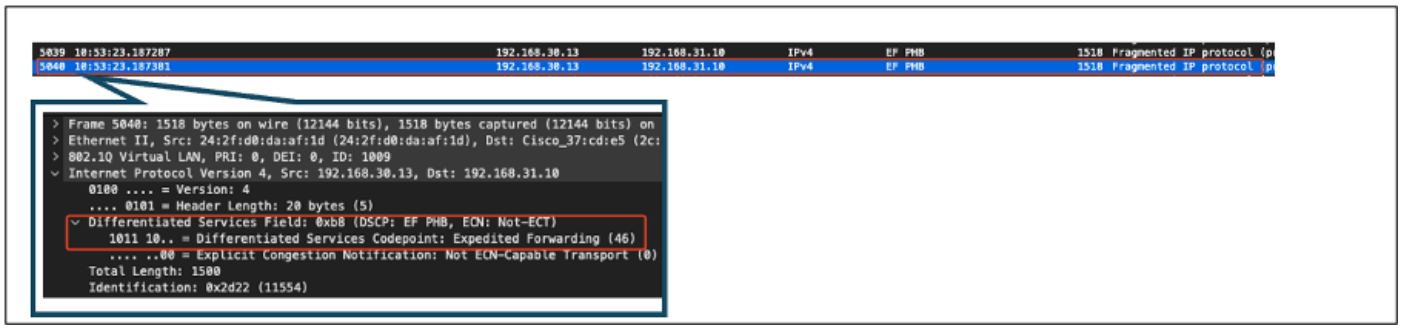
APからのパケットを示すWLC EPC

パケットがWLCでヘアピニングを行った後、有線PC宛てのアップリンクスイッチに戻されます。WLCは、DSCP値が46のパケットを転送します。



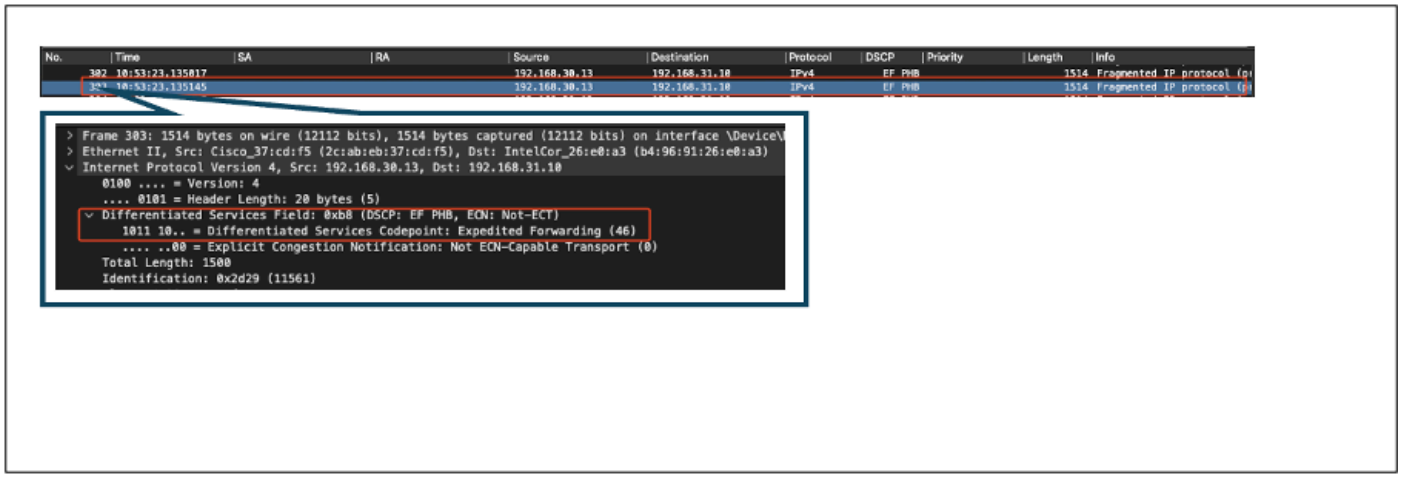
有線PCに送信されたパケットを示すWLC EPC

最後に、有線PCのアップリンクでのパケットキャプチャが分析され、パケットがWLCから到着する際にDSCP値が維持されます。



アップストリーム方向での有線PCアップリンクスイッチのキャプチャ

最終段階で、有線PCで受信されたパケットが分析され、DSCP値が46の有線PCにパケットが到達することが確認されます。



有線PCキャプチャ – アップストリーム方向

アップストリームQoSテストでは、無線PCから有線PCへのトラフィックフローのQoS設定が正常に検証されました。伝送パス全体を通じてDSCP値46を一貫して保持することで、QoSポリシーが正しく適用および適用されていることを確認できます。

トラブルシューティング

音声、ビデオ、およびその他のリアルタイムアプリケーションは、ネットワークパフォーマンスの問題に特に敏感です。また、Quality of Service(QoS)の低下は、著しく有害な影響を及ぼす可能性があります。QoSパケットが低いDSCP値で再マーキングされると、音声とビデオに大きな影響を与える可能性があります。

音声への影響：

