コンバージド アクセス制御上の QoS および Lightweight AP の設定例

内容

概要
前提条件
要件
使用するコンポーネント
背景説明
L3 QoS パケット マーキングの機能拡張
MQC による QoS のワイヤレス ネットワークの設定。
デフォルトのハードコード ポリシー
Platinum
ゴールド
シルバー
Bronze
手動設定
ステップ 1：音声トラフィックの特定とマーキング
ステップ 2：ポート レベルの帯域幅および優先度管理
ステップ 3：SSID レベルの帯域幅および優先度管理
ステップ 4：CAC によるコールの制限
確認
show class-map
show policy-map
show wlan
show policy-map interface
show platform qos policies
show wireless client mac-address <mac> service-policy
トラブルシュート

概要

このドキュメントでは、Lightweight アクセス ポイント（LAP）と、Cisco Catalyst 3850 スイッチまたは Cisco 5760 Wireless LAN controller（WLC）で、Cisco 統合アクセス ネットワークの QoS を設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- LAP および Cisco 統合アクセス コントローラの設定方法に関する基本的な知識
- 有線ネットワークでの基本的なルーティングおよび QoS の設定方法に関する知識

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。

- Cisco IOS?XEソフトウェアリリース3.2.2(SE)
- Cisco IOS XE ソフトウェア リリース 3.2.2(SE) が稼働する Cisco 5760 Wireless LAN Controller
- Cisco 3600 シリーズ Lightweight アクセス ポイント

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、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

QoS とは、一連のユーザまたはアプリケーションに、他のユーザまたはアプリケーションを犠牲にして、より良いサービスまたは特殊なサービスをネットワークが提供できる能力のことです。

QoS を使用すると、無線 LAN（WLAN）および WAN を含む各 LAN 上で、より効率的に帯域幅を管理できます。QoS は、次のサービスにより、拡張された信頼性の高いネットワーク サービスを提供します。

- 重要なユーザおよびアプリケーションを対象とした専用の帯域幅のサポート。
- リアルタイム トラフィックに必要なジッターと遅延の制御。
- ネットワークの輻輳の管理と最小化。
- ネットワーク トラフィックの調整によるトラフィック フローの平滑化。
- ネットワーク トラフィックの優先順位の設定。

WLAN は以前、低帯域幅のデータ アプリケーション トラフィックの転送に主に使用されていました。現在では、WLAN は、垂直環境（小売り、財務、教育など）およびエンタープライズ環境に拡張されているため、時間依存型のマルチメディア アプリケーションとともに高帯域幅のデータ アプリケーションを転送するために使用されています。この要件を満たすために、ワイヤレス QoS が必要になったのです。

IEEE 802.11 規格委員会の IEEE 802.11e のワーキング グループが規格の定義を完了し、Wi-Fi Alliance が Wi-Fi Multimedia（WMM）証明書を作成していますが、802.11e 規格の採用は、まだ限定的です。ほとんどのデバイスは WMM 認定されています。これは、802.11n および 802.11ac 認定には WMM 証明書が必要であるためです。 多くの無線デバイスは、データリンク層に送信されるパケットには、さまざまな QoS レベルを割り当てません。したがって、これらのデバイスでは、ほとんどのトラフィックが、QoS マーキングも相対的な優先順位付けも行われずに送信されます。ただし、ほとんどの 802.11 Voice over Wireless LAN（VoWLAN）IP Phone では、音声トラフィックをマーキングし、優先順位付けします。このドキュメントでは、VoWLAN IP Phone の QoS 設定と、音声トラフィックをマーキングするビデオ対応 Wi-Fi デバイスについて重点的に

説明します。

> **注：**内部マーキングを行わないデバイスの QoS 設定は、このドキュメントでの説明の範囲外です。

802.11e 修正では、8 つのユーザ プライオリティ（UP）レベルを定義しており、これらは、2 つずつ、次の 4 つの QoS レベル（アクセス カテゴリ）にグループ化されます。

- Platinum/音声（UP 7 および 6）：Voice Over Wireless 用の高品質サービスを保証します。
- Gold/ビデオ（UP 5 および 4）：高品質のビデオ アプリケーションをサポートします。
- Silver/ベスト エフォート（UP 3 および 0）：クライアント用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。
- Bronze/バックグラウンド（UP 2 および 1）：ゲスト サービス用の最小の帯域幅を提供します。

通常、Platinum は VoIP クライアントに、Gold はビデオ クライアントに使用されます。このドキュメントでは、コントローラでの QoS の設定方法と、VoWLAN およびビデオ クライアント用の QoS で設定された有線ネットワークとの通信方法を説明した設定例を示します。

L3 QoS パケット マーキングの機能拡張

Cisco 統合アクセス コントローラは、WLC と LAP によって送信されるパケットのレイヤ 3（L3）IP DiffServ コード ポイント（DSCP）マーキングをサポートします。この機能により、この L3 情報をアクセス ポイント（AP）が使用する方法が拡張されるため、パケットが確実に、AP からワイヤレス クライアントへの地上波（Over-the-Air）優先度を正確に設定されるようにします。

