



Cisco Unified Wireless QoS

この章では、WLAN 実装に関連する QoS について説明します。ここでは WLAN QoS 全般について説明します。セキュリティやセグメンテーション、Voice over WLAN (VoWLAN) などのトピックにも QoS コンポーネントが含まれますが、これらのトピックについてはここでは詳しく取り上げません。

この章は、Cisco Unified Wireless テクノロジーを使用して企業の WLAN 展開の設計および実装に取り組んでいるユーザを対象としています。

QoS の概要

QoS とは、さまざまなネットワーク テクノロジーを介して、選択されたネットワーク トラフィックに差別化サービスを提供するネットワークの機能のことです。QoS テクノロジーには次のような利点があります。

- キャンパス、WAN、およびサービス プロバイダー ネットワークで使用されるビジネス マルチメディアおよび音声アプリケーションに構成要素を提供します。
- ネットワーク管理者がネットワーク ユーザとのサービス レベル契約 (SLA) を制定できます。
- ネットワーク リソースをさらに効率的に共有できるようにし、ミッションクリティカルなアプリケーションの処理を効率化します。
- 時間依存型マルチメディアおよび音声アプリケーションのトラフィックを管理し、このトラフィックがベストエフォート型のデータ トラフィックよりも優先度が高く、帯域幅が大きく、かつ遅延が少なくなるようにします。

QoS を使用して、WLAN および WAN などの LAN 全体で帯域幅をより効率的に管理できます。QoS により、次の点で拡張された信頼性のあるネットワーク サービスが提供されます。

- 重要なユーザおよびアプリケーションに対する専用の帯域幅のサポート
- ジッターおよび遅延の制御 (リアルタイムのトラフィックで必要)
- ネットワーク 輻輳の管理および最小化
- トラフィック フローを円滑化するネットワーク トラフィックのシェーピング
- ネットワーク トラフィックの優先度の設定

無線 QoS の展開方式

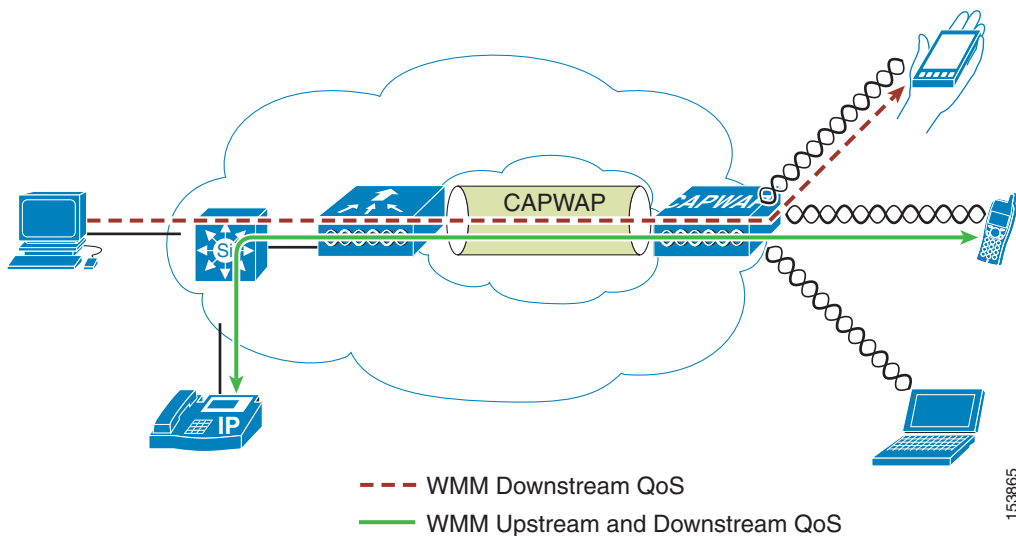
従来、WLAN は主に低帯域幅のデータ アプリケーション トラフィックの伝達に使用されていました。現在では、WLAN は縦方向の環境（小売、金融、教育など）および企業環境に拡張され、時間依存型のマルチメディア アプリケーションと共に高帯域幅のデータ アプリケーションの伝達に使用されています。この要件に対応するために、無線 QoS が必要になりました。

シスコを含む複数のベンダーでは、音声アプリケーション対応の専用無線 QoS 方式をサポートしています。QoS の導入速度を高め、複数のベンダーの時間依存型アプリケーションに対応するには、無線 QoS に対する統一手法が必要です。IEEE 802.11 標準化委員会内の IEEE 802.11e グループにより、標準の定義は完了しています。しかし、802.11e 規格の採択は初期段階にあり、多くの標準と同じく、多数の任意の選択要素があります。802.11i の 802.11 セキュリティ規格の際と同様、Wi-Fi Alliance などの業界グループおよびシスコのような業界トップのメーカーは、認証プログラムを使用して主要な機能や互換性を確実に備えられるよう、WMM プログラムおよび Cisco Compatible Extensions プログラムを介して WLAN QoS の主要な要件を定義しています。