- 遅延の増加：音声通信では、会話を自然で流動的なものにするために、低遅延が必要です。DSCP値が低いと、音声パケットの遅延が発生し、会話に著しい遅延が生じる可能性があります。
- ジッタ：パケット到着時間の変動（ジッタ）により、音声パケットの円滑な配信が中断される可能性があります。このため、音声が途切れたり不明瞭になったりして、話し手が聞き取りにくくなります。
- パケット損失：音声パケットはパケット損失の影響を非常に受けやすいです。わずかなパケット損失でも、単語や音節の欠落が生じ、通話品質の低下や誤解を招く可能性があります。
- エコーと歪み：遅延とジッタが増加すると、エコーと音声の歪みが発生し、音声コールの品質がさらに劣化する可能性があります。

ビデオへの影響：

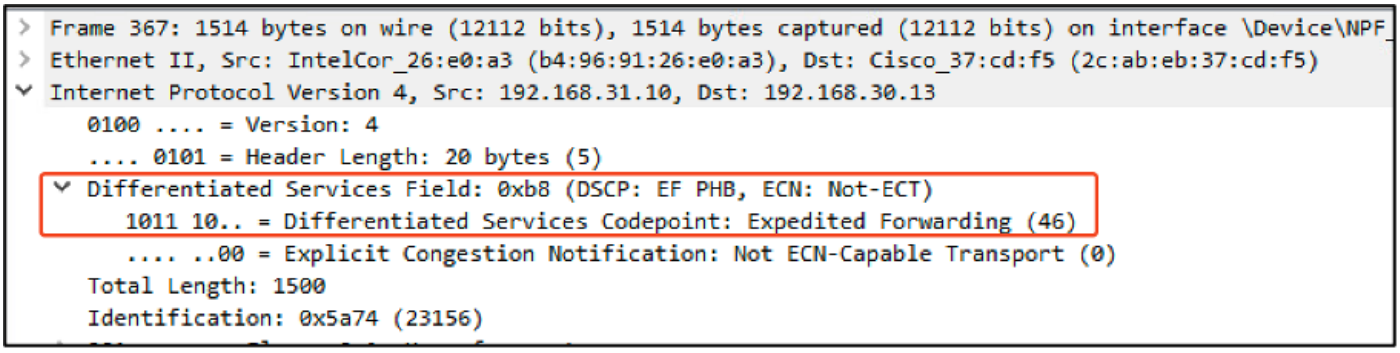
- 遅延の増加：ビデオ通信では、オーディオストリームとビデオストリーム間の同期を維持するために低遅延が必要です。遅延が増加すると遅延が発生し、リアルタイムの対話が困難になる可能性があります。
- ジッタ：ジッタが発生すると、ビデオフレームが順不同または不規則な間隔で到着し、ビデオが途切れたり途切れたりすることがあります。

- パケット損失：損失パケットはフレームの欠落を引き起こし、ビデオがフリーズしたり、アーティファクトが表示されたりする可能性があります。
- ビデオ品質の低下：DSCP値が低いと、ビデオストリームの帯域幅割り当てが減少し、解像度が低下してビデオ品質が低下する可能性があります。そのため、ビデオでは重要な詳細を確認することが困難になる可能性があります。