ワイヤレス コントローラとして Catalyst 3850 を使用する統合アクセス WLAN アーキテクチャでは、AP がスイッチに直接接続します。5760 コントローラを使用する統合アクセス WLAN アーキテクチャでは、WLAN データが Control and Provisioning of Wireless Access Points（CAPWAP）プロトコルによって、AP と WLC の間でトンネリングされます。このトンネル全体に渡って元の QoS 分類を維持するには、カプセル化されたデータ パケットの QoS 設定を、外側のトンネル パケットのレイヤ 2（L2）（802.1p）および L3（IP DSCP）フィールドに適切にマッピングする必要があります。

VoWLAN およびビデオ用の QoS を設定すると、ワイヤレス クライアント専用の QoS ポリシー、WLAN 専用のポリシー、またはその両方を設定できます。また、特に Catalyst 3850 スイッチに AP をリンクするポートに固有の設定でセットアップを補完することもできます。この設定例では、ワイヤレス クライアント、WLAN、および AP へのポートの QoS 設定に焦点を当てています。VoWLAN およびビデオ アプリケーション用の QoS 設定の主な目的は次のとおりです。

- アップストリームとダウンストリームの両方の音声およびビデオ トラフィックの認識（トラフィックの分類とマーキング）。
- 音声およびビデオ トラフィックに対する、音声の優先順位のマーキング： 音声には 802.11e UP 6、802.1p 5、DSCP 46。ビデオには 802.11e UP 5、DSCP 34。
- 音声トラフィック、音声シグナリング、およびビデオ トラフィックの帯域幅の割り当て。

MQC による QoS のワイヤレス ネットワークの設定。

QoS を設定する前に、Catalyst 3850 スイッチまたは Cisco 5760 WLC のワイヤレス コントロー

ラ モジュール（WCM）機能を基本動作用に設定し、WCM に LAP を登録する必要があります。このドキュメントでは、基本動作用に WCM が設定されており、WCM に LAP が登録されていることを前提としています。

統合アクセス ソリューションでは、モジュラ QoS（MQC）コマンドライン インターフェイス（CLI）を使用します。 Catalyst 3850 スイッチでの QoS 設定での MQC の使用の詳細については、「QoS 設定ガイド、Cisco IOS XE Release 3SE（Catalyst 3850 スイッチ）」を参照してください。

統合アクセス コントローラでの MQC による QoS 設定は、次の 4 要素に依存しています。

- **クラス マップは、対象トラフィックを認識するために使用されます。**クラス マップでは、対象トラフィックを識別するための、さまざまな方法（既存の QoS マーキング、アクセス リスト、VLAN など）を使用できます。
- **ポリシー マップは、どのような QoS 設定を対象トラフィックに適用するかを決定するために使用されます。**ポリシー マップは、クラス マップをコールし、さまざまな QoS 設定（固有のマーキング、プライオリティ レベル、帯域幅割り当てなど）を各クラスに適用します。
- **サービス ポリシーは、ネットワークの戦略的ポイントにポリシー マップを適用するために使用されます。**統合アクセス ソリューションでは、サービス ポリシーをユーザ、Service Set Identifier（SSID）、AP 無線、およびポートに適用できます。ポート、SSID、およびクライアントのポリシーは、ユーザが設定できます。無線ポリシーはワイヤレス制御モジュールによって制御されます。ポート、SSID、クライアント、および無線のワイヤレス QoS ポリシーは、トラフィックがスイッチまたはコントローラからワイヤレス クライアントに流れているときにダウンストリーム方向に適用されます。
- **テーブル マップは、着信 QoS を調べ、発信 QoS マーキングを決定するために使用されます**。テーブル マップでは、SSID に適用されるポリシー マップ内に配置されます。テーブル マップは、マーキングを保持（コピー）するか、変更するために使用できます。テーブル マップは、有線マーキングとワイヤレス マーキングとのマッピングを作成するために使用することもできます。有線マーキングは、DSCP（L3 QoS）または 802.1p（L2 QoS）を使用します。 ワイヤレス マーキングはユーザ プライオリティ（UP）を使用します。 テーブル マップは、対象の各 UP に使用する DSCP マーキングと、対象の各 DSCP 値に使用する UP を決定するために一般的に使用されます。DSCP 値と UP 値は直接変換されないため、テーブル マップは、統合アクセス QoS の基盤となります。

ただし、DSCP から UP へのテーブル マップでは、*コピー手順も実行できます*。この場合、統合アクセス ソリューションでは、Cisco Architecture for Voice, Video, and Integrated Data（AVVID）のマッピング テーブルを使用して、UP から DSCP へ、または DSCP から UP への変換を決定します。

ラベル インデックス	キー フィールド	着信値	外部 DSCP	CoS	UP
0	なし	オフ	0	0	0
1-10	DSCP	0 ~ 7	0 ~ 7	0	0
11-18	DSCP	8 ~ 15	8 ~ 15	1	0
19-26	DSCP	16 ~ 23	16 ~ 23	0	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	0
67	CoS	0	16	0	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	UP	0	0	0	0
74	UP	1	8	1	1
75	UP	0	16	1	0
76	UP	3	24	0	3
77	UP	4	34	3	4
78	UP	5	34	4	5
79	UP	6	46	5	6
80	UP	7	46	7	7