Cisco Unified Wireless 製品は、Wi-Fi Alliance が公開した IEEE 802.11e に基づく QoS システムである Wi-Fi MultiMedia (WMM)、WMM Power Save、および WMM Admission Control をサポートしています。

図 5-1 では、Cisco Unified Wireless テクノロジーの機能に基づく Wireless QoS の展開例を示します。

図 5-1 QoS の展開例



QoS パラメータ

QoS は、通信の質およびサービスの可用性を反映した通信システムのパフォーマンスの基準として定義されています。サービスの可用性は QoS の重要な要素です。QoS を正しく実装するには、ネットワーク インフラストラクチャの可用性が高くなければなりません。

ネットワークの通信の質は、遅延、ジッター、および損失で決まります（表 5-1 を参照）。

表 5-1 QoS の送信の質

要素	説明
遅延	遅延とは、パケットが送信エンドポイントから伝送されて受信エンドポイントへ到達するまでにかかる時間を意味します。この時間をエンドツーエンド遅延といい、次の 2 つの領域に分けることができます。 <ul style="list-style-type: none"> 固定ネットワーク遅延：符号化および復号の時間（音声およびビデオ）、および電気パルスまたは光パルスがメディアを通過して送信先へ届くまでの限られた時間が含まれます。 可変ネットワーク遅延：通常、伝送に必要な時間全体に影響を及ぼす可能性のあるキューイングや輻輳などのネットワークの状態を意味します。
ジッター	ジッター（遅延差異）は、パケット間のエンドツーエンド遅延の差です。たとえば、あるパケットが発信エンドポイントから送信先エンドポイントまでネットワークを通過するのに 100 ミリ秒かかり、次のパケットでは同じ伝送に 125 ミリ秒かかる場合、ジッターは 25 ミリ秒となります。
損失	損失（パケットの損失）は、伝送された総数が正常に送受信された場合のパケットの比較基準です。損失はドロップされたパケットの割合として表されます。

無線アップストリームおよびダウンストリーム QoS

図 5-2 では、無線アップストリームおよび無線ダウンストリーム QoS の定義を示します。

図 5-2 アップストリームおよびダウンストリーム QoS

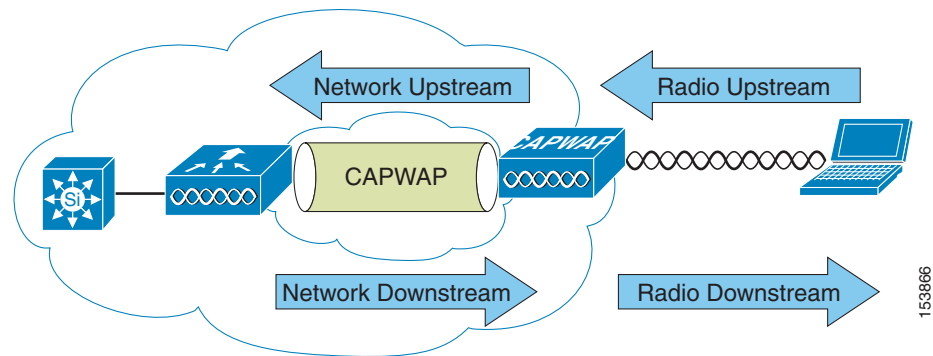


図 5-2 は、以下のことについて示しています。

- 無線ダウンストリーム QoS：AP から発信され、WLAN クライアントまで伝送されるトラフィック。無線ダウンストリーム QoS が今でも最も一般的な展開であるため、この章の最重要点となっています。クライアントの無線アップストリーム QoS は、クライアントの実装によって異なります。
- 無線アップストリーム QoS：WLAN クライアントから発信され、AP まで伝送されるトラフィック。WMM では、WMM をサポートする WLAN クライアントのアップストリーム QoS が提供されます。

- ネットワーク ダウンストリーム：ワイヤレス LAN コントローラ (WLC) から発信され、AP まで伝送されるトラフィック。この時点で QoS を適用することで、AP へのトラフィックの優先順位付けとレート制限を行うことができます。



(注) イーサネットのダウンストリーム QoS の設定は、本書では取り上げません。

- ネットワーク アップストリーム：AP から発信され、WLC まで伝送されるトラフィック。AP は、その AP のトラフィック分類ルールに従って、AP からアップストリーム ネットワークまでのトラフィックを分類します。