シナリオ1：中継スイッチによるDSCPマーキングの書き換え

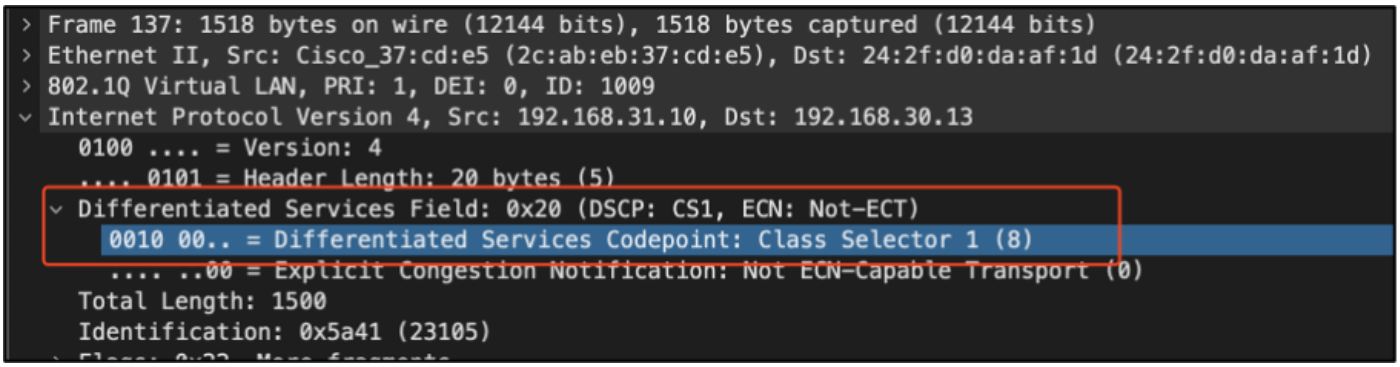
このトラブルシューティングシナリオでは、中間スイッチがWLCに到達したトラフィックのDSCPマーキングを書き換える影響を調査します。これを再現するために、スイッチは有線PCアップリンクインターフェイスのCS1にDSCP 46マーキングを書き換えるように設定されています。