デフォルトのハードコード ポリシー

統合アクセス コントローラは、WLAN に適用できるハードコード QoS ポリシー プロファイルをロードします。これらのプロファイルは、Cisco Unified Wireless Networks（CUWN）コントローラの管理者によく知られている金属（Platinum、Gold など）のポリシーを適用します。音声トラフィックに特定の帯域幅を割り当てるポリシーを作成することではなく、単に音声トラフィックが適切な QoS マーキングを確実に受信するようにすることである場合は、ハードコード ポリシーを使用できます。ハードコード ポリシーは WLAN に適用できます。また、アップストリーム方向とダウンストリーム方向で異なるポリシーを適用できます。

> **注：**
>
> このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。
>
> アウトプット インタープリタ ツール（登録ユーザ専用）は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

Platinum

音声用のハードコード ポリシーは Platinum と呼ばれます。この名前は変更できません。

次に示すのは、Platinum QoS レベルのダウンストリームのポリシーです。

```
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
```
次に示すのは、Platinum QoS レベルのアップストリームのポリシーです。

```
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
```

ゴールド

ビデオ用のハードコード ポリシーは Gold と呼ばれます。この名前は変更できません。

次に示すのは、Gold QoS レベルのダウンストリームのポリシーです。

```
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
```
次に示すのは、Gold QoS レベルのアップストリームのポリシーです。

```
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
```

シルバー

ベスト エフォート用のハードコード ポリシーは Silver と呼ばれます。この名前は変更できません。

次に示すのは、Silver QoS レベルのダウンストリームのポリシーです。

```
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
```

次に示すのは、Silver QoS レベルのアップストリームのポリシーです。

```
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
```

Bronze

バックグラウンド トラフィック用のハードコード ポリシーは Bronze と呼ばれます。この名前は変更できません。

次に示すのは、Bronze QoS レベルのダウンストリームのポリシーです。

```
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
```

次に示すのは、Bronze QoS レベルのアップストリームのポリシーです。

```
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
```

どのテーブル マップが特定の SSID のターゲット トラフィックに最も一致するかを決定したら、一致するポリシーを WLAN に適用できます。この例では、1 つのポリシーがダウンストリーム方向（出力、AP からワイヤレス クライアントへ）に、1 つのポリシーがアップストリーム方向（入力、ワイヤレス クライアントから AP 経由でコントローラへ）に適用されています。

```
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#
```

WLAN 設定を確認して、どのポリシーが WLAN に適用されているかを確認してください。

```
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
```

手動設定

ハードコード ポリシーでは、デフォルトの QoS マーキングが適用されますが、帯域幅割り当ては適用されません。また、ハードコード ポリシーでは、トラフィックがすでにマーキングされていると想定しています。複雑な環境では、ポリシーの組み合わせを使用して、音声およびビデオ トラフィックを適切に認識したり、ダウンストリームおよびアップストリーム方向に帯域幅割り当てを設定したり、コール アドミッション制御を使用したりして、無線セルから開始されたコールの数を制限することが必要な場合があります。

> **注**：このセクションで使用されるコマンドの詳細については、Command Lookup Tool（登録ユーザ専用）を使用してください。

ステップ 1：音声トラフィックの特定とマーキング

最初のステップは、音声およびビデオ トラフィックを認識することです。音声トラフィックは 2 種類のカテゴリに分類できます。

- 通信の音声部分を伝送する音声フロー。
- 音声エンドポイント間で交換される統計情報を伝送する音声シグナリング。

音声フローは、通常、16384 ~ 32767の範囲のReal-time Transport Protocol(RTP)およびUser Datagram Protocol(UDP)宛先ポートを使用します。これは範囲です。実際のポートはより狭く、実装によって異なるのが普通です。

音声シグナリングのプロトコルは複数あります。この設定例では、Jabber を使用しています。Jabber では、接続とディレクトリに次の TCP ポートを使用します。

- TCP 80（HTTP）
- 143（Internet Message Access Protocol [IMAP]）
- 443（HTTPS）
- 会議用の Cisco Unified MeetingPlace または Cisco WebEx、およびボイスメール機能用の Cisco Unity または Cisco Unity Connection などのサービス用の 993（IMAP）
- TCP 389/636（連絡先の検索用の Lightweight Directory Access Protocol [LDAP] サーバ）
- FTP（1080）
- ピアまたはサーバからのファイルの転送（コンフィギュレーション ファイルなど）用の TFTP（UDP 69）

これらのサービスには、特定の優先順位付けが不要な場合もあります。

Jabber は、Session Initiation Protocol（SIP）（UDP/TCP 5060 および 5061）を使用して音声シグナリングを実行します。

ビデオ トラフィックは、実装によって異なるさまざまなポートおよびプロトコルを使用します。この設定例では、ビデオ会議に Tandberg PrecisionHD 720p カメラを使用します。Tandberg PrecisionHD 720p カメラは、複数のコーデックを使用できます。消費される帯域幅は、選択されたコーデックによって異なります。

- C20、C40、C60 の各コーデックは H.323/SIP を使用し、ポイントツーポイント接続で 6 Mbps まで消費する可能性があります。
- C90 コーデックは、これらの同じプロトコルを使用し、マルチサイト通信で 10 Mbps まで消費する可能性があります。

H.323 の Tandberg 実装では、通常、ストリーミング ビデオに UDP 970、ビデオ シグナリング

に UDP 971、ストリーミング音声に UDP 972、音声シグナリングに UDP 973 を使用します。Tandberg のカメラは、次のような他のポートも使用します。