QoS およびネットワークのパフォーマンス

QoS 機能の適用は、負荷の軽いネットワークでは簡単に検出されないことがあります。メディアの負荷が軽いときに遅延、ジッター、および損失が顕著な場合、それはシステム障害やネットワーク設計の不備、またはアプリケーションの遅延、ジッター、および損失の要件がネットワークと適合していないことを示しています。ネットワークの負荷が増大するにつれて、QoS 機能がアプリケーションのパフォーマンスに作用し始めます。QoS は、選択されたトラフィック タイプの遅延、ジッター、および損失を、妥当な範囲内に維持しようとし、AP から無線ダウンストリーム QoS のみが提供される場合、無線アップストリームのクライアント トラフィックはベストエフォートと認識されます。クライアントは、アップストリーム伝送に対しても、また AP からのベストエフォート伝送に対しても、他のクライアントと競合します。特定の負荷状況下では、クライアントにアップストリームの輻輳が発生し、AP で QoS 機能を適用しても、QoS 依存型アプリケーションのパフォーマンスが許容できないほど低下することがあります。理想的には、アップストリームおよびダウンストリーム QoS を操作するためには AP と WLAN クライアントの両方で WMM を使用するか、WMM およびクライアントの独自の実装を使用します。



(注) WLAN クライアントにおける WMM のサポートは、クライアント トラフィックが WMM から自動的に利益を得ているという意味ではありません。WMM の利点を求めるアプリケーションが適切な優先度の分類をそのトラフィックに割り当て、オペレーティング システムはその分類を WLAN インターフェイスに渡す必要があります。VoWLAN 端末などの専用デバイスでは、設計の一部としてこの機能があります。ただし、PC のような汎用的なプラットフォームに実装する場合は、アプリケーションのトラフィック分類と OS によるサポートがないと、WMM 機能の効果が望めません。

WLAN クライアント上で WMM のサポートがなくても、Cisco Unified Wireless ソリューションはネットワークのアップストリームとダウンストリームの両方でネットワークの優先順位を付けることができます。

802.11 Distributed Coordination Function

802.11 のデータ フレームは、Distributed Coordination Function (DCF) を使用して送信されます。DCF は次の 2 つの主要コンポーネントで構成されています。

- フレーム間スペース (SIFS、PIFS、DIFS などを含む IFS。詳細は後述)
- ランダム バックオフ (コンテンション ウィンドウ)。

DCF を 802.11 ネットワークで使用して RF メディアへのアクセスを管理します。802.11e ベースの拡張型分散チャネル アクセス (EDCA) を展開するには、DCF の基本的な理解が必要です。DCF の詳細は、次の Web ページで IEEE 802.11 の仕様を参照してください。

<http://www.ieee802.org/11/>

これらの 802.11 DCF コンポーネントについては、以降のセクションで詳しく説明します。

フレーム間スペース

802.11 標準は、フレーム間スペース (IFS) を次のように定義します。

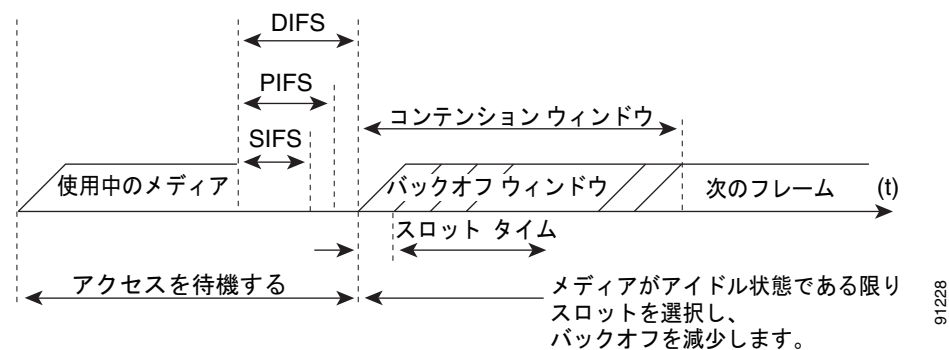
- 短いフレーム間スペース (SIFS) : 10 μ s
- PCF のフレーム間スペース (PIFS) : SIFS + 1 x スロット タイム = 30 μ s
- DCF のフレーム間スペース (DIFS) : 50 μ s SIFS + 2 x スロット タイム = 50 μ s



(注) 図 5-3 で示した IFS の例で使用しているベース タイミングは、802.11b に対するものです。802.11g と 802.11a のタイミングは異なりますが、適用する原則は同じです。

IFS では、キャリア検知でチャネルの空きが示された後に、最初にチャネルにアクセスするトラフィックを 802.11 で制御できます。通常、802.11 の管理フレームとコンテンションを起こさないフレーム (フレーム シーケンスの一部であるフレーム) では SIFS が使用され、データ フレームでは DIFS が使用されます (図 5-3 を参照)。

図 5-3 フレーム間スペース



ランダム バックオフ

DCF のデータ フレームが送信可能になると、DCF は次の手順で処理を行います。

1. 0 から最小コンテンション ウィンドウまでの範囲のランダム バックオフ番号を生成します (「aCWmin、aCWmax および再試行」(P.5-6) を参照)。
2. DIFS 間隔の間、チャネルが空くまで待機します。
3. チャネルがまだ空いている場合は、チャネルが空いているスロット タイム (20 μ s) ごとの、ランダム バックオフ番号のデクリメントを開始します。
4. ステーションが 0 に達した場合など、チャネルが使用中になると、デクリメントを停止し、手順 2 ~ 3 を繰り返します。
5. ランダム バックオフ番号が 0 に達するまでチャネルが空いたままであれば、フレームを送信できます。