パケットはDSCP 46タグ付きで有線PCから送信されます。



DSCP 46タグでパケットを送信する有線PC

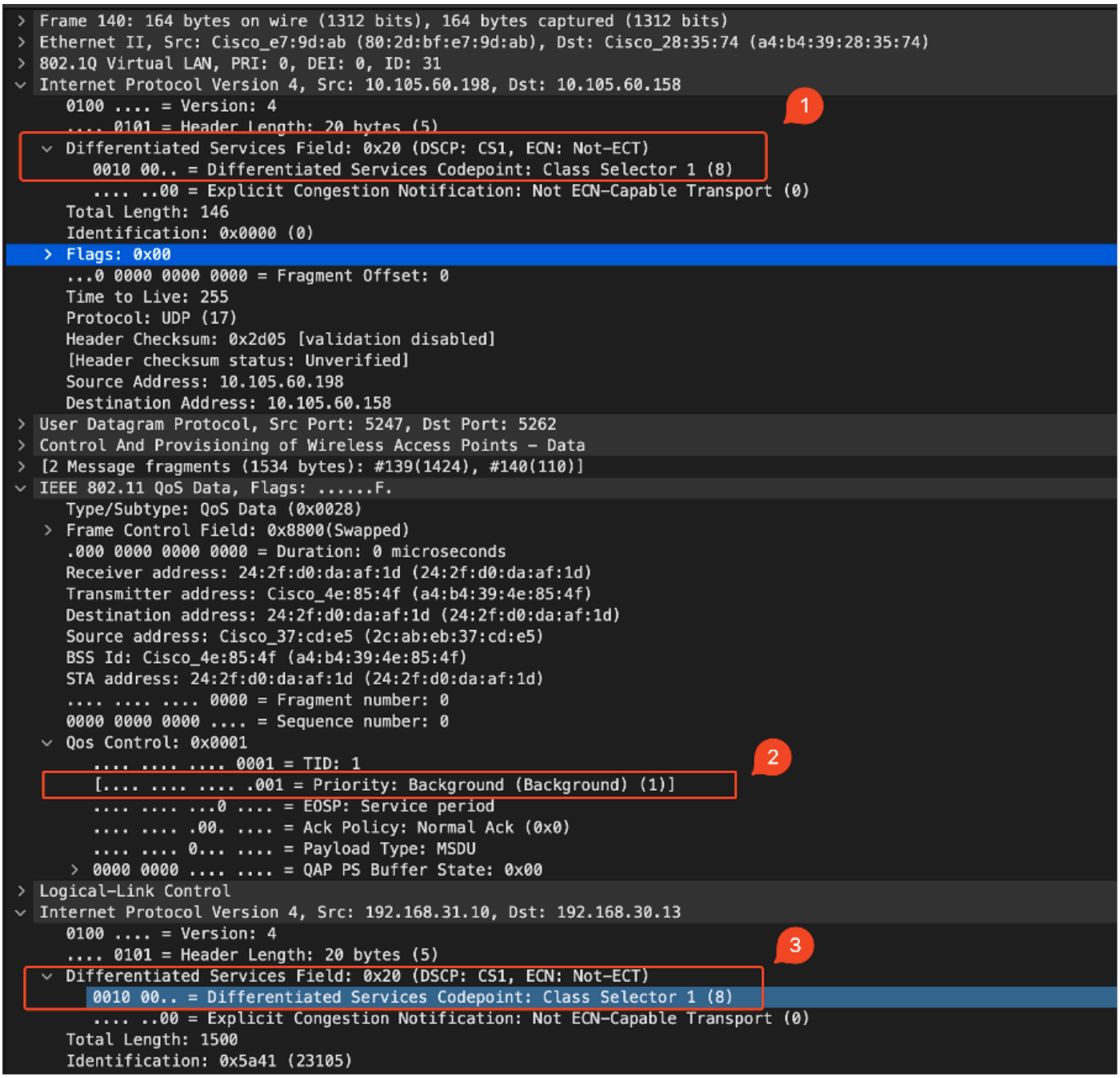
パケットは、DSCP値CS1(DSCP 8)でWLCに到達します。DSCP 46からDSCP 8への変更により、パケットの優先順位が大幅に下がります。



CS1マーキングを示すWLC EPC

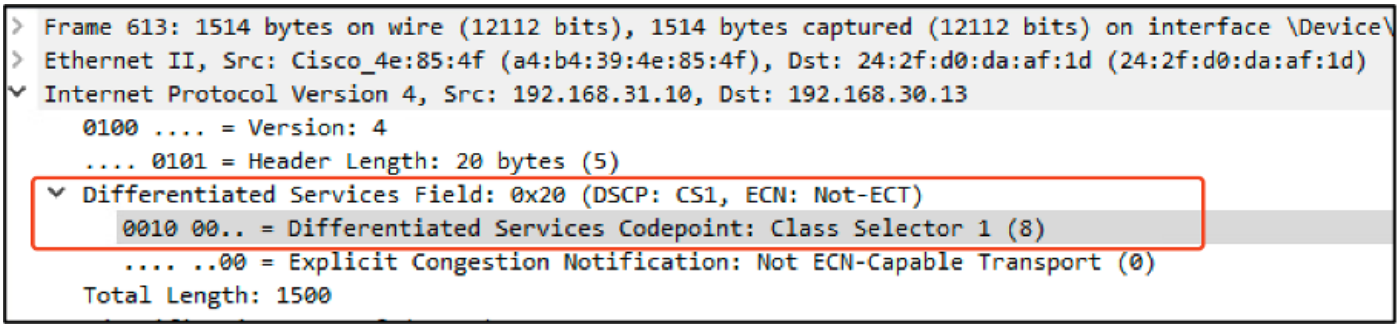
このステップでは、WLCからAPに転送されたパケットが分析されます。

- 外部CAPWAPヘッダーはCS1(DSCP 8)でタグ付けされます。
- 内側のCAPWAPヘッダーもCS1(DSCP 8)でタグ付けされています。
- User Priority (UP)の値はBK (Background)に設定されています。