- UDP 161
- UDP 962（簡易ネットワーク管理プロトコル [SNMP]）
- TCP 963（netlog）、TCP 964（FTP）
- TCP 965（Virtual Network Computing [VNC]）
- UDP 974（Session Announcement Protocol [SAP]）

これらの追加ポートには、特定の優先順位付けが不要な場合もあります。

トラフィックを識別する一般的な方法は、目的のトラフィックを対象とするクラス マップを作成することです。各クラス マップは、音声ポートとビデオ ポートを使用するあらゆるトラフィックを対象とするアクセス リストをポイントすることができます。

```
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
```

その後、トラフィックのタイプごとに 1 つのクラス マップを作成できます。各クラス マップは、関連するアクセス リストをポイントします。

```
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
```

音声トラフィックとビデオ トラフィックがクラス マップによって識別されたら、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てください。これは、テーブル マップを使用して WLAN レベルで実行できます。また、クライアントのポリシー マップでも実行できます。

テーブル マップは、着信トラフィックの QoS マーキングを調べ、必要な出力 QoS マーキングがどれかを判断します。したがって、テーブル マップは、着信トラフィックにすでに QoS マーキングがある場合に便利です。テーブル マップは、SSID レベルでのみ使用されます。

これに対して、ポリシー マップは、クラス マップで識別されるトラフィックを対象とすることができるため、タグなしの可能性のある目的のトラフィックに、より適応しています。この設定例では、Catalyst 3850 スイッチまたは Cisco 5760 WLC を入力する前に、有線側からのトラフィックがすでに正しくマーキングされていると想定しています。そうでない場合は、ポリシー マップを使用し、それを SSID レベルでクライアント ポリシーとして適用できます。ワイヤレス クライアントからのトラフィックがマーキングされていないことがあるため、音声トラフィックとビデオ トラフィックは正しくマーキングする必要があります。

- リアルタイム音声は、DSCP 46（緊急転送 [EF]）とマーキングする必要があります。
- ビデオは、DSCP 34（相対的優先転送クラス 41 [AF41]）とマーキングする必要があります。
- 音声とビデオのシグナリングは、DSCP 24（クラス セレクタ サービス値 3 [CS3]）とマーキングする必要があります。

これらのマーキングを適用するには、これらのクラスのそれぞれを呼び出し、同等のトラフィックをマーキングするポリシー マップを作成します。

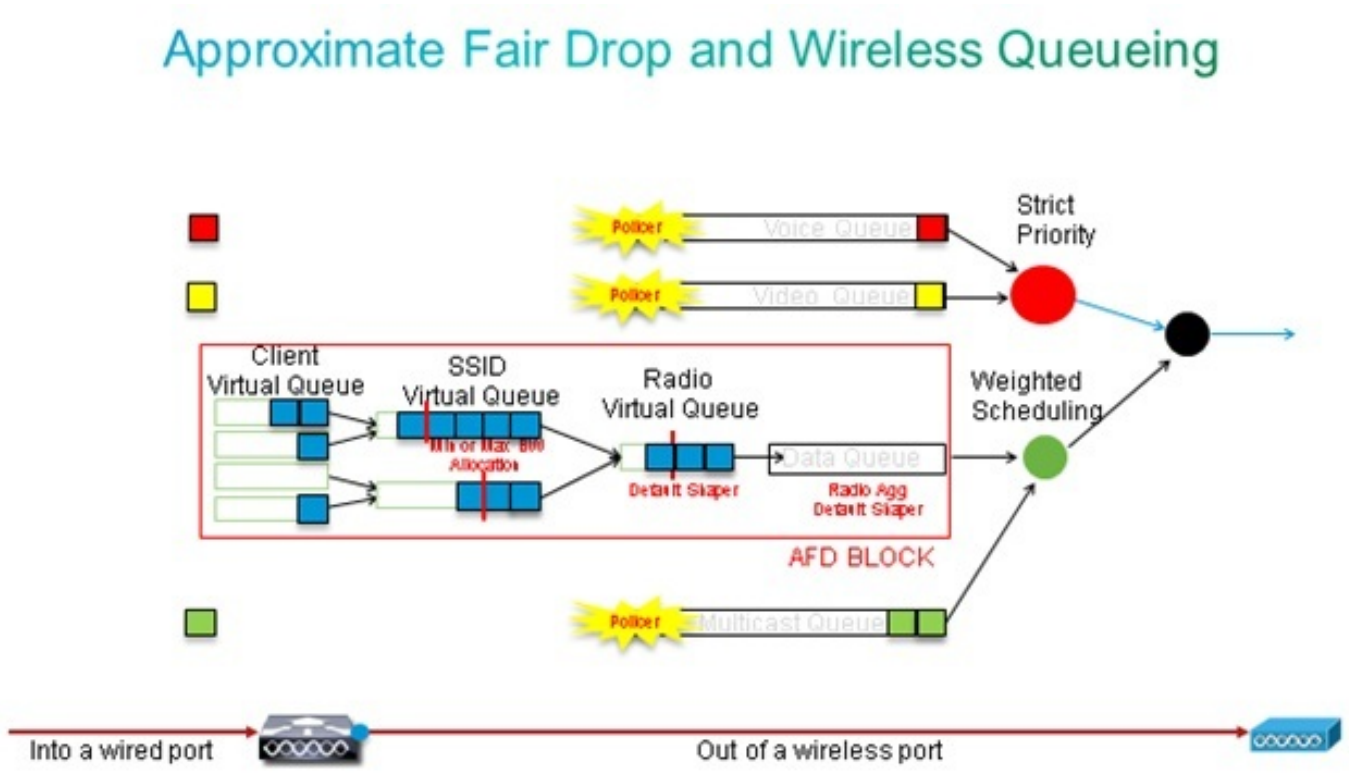
```
policy-map taggingPolicy
 class RTPaudio
 set dscp ef

 class H323realtimevideo
 set dscp af41

 class signaling
 set dscp cs3
```