図 5-4 は、DCF プロセスが動作する様子を示した簡単な例です。この DCF プロセスでは、確認応答は示されず、断片化は発生しません。

図 5-4 分散コーディネーション機能の例

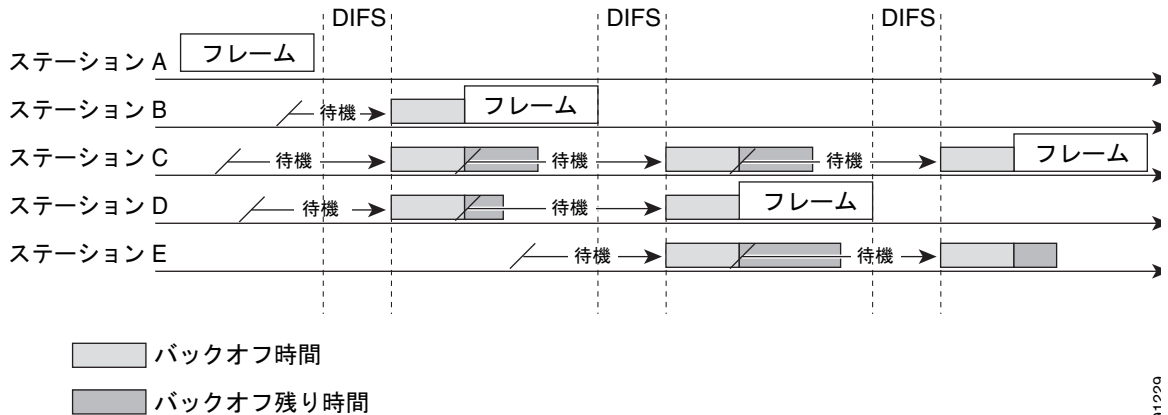


図 5-4 で示している DCF の手順は次のとおりです。

1. ステーション A は正常にフレームを送信します。他の 3 つのステーションもフレームを送信しようとしていますが、ステーション A のトラフィックが完了するまで待つ必要があります。
2. ステーション A が伝送を完了した後も、すべてのステーションはさらに DIFS の間待機する必要があります。
3. DIFS が完了すると、フレームの送信を待機していたステーションが、スロット タイムごとに 1 度バックオフカウンタのデクリメントを開始します。
4. ステーション B のバックオフカウンタがステーション C および D の前に 0 に達したので、ステーション B がフレームの送信を開始します。
5. ステーション C および D はステーション B の送信を検知すると、バックオフカウンタのデクリメントを停止し、ステーション B のフレームが送信され DIFS が経過するまで待機しなければなりません。
6. ステーション B がフレームを送信している間、ステーション E は送信するフレームを受信しますが、ステーション B が送信中であるため、ステーション C および D と同様に待機しなければなりません。
7. ステーション B が送信を完了し、DIFS が経過すると、送信すべきフレームを持つステーションがバックオフカウンタのデクリメントを開始します。この場合、ステーション D のバックオフカウンタが最初に 0 に達し、フレームの送信を開始します。