CAPWAPトラフィックのCS1タグを示すWLC EPC

パケットは、DSCP値CS1(DSCP 8)でワイヤレスPCに到着します。



CS1マーキングを示すワイヤレスPCキャプチャ

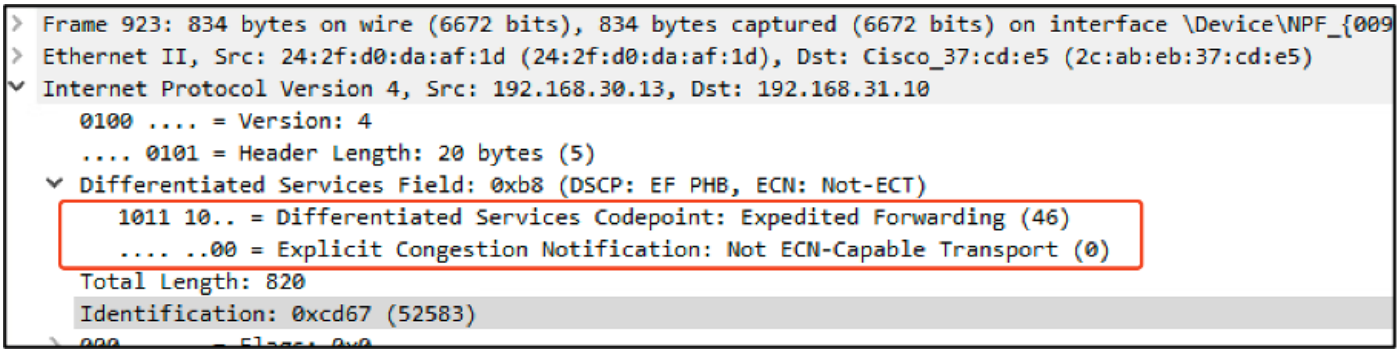
このシナリオでは、中継スイッチの設定ミスが原因でQoS設定が崩れ、優先度の高いトラフィッ

クのパフォーマンスが低下する状況について説明します。最初に高優先順位としてマークされた音声パケットは、DSCPの書き換えにより、優先順位の低いトラフィックとして扱われました。このシナリオでは、優先度の高いトラフィックに対して望ましいQuality of Service(QoS)を維持するために、中間ネットワークデバイスでQoSマーキングを正しく保持することが重要です。

シナリオ2:APリンクスイッチによるDSCPマーキングの書き換え

このシナリオでは、APに接続された中継スイッチがDSCPマーキングを書き換えることによるトラフィックへの影響を調査します。

- APに接続されているスイッチは、APアップリンクインターフェイスでDSCP 46マーキングを別の値CS1に書き換えるように設定されています。
- パケットは、DSCPタグ46で有線PCから送信されます。これにより、送信元でトラフィックがDSCP 46で正しくマーキングされていることを確認できます。