ステップ 2：ポート レベルの帯域幅および優先度管理

次のステップでは、AP で発着信するポートの QoS ポリシーを決定します。このステップは、主に Catalyst 3850 スイッチに適用されます。設定を Cisco 5760 のコントローラで実行した場合は、この手順は必須ではありません。Catalyst 3850 のポートは、ワイヤレス クライアントと AP で発着信する音声トラフィックとビデオ トラフィックを伝送します。このコンテキストの QoS 設定は、次の 2 つの要件に一致します。

1. **帯域幅を割り当てる**。トラフィック タイプごとに割り当てる帯域幅の量を決定する必要がある場合があります。この帯域幅割り当ても、SSID レベルで実行できます。帯域幅の割り当てを設定して、ターゲット SSID を提供する各 AP で受信できる帯域幅の量を調整します。この帯域幅は、ターゲット AP のすべての SSID に対して設定する必要があります。この簡略化された設定例は、SSID と AP が 1 つずつのみであり、音声とビデオのポート帯域幅割り当てが、SSID レベルでの音声およびビデオのグローバル帯域幅割り当てと同じであることを前提としています。各トラフィックのタイプには 6 Mbps が割り当てられ、この割り当てられた帯域幅を超えないようにポリシングされます。

2. **トラフィックに優先順位を付ける**。ポートには 4 つのキューがあります。最初の 2 つのキューはリアルタイム トラフィック用に優先順位が付けられ、予約されており、通常はそれぞれ、音声とビデオです。4 番目のキューは、非リアルタイム マルチキャスト トラフィック用に予約されており、3 番目のキューに、その他のすべてのトラフィックが含まれます。統合アクセス キューイング ロジックによって、各クライアントのトラフィックは仮想キューに割り当てられ、ここで、QoS を設定できます。クライアント QoS ポリシーの結果は SSID 仮想キューに注入され、ここでも QoS を設定できます。特定の AP 無線に複数の SSID がある可能性があるため、AP 無線にある各 SSID の結果は、AP 無線の仮想キューに注入されます。ここで、無線容量に基づいてトラフィックが調整されます。トラフィックは、Approximate Fair Drop（AFD）と呼ばれる QoS メカニズムを使用して、これらのステージのいずれかで遅延させたり、ドロップしたりできます。 次に、このポリシーの結果が AP ポート（無線ポートと呼ばれます）に送信され、ここで、最初の 2 つのキュー（帯域幅の設定可能な量まで）に優先度が指定されます。その後、この段落ですでに説明したように、3 番目と 4 番目のキューに優先度が指定されます。



この設定例では、**priority level コマンドを使用して、最初の優先キューに音声が、2 番目の優先キューにビデオが入れられています。**残りのトラフィックには、残りのポート帯域幅が割り当てられます。

アクセス コントロール リスト（ACL）に基づいて対象トラフィックを決定するクラス マップは使用できないことに注意してください。 ポート レベルで適用されるポリシーは、クラス マップに基づいて対象トラフィックを決定できますが、これらのクラス マップは、QoS 値で識別されるトラフィックを対象にする必要があります。ACL に基づいてトラフィックを特定し、このトラフィックをクライアント SSID レベルで正しくマーキングしたら、同じトラフィックの 2 回目の詳しい検査をポート レベルで実行する必要はなくなります。トラフィックは、AP に向かうポートに到達したときは、すでに正しくマーキングされています。

この例では、SSID ポリシー用に作成された汎用クラス マップを再利用して、音声 RTP トラフィックとビデオ リアルタイム トラフィックを直接、対象にします。

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

対象トラフィックを特定したら、適用するポリシーを決定できます。デフォルト ポリシー（parent_port と呼ばれます）は、AP が検出されると、各ポートで自動的に適用されます。このデフォルトは、次のように設定されています。これは変更しないでください。

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

デフォルトの parent_port ポリシーは port_child_policy を呼び出すため、port_child_policy を編集するという方法もあります（名前は変更しないでください）。 この子ポリシーで、各キューに入る必要があるトラフィックはどれか、および割り当てる必要のある帯域幅の量が決定されます。

最初のキューが最も優先順位が高く、2 番目のキューが 2 番目に高い優先順位です。このように、優先順位はキーの順序どおりとなります。これらの 2 つのキューは、リアルタイム トラフィック用に予約されています。4 番目のキューは、非リアルタイム マルチキャスト トラフィックに使用されます。3 番目のキューには、その他すべてのトラフィックが含まれます。

次の例では、音声トラフィックを最初のキューに、ビデオ トラフィックを 2 番目のキューに割り当て、各キューと他のすべてのトラフィックに帯域幅を割り当てることにしています。

```
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
```