トラフィックが別のステーションに届くと、このプロセスが続行されます。

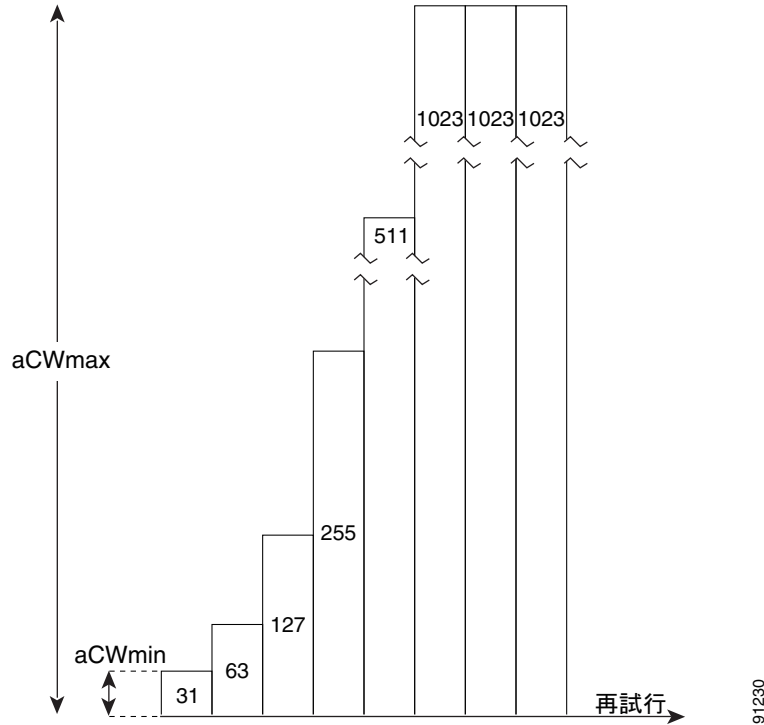
aCWmin、aCWmax および再試行

DCF はコンテンション ウィンドウ (CW) パラメータを使用して、ランダム バックオフのサイズを制御します。CW は、次のパラメータで定義されます。

- aCWmin : 最小コンテンション ウィンドウ
- aCWmax : 最大コンテンション ウィンドウ

ランダム バックオフで使用されるランダム番号は、最初は $0 \sim aCWmin$ です。最初のランダム バックオフがフレームを正常に送信せずに時間切れになった場合、ステーションまたは AP は再試行カウンタを増やし、ランダム バックオフ ウィンドウのサイズを 2 倍にします。このサイズの倍増は、サイズが $aCWmax$ と同じになるまで続行されます。再試行は、最大再試行回数または存続可能時間 (TTL) に達するまで続行されます。バックオフ ウィンドウを倍増させるこのプロセスは通常、バイナリ指数バックオフと呼ばれています。詳しくは図 5-5 で示します。ここでは、 $aCWmin$ が $2^5 - 1$ の場合 $2^6 - 1$ に増加し、その後次のバックオフ レベルでは $aCWmax$ 値である $2^{10} - 1$ にまで増加しています。

図 5-5 再試行に伴うランダム バックオフ範囲の増加



(注)

これらの値は 802.11b 実装に対するものです。別の物理レイヤの実装では、値が異なる場合があります。

Wi-Fi Multimedia

この項では、Wi-Fi multimedia (WMM) に関する次の 3 つの重要なトピックについて説明します。

- WMM のアクセス
- WMM の分類
- WMM キュー

WMM のアクセス

WMM は、802.11e 草案に述べられている一連の機能に対応した Wi-Fi Alliance の認証です。この認証はクライアントと AP の両方を対象としており、WMM の操作を認定します。WMM は基本的に、802.11e の EDCA コンポーネントの実装です。Wi-Fi の追加認証が、802.11e の別のコンポーネントを対象に計画されています。

WMM の分類

WMM では 802.1P 分類方式 (IEEE 802.1D MAC Bridges 標準の一部) が使用されています。この分類方式には 8 つの優先度があり、WMM ではこれが次の 4 つのアクセス カテゴリにマッピングされます。

- AC_BK : バックグラウンド
- AC_BE : ベスト エフォート
- AC_VI : ビデオ
- AC_VO : 音声

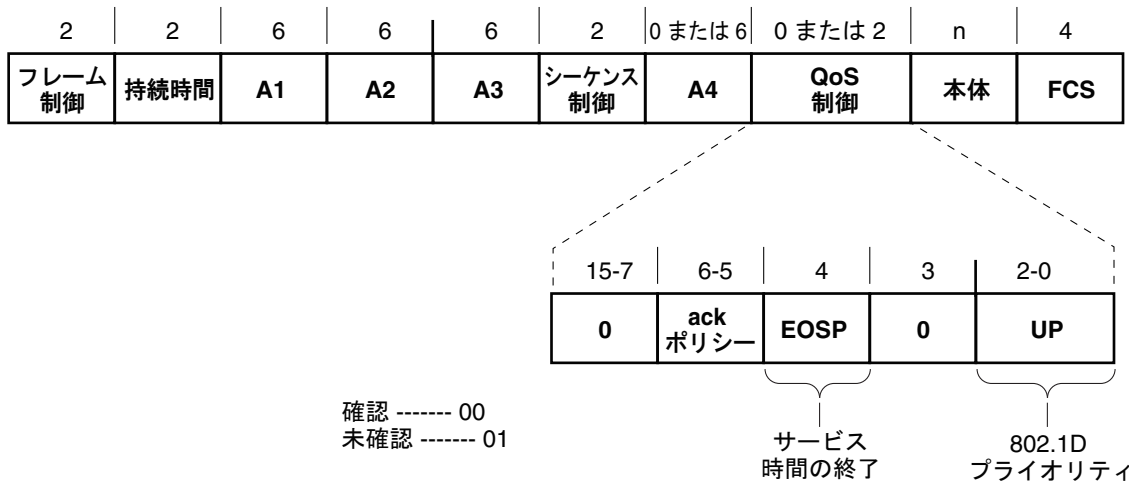
表 5-2 で示すように、これらのアクセス カテゴリは WMM デバイスに必要な 4 つのキュー (「WMM キュー」 (P.5-9) を参照) にマッピングします。