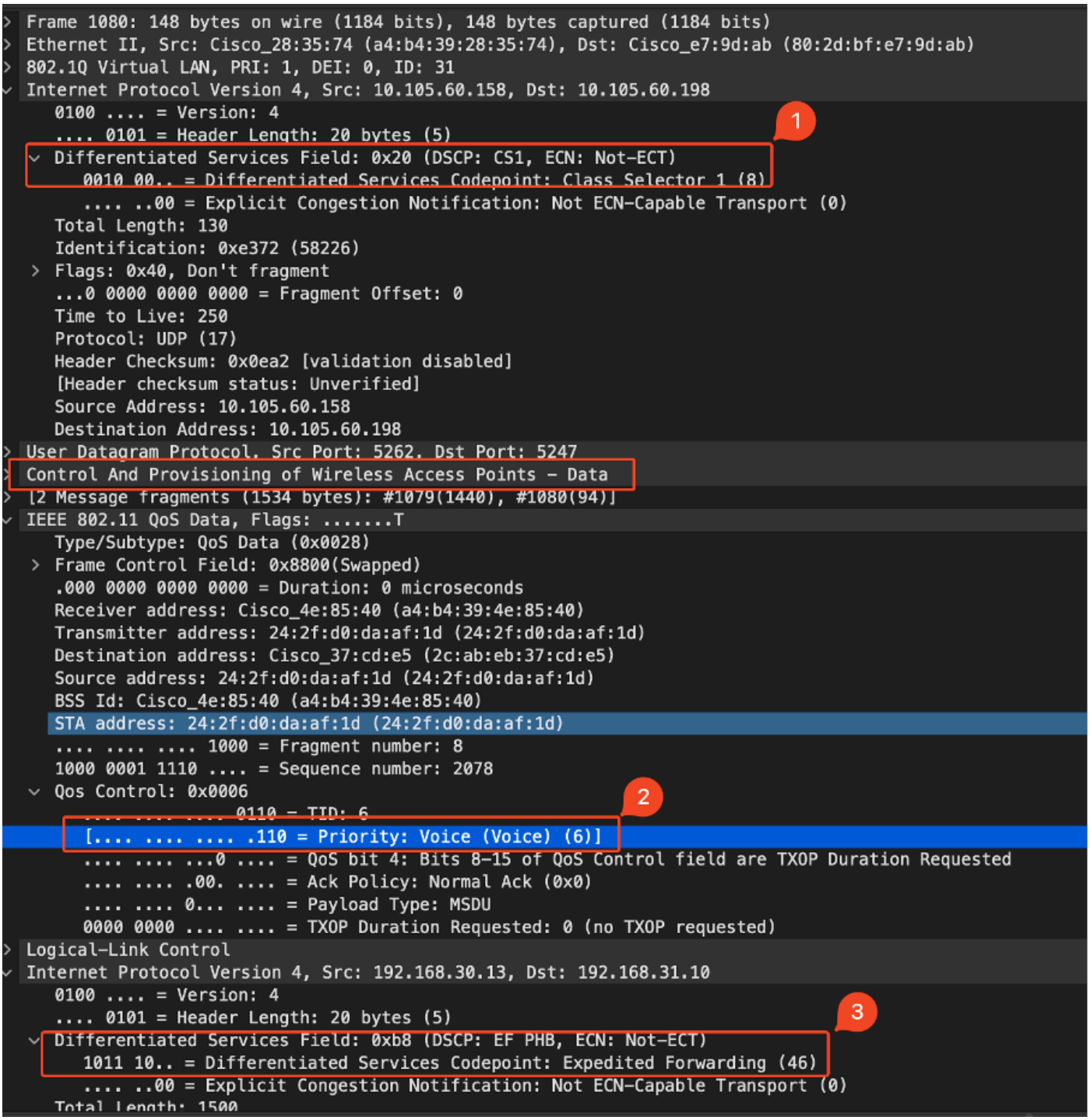


DSCP 46を示すワイヤレスPCキャプチャ

キャプチャは、パケットがスイッチから到着したときにWLCで取得されます。

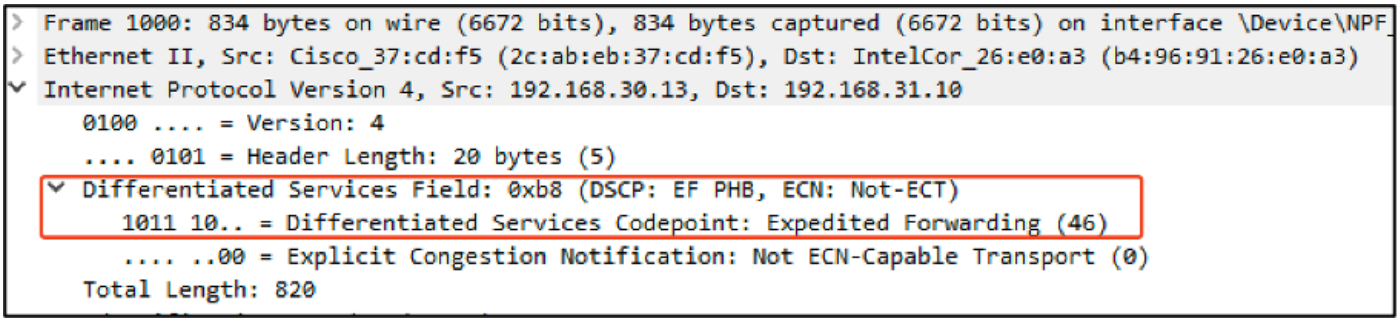
パケットは、外部CAPWAPヘッダーのDSCP値がCS1(DSCP値 と内部DSCP値が46)のWLCに到達します。これは、中継スイッチがCAPWAPトンネル内にカプセル化されたトラフィックを認識できないために発生します。