このポリシーでは、「voice」および「videoandsignaling」クラスに関連付けられた優先順位の記述により、そのトラフィックを、関連する優先キューに割り当てることができます。ただし、ポリシング レートのパーセンテージの記述は、ユニキャストではなく、マルチキャスト トラフィックにだけ適用されます。

このポリシーは、AP が検出された時点で自動的に適用されるため、ポート レベルで適用する必要はありません。

ステップ 3：SSID レベルの帯域幅および優先度管理

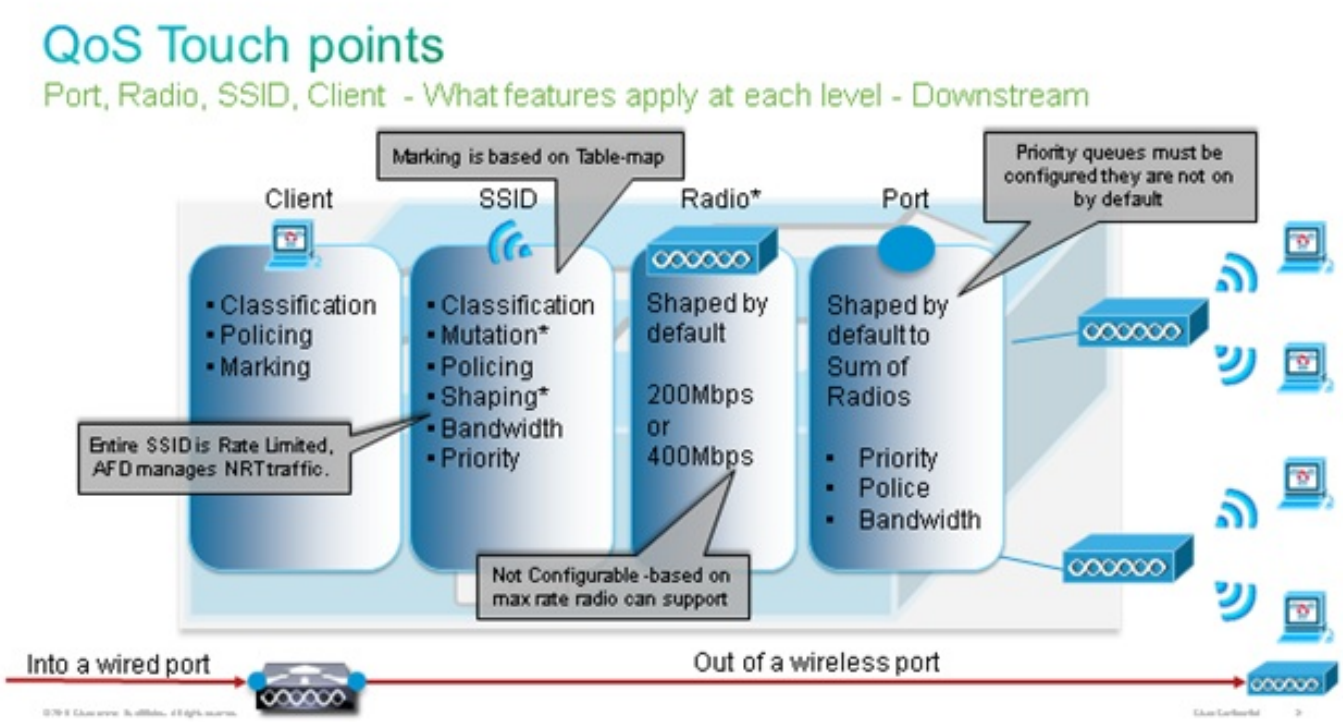
次のステップでは、SSID レベルで QoS ポリシーを処理します。このステップは、Catalyst 3850 スイッチと 5760 コントローラの両方に適用します。この設定では、音声トラフィックとビデオ トラフィックがクラス マップとアクセス リストの使用によって識別され、正しくタグ付けされていることを前提としています。ただし、アクセス リストの対象でない着信トラフィックには、QoS マーキングが表示されないものがあります。この場合は、このトラフィックをデフォルト値でマーキングするか、またはタグなしのままにするかをユーザが決定できます。すでにマーキングされているが、クラス マップの対象とされていないトラフィックも同様です。マーキングされていないトラフィックをマーキングなしのままにし、タグ付けされたトラフィックがタグを保持し、再マーキングされないようにするには、テーブル マップで *default copy 文を使用します。*

テーブル マップは、発信 DSCP 値を決定しますが、802.11 フレームを作成してフレーム UP 値を決定するためにも使用されます。

この例では、音声 QoS レベル（DSCP 46）を示す着信トラフィックは、その DSCP 値を保持し、値は、同等の 802.11 マーキング（UP 6）にマッピングされます。 ビデオ QoS レベル（DSCP 34）を示す着信トラフィックは、その DSCP 値を保持し、値は、同等の 802.11 マーキング（UP 5）にマッピングされます。 同様に、DSCP 24 とマーキングされたトラフィックは、音声シグナリングである可能性があります。DSCP 値は保持され、802.11 UP 3 に変換される必要があります。

```
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
```