表 5-2 表 2 802.1P および WMM の分類

プライオリティ	802.1P のプライオリティ	802.1P の指定	アクセス カテゴリ_WMM の指定
最低	1	BK	AC_BK
	2	-	
	0	BE	AC_BE
	3	EE	
	4	CL	AC_VI
	5	VI	
	6	VO	AC_VO
	7	NC	
最高			

図 5-6 は、WMM データ フレーム形式を示しています。8 つの 802.1P 分類は WMM で 4 つのアクセス カテゴリにマッピングされますが、802.11D の分類はフレーム内で送信されることに注意してください。

図 5-6 WMM フレーム形式

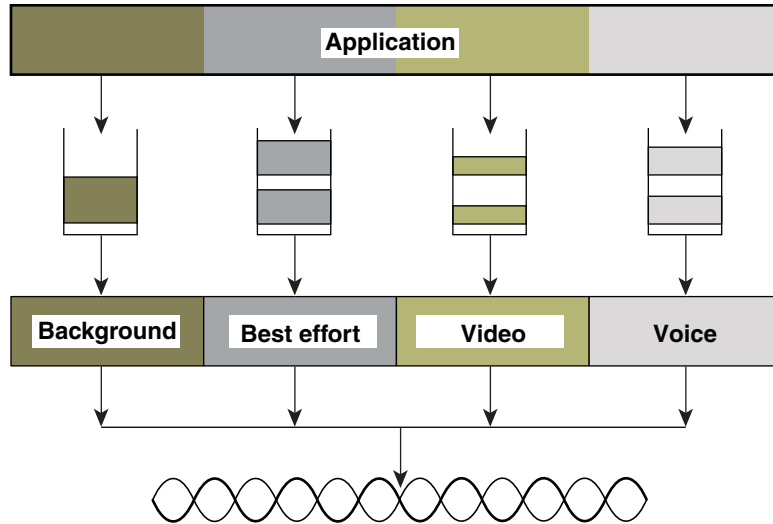


WMM および IEEE 802.11e の分類は、シスコのネットワークで推奨および使用されている、IETF 推奨の分類に基づく分類とは異なります。分類の主な違いは、音声とビデオのトラフィックをそれぞれ 5 および 4 のユーザ プライオリティ (UP) に変更している点です。これにより、6 つの分類をレイヤ 3 ネットワーク制御に使用できます。両方の標準に準拠するため、Cisco Unified Wireless ソリューションでは、トラフィックが無線と有線の境界を横切る際に、さまざまな分類標準間の変換が実行されます。

WMM キュー

図 5-7 は、WMM クライアントまたは AP で実行されるキューイングを示しています。4 つの別個のキューが、各アクセス カテゴリに 1 つずつあります。これらのキューはそれぞれ、前述した DCF メカニズムに対するのと同様の方法で無線チャネルを確保するために競います。このとき、各キューには異なる IFS、CWmin、および CWmax の値が使用されます。異なるアクセス カテゴリからの複数のフレームが内部で衝突した場合、優先度の高いフレームが送信され、優先度の低いフレームは、バックオフパラメータをキューイングメカニズムの外部のフレームと衝突した場合と同様に調整します。このシステムは、拡張型分散チャネルアクセス (EDCA) と呼ばれています。

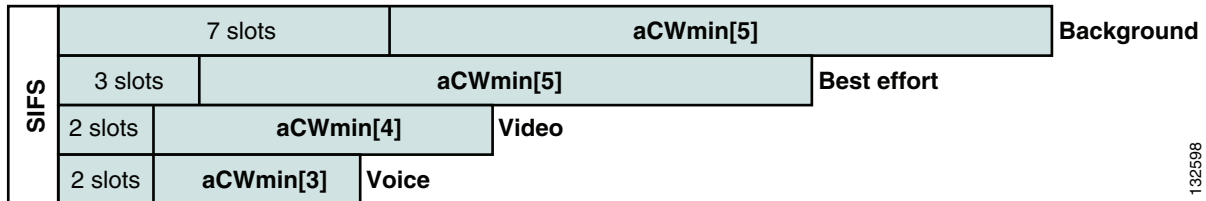
図 5-7 WMM キュー



132600

図 5-8 は、EDCF の背後の原則を示しています。ここでは、異なるフレーム間スペースと CWmin および CWmax の値が、トラフィックの分類ごとに適用されています (明確にするため CWmax は示されていません)。トラフィック タイプが異なると、ランダム バックオフをカウントダウンする前に別の IFS を待機させることができます。ランダム バックオフ番号の生成に使用される aCW 値も、トラフィックの分類によって異なります。たとえば、音声の CWmin[3] は 23 -1 で、ベストエフォートトラフィックの CWmin[5] は 25 -1 です。優先度が高いトラフィックでは IFS が小さく aCWmin 値も小さいため、ランダム バックオフが短くなりますが、一方ベストエフォートトラフィックでは IFS が長く aCWmin 値も大きくなるため、ランダム バックオフ数が平均して高くなります。