WLCはCAPWAPトンネル内のDSCPタグを信頼し、内部DSCPタグが46の有線PCにトラフィックを転送します。



CAPWAP DSCP値を示すWLC EPC

パケットは、DSCP値46で有線PCに到達します。WLCが元のDSCP値46でパケットを正しく転送し、優先度の高いマーキングを保持することを確認します。



WLCはDSCPタグ46でトラフィックを転送しましたが、外部DSCPタグがCS1(DSCP 8)に書き換えられているため、APからWLCへのトラフィックは低優先順位として扱われていることを理解することが重要です。

APとWLCの間に複数のスイッチが存在することがあり、トラフィックに低い優先順位が与えられている場合、トラフィックはWLCに遅れて到達することがあります。これにより、遅延、ジッタ、および潜在的なパケット損失が増加し、音声などの優先度の高いトラフィックのQuality of Service(QoS)が低下する可能性があります。

トラブルシューティングのヒント

1. 初期DSCPマーキングの確認：送信元（有線PCなど）でパケットをキャプチャし、目的のDSCP値でトラフィックが正しくマーキングされていることを確認します。
2. 中継装置の設定の確認：すべての中継スイッチとルータの設定を見直して、DSCP値が誤って書き換えられないことを確認します。
3. キーポイントでトラフィックをキャプチャ：
    1. 中間スイッチの前と後
    2. をWLCで実行します。
    3. 宛先（無線PCなど）。
4. トラフィックシナリオのシミュレーション：トラフィックジェネレータまたはネットワークシミュレーションツールを使用して、さまざまなタイプのトラフィックを作成し、ワイヤレスネットワークでQoSがどのように処理されるかを確認します。
5. 9800のベストプラクティスドキュメントを参照してください。QoSおよびDSCPマーキングの設定に関する9800のベストプラクティスドキュメントを確認してください。

設定の確認

<#root>

```
On the WLC, these commands can be used to verify the configuration.
# show run qos
# show policy-map <policy-map name>
# show class-map <policy-map name>
# show wireless profile policy detailed <policy-profile-name>

# show policy-map interface wireless ssid/client profile-name <name> radio type 2GHz|5GHz|6GHz ap name <

# show policy-map interface wireless client mac <MAC> input|output
# show wireless client mac <MAC> service-policy input|output

On AP, these commands can be used to check the QoS.
# show dot11 qos
# show controllers dot11Radio 1 | begin EDCA
```

結論

ネットワーク全体で一貫したQoS設定を維持することは、音声やビデオなどの優先度の高いトラフィックに適切なレベルのサービスとパフォーマンスを確実に提供するために不可欠です。すべてのネットワークデバイスが意図されたQoSポリシーに準拠していることを確認するために、QoS設定を定期的に検証することが不可欠です。この検証により、ネットワークパフォーマンスを低下させる可能性のある設定ミスや変更を特定して修正できます。

参考資料

- Cisco Catalyst 9800シリーズワイヤレスコントローラの説明とトラブルシューティング
- Cisco Catalyst 9800シリーズ設定のベストプラクティス
- Cisco Catalyst 9800シリーズワイヤレスコントローラソフトウェアコンフィギュレーションガイド、Cisco IOS® XE Dublin 17.12.x
- Voice Over Wireless LAN(VoWLAN)トラブルシューティングガイド
- WindowsマシンでのDSCP QoSタギングの有効化

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。