マーキングは、着信有線ポート レベルでも実行できます。次の図は、有線から無線へのトラフィックの移行時に実行できる QoS アクションを示します。



この設定例では、QoS 設定の無線側に焦点をあて、ワイヤレス クライアント レベルでトラフィックをマーキングします。マーキングの部分が完了したら、帯域幅を割り当てる必要があります。ここでは、6 Mbps の帯域幅が、音声トラフィック フローに割り当てられます (帯域幅全体が音声に割り当てられますが、各コールの消費は減少し、128 kbps などになります) 。 この帯域幅は **police コマンドで割り当てられ、帯域幅が予約されて、超過分のトラフィックがドロップされます。**

ビデオ トラフィックにも、6 Mbps が割り当てられ、ポリシングされます。この設定例では、ビデオ フローが 1 つしかないと想定しています。

ビデオ トラフィックと音声トラフィックのシグナリング部分にも、帯域幅を割り当てる必要があります。考えられる戦略は 2 つあります。

- **shape average コマンドを使用すると、超過するトラフィックが許容され、バッファされて後で送信されます。**音声やビデオのフローには、一貫した遅延とジッターが必要であるため、このロジックは、これらのフロー自体には効率的ではありません。ただし、コール品質に影響を与えずに、シグナリングがわずかに遅延する場合があるため、シグナリングには効率的である可能性があります。統合アクセス ソリューションでは、shape コマンドで、「バケット設定」と呼ばれる設定は使用できません。これは、割り当てられた帯域幅を超えるトラフィックのうち、バッファできる量を決定する設定です。したがって、バケットサイズが0で

あることを指定するには、2番目のコマンドqueue-buffers ratio 0を追加する必要があります。残りのトラフィックにシグナリングを含め、shapeコマンドを使用すると、輻輳が発生した場合にシグナリングトラフィックが廃棄される場合があります。これにより、通信が行われていないと両端で判断されるため、コールがドロップされる場合があります。

- 優先キューの 1 つがにシグナリングを含めると、コールがドロップされるリスクを回避できます。この設定例では、以前に優先キューを音声とビデオとして定義したので、今度はビデオ キューにシグナリングを追加します。

ポリシーでは、音声フローにコール アドミッション制御（CAC）を使用します。CAC は無線トラフィックを対象とし、特定の UP（この設定例では、UP 6 および 7）と照合します。その後、CAC は、このトラフィックが使用する必要のある帯域幅の最大量を決定します。音声トラフィックをポリシングする設定では、CAC に、音声に割り当てられた帯域幅全体の量のサブセットを割り当てる必要があります。たとえば、音声が 6 Mbps にポリシングされる場合は、CAC が 6 Mbps を超えることはできません。CAC は、主要なダウンストリーム ポリシー マップ（親ポリシーと呼ばれます）に統合されているポリシー マップ（子ポリシーと呼ばれます）で設定されます。CAC は、**admit cac wmm-tspec コマンドで導入され、ターゲット UP と、ターゲット トラフィックに割り当てられる帯域幅が後に続きます。**

各コールで、音声に割り当てられた帯域幅をすべて消費するわけではありません。たとえば、各コールが各方向に 64 kbps を消費するため、有効な双方向帯域幅消費が 128 kbps となる場合があります。レートの指示で、各コールの帯域幅消費が決定され、police 文で、音声トラフィックに割り当てられる帯域幅全体が決定されます。セル内で発生するすべてのコールが、最大許容帯域幅に近い帯域幅を使用する場合、新しいコールがセル内から開始されても、音声に許可される最大帯域幅を超えることになると、拒否されます。このプロセスは、帯域レベルの CAC の設定により調整できます。これについては、「ステップ 4:CAC によるコールの制限」で説明しています。

したがって、CAC 手順を含み、主要なダウンストリーム ポリシーに統合されている子ポリシーを設定する必要があります。CAC は、アップストリーム ポリシー マップでは設定されません。CAC は、セルから開始された音声コールには適用されますが、これらのコールへの応答であるため、ダウンストリーム ポリシーマップにのみ設定されます。アップストリーム ポリシーマップは異なります。以前に作成したクラス マップは、対象トラフィックが ACL に基づいているため、使用できません。SSID ポリシーに注入されたトラフィックは、クライアントのポリシーですでに処理されているため、パケットの詳しい検査を実行する必要はありません。代わりに、クライアントのポリシーの結果である、QoS マーキングのあるトラフィックを対象とします。

デフォルト クラスにシグナリングを残さない場合は、シグナリングの優先順位付けも必要になります。

この例では、シグナリングとビデオは同じクラスにあり、シグナリング部分に対応するために、より大きな帯域幅が、そのクラスに割り当てられます。6 Mbps がビデオ トラフィック（1 つの Tandberg カメラのポイントツーポイント フロー）に割り当てられ、1 Mbps が、すべての音声コールおよびビデオ フローのシグナリングに割り当てられます。

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

ダウンストリームの子ポリシーは次のとおりです。

```
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
```

ダウンストリームの親ポリシーは次のとおりです。

```
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
```

アップストリーム トラフィックは、ワイヤレス クライアントから発信され、WCM に送信された後、有線ポートから送信されるか、別の SSID に送信されます。いずれの場合も、各タイプのトラフィックに割り当てる帯域幅を定義するポリシー マップを設定できます。ポリシーは、トラフィックが有線ポートから送信されるか、別の SSID に送信されるかによって異なります。