図 5-8 アクセス カテゴリのタイミング

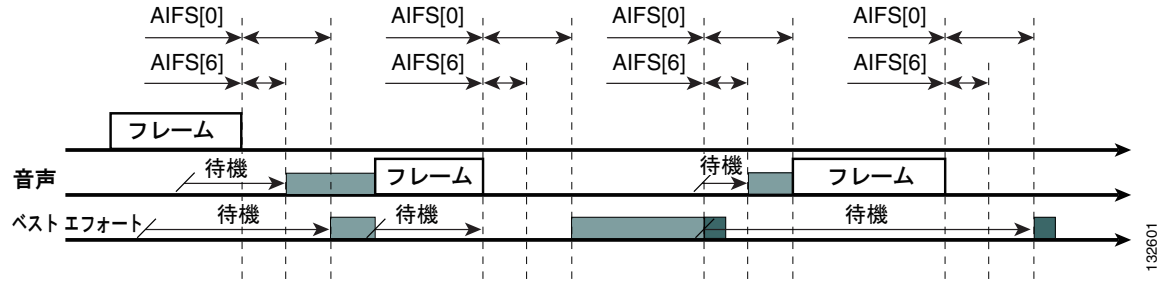


132598

EDCA

図 5-9 は、拡張型分散チャネルアクセス (EDCA) のプロセスの例を示しています。

図 5-9 EDCA の例



EDCA プロセスでは、次の順序で処理が行われます。

1. ステーション X がフレームを送信中に、他の 3 つのステーションがフレームを送信する必要があると判断します。フレームはすでに送信中なので、各ステーションは待機し、ランダム バックオフを生成します。
2. 音声のステーションには音声のトラフィック分類があるため、2 の調停フレーム間スペース (AIFS) があり、3 の初期 aCWmin を使用します。したがって、ランダム バックオフのカウントダウンを待機する必要があるのは 2 のスロット タイムです。ランダム バックオフ値も短くなります。
3. ベストエフォートの CWmin 値は 5 なので、ベストエフォートのステーションには 3 の AIFS があり、ランダム バックオフ タイムは長くなります。
4. 音声のステーションのランダム バックオフ タイムが最短であるため、ここが最初に送信を開始します。音声を送信を開始すると、他のすべてのステーションは待機します。
5. 音声のステーションが送信を終えると、すべてのステーションはそれぞれの AIFS の間待機し、その後再びランダム バックオフ カウンタのデクリメントを開始します。
6. 次にベストエフォートがランダム バックオフ カウンタのデクリメントを完了し、送信を開始します。他のすべてのステーションは待機します。

送信を待機している音声のステーションがある場合でも、この動作が発生します。これは、ランダム バックオフのデクリメントプロセスで最終的にはベストエフォート バックオフが高優先度トラフィックと同様のサイズにまで縮小されるため、音声トラフィックによってベストエフォートトラフィックが漸減しないこと、およびランダム プロセスが、場合に応じて、ベストエフォートトラフィックに対して小さいランダム バックオフ番号を生成することを示しています。

7. 他のトラフィックがシステムに入ると、このプロセスが続行されます。

表 5-3 および表 5-4 に示されているアクセス カテゴリの設定は、デフォルトでは 802.11a 無線と同じで、WMM で定義されている式に基づいています。



(注)

表 5-3 に、クライアントのパラメータ設定を示します。この設定は、AP の設定とは若干異なります。AP では、音声およびビデオのアドミッション制御 (AC) に対する AIFS[n] が大きくなります。

表 5-3 WMM クライアント パラメータ

AC	CWmin	aCWmax	AIFS[n]	TXOP 制限 (802.11b)	TXOP 制限 (802.11a/g)
AC_BK	CWmin	aCWmax	7	0	0
AC_BE	CWmin	$4 * (aCQmin + 1) - 1$	3	0	0

表 5-3 WMM クライアント パラメータ (続き)

AC	CWmin	aCWmax	AIFS[n]	TXOP 制限 (802.11b)	TXOP 制限 (802.11a/g)
AC_VI	$(CWmin+1) / 2 - 1$	CWmin	1	6.016 ミリ秒	3.008 ミリ秒
AC_VO	$(CWmin+1) / 4 - 1$	$(CWmin+1) / 2 - 1$	1	3.264 ミリ秒	1.504 ミリ秒