アップストリーム方向で最も重要となるのは、帯域幅ではなく、優先順位を決定することです。つまり、アップストリーム ポリシー マップでは、各トラフィックのタイプに帯域幅を割り当てません。トラフィックが AP にすでに存在しており、半二重無線領域で形成されるボトルネックをすでに通過しているため、目標は、次の処理のために、Catalyst 3850 スイッチまたは Cisco 5760 WLC のコントローラ機能へと、このトラフィックを導くことです。トラフィックが AP レベルで収集される場合は、コントローラに送信されるトラフィック フローの優先順位を付けるために、潜在的な既存の QoS マーキングを信頼する必要があるかどうかを決定できます。この例では、DSCP 値を信頼できます。

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

ポリシーが作成されたら、WLAN にポリシー マップを適用します。この例では、WLAN に接続するデバイスはすべて WMM をサポートすると想定されるため、WMM が必要です。

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

ステップ 4：CAC によるコールの制限

最後のステップは、特定の状況に合わせて CAC を調整することです。「ステップ 3:SSID レベルでの帯域幅と優先順位の管理」で説明した CAC 設定では、割り当てられた帯域幅を超える音声パケットは、AP によってすべてドロップされます。

帯域幅の最大値を回避するには、WCM を設定して、発信されたコールと、帯域幅を超えるコールが認識されるようにします。電話機には、WMM トラフィック仕様（TSPEC）をサポートしており、該当コールが消費すると予想される帯域幅をワイヤレス インフラストラクチャに通知する

ものもあります。この場合は、WCM が、発信される前にコールを拒否できます。

一部の SIP 電話機は TSPEC をサポートしていませんが、SIP ポートに送信されるコール開始パケットを認識するように WCM と AP を設定できます。また、この情報を使用して、SIP コールがまもなく発信される状態を確立できます。SIP 電話機では、コールによって消費される帯域幅が指定されないため、管理者は、コーデックやサンプリング期間などに基づいて、予想される帯域幅を決定する必要があります。

CAC は、各 AP レベルでの消費帯域幅を計算します。CAC は、その計算でクライアントの帯域幅消費だけを使用する（スタティック CAC）か、または、同じチャネルの隣接する AP およびデバイスも考慮する（負荷ベースの CAC）ように設定できます。 シスコでは、SIP 電話機にはスタティック CAC を、TSPEC 電話機には負荷ベース CAC を使用することを推奨します。

最後に、CAC は、帯域単位で動作することに注意してください。

この例では、セッション開始に TSPEC ではなく、SIP が電話機で使用され、各コールが各ストリーム方向に 64 kbps を使用し、負荷ベース CAC を無効にしてスタティック CAC を有効にしており、各 AP 帯域幅の最大値の 75% が音声トラフィックに割り当てられます。

```
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
```

2.4 GHz の帯域にも同じ設定を繰り返すことができます。

```
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
```

CAC が帯域ごとに適用されると、WLAN レベルでも SIP CAC を適用する必要があります。このプロセスにより、AP が、ワイヤレス クライアント トラフィックのレイヤ 4（L4）情報を検査し、UDP 5060 に送信されて SIP コール試行を示すクエリーを識別することができます。TSPEC は 802.11 レベルで動作し、AP によってネイティブで検出されます。SIP 電話機は TSPEC を使用しないため、AP は、SIP トラフィックを識別するために、より詳細なパケット検査を実行する必要があります。すべての SSID に AP がこの検査を実行することは望ましくないため、どの SSID で SIP トラフィックが想定されるかを判断する必要があります。その後、これらの SSID でコール スヌーピングを有効にして、音声コールを探すことができます。また、SIP コールを拒否する必要がある場合に実行するアクション（SIP クライアントの関連付けを解除するか、SIP 使用中のメッセージを送信する）も決定できます。

次の例では、コール スヌーピングが有効であり、SIP コールを拒否する必要がある場合は、使用中のメッセージが送信されます。これが、「ステップ 3:SSID レベルの帯域幅および優先度管理」からの QoS ポリシーを追加した、サンプル WLAN の SSID 設定です。

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

```
call-snoop
sip-cac send-486busy
```

確認

次のコマンドを使用して、QoS 設定が正しく機能することを確認します。

> **注：**
>
> このセクションで使用されるコマンドの詳細については、Command Lookup Tool (登録ユーザ専用) を使用してください。
>
> アウトプット インタープリタ ツール (登録ユーザ専用) は、特定の show コマンドをサポートしています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。

show class-map

このコマンドで、プラットフォームで設定されたクラス マップが表示されます。

```
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
```

show policy-map

このコマンドで、プラットフォームで設定されたポリシー マップが表示されます。

```
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
```

show wlan

このコマンドで、WLAN 設定およびサービス ポリシー パラメータが表示されます。

```
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 interface

このコマンドで、特定のインターフェイス用にインストールされたポリシー マップが表示されます。

```
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: 0x01023F4000000033.0x00C8384000000004.0x00DB568000000020

 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
```

show platform qos policies

このコマンドで、ポート、AP 無線、SSID、およびクライアント用にインストールされた QoS ポリシーが表示されます。無線ポリシーは、確認できますが、変更できないことに注意してください。

```
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_policyINSTALLED 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

このコマンドで、クライアント レベルで適用されたポリシー マップが表示されます。

```
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
```

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。