表 5-4 WMM AP パラメータ

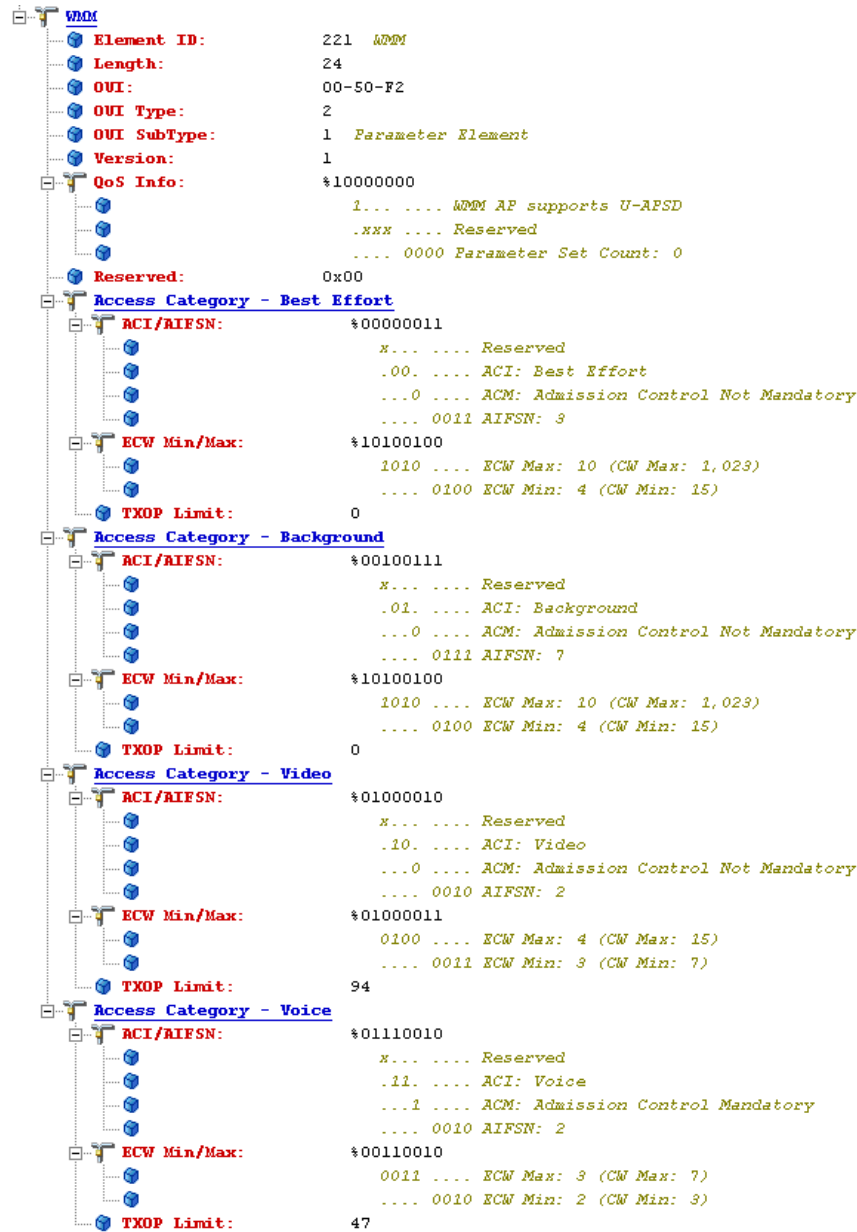
アクセス カテゴリ	CWmin	aCWmax	AIFS[n]	TXOP 制限 (802.11b)	TXOP 制限 (802.11a/g)
AC_BK	CWmin	aCWmax	7	0	0
AC_BE	CWmin	$4 * (aCQmin+1) - 1$	3	0	0
AC_VI	$(CWmin+1) / 2 - 1$	CWmin	2	6.016 ミリ秒	3.008 ミリ秒
AC_VO	$(CWmin+1) / 4 - 1$	$(CWmin+1) / 2 - 1$	2	3.264 ミリ秒	1.504 ミリ秒

異なる AIFS、CWmin、および aCWmax の値が全体に及ぼす影響は、その影響が本来は統計に基づくことが多いため、タイミング ダイアグラムに示すことは困難です。AIFS とランダム バックオフ ウィンドウのサイズを比較する方が簡単です (図 5-8 を参照)。

例として音声フレームとバックグラウンドフレームを比較すると、これらのトラフィック カテゴリの CWmin 値はそれぞれ $2^3 - 1$ (7)、 $2^5 - 1$ (31) で、AIFS は 2、7 です。フレームを送信するまでの平均の遅延は、音声フレームでは $5 (2+7/1)$ スロット タイム、バックグラウンドフレームでは $22 (7+31/2)$ スロット タイムです。したがって、音声フレームは、統計的にはバックグラウンドフレームの前に送信される傾向が強くなります。

図 5-10 では、プローブ応答内の WMM 情報を示します。この要素に含まれる WMM アクセス カテゴリ情報とは別に、クライアントはアドミッション制御を必要とする WMM カテゴリについても認識します。この例で示すとおり、音声アドミッション制御が必須に設定されています。そのため、クライアントは要求を AP に送信し、受け入れられてからでないと、その AC を使用できません。アドミッション制御については、この章で後述します。

図 5-10 プローブ応答の WMM 要素情報



221939

不定期自動省電力配信 (U-APSD)

不定期自動省電力配信 (U-APSD) は、次の 2 つの主要な特長を持つ機能です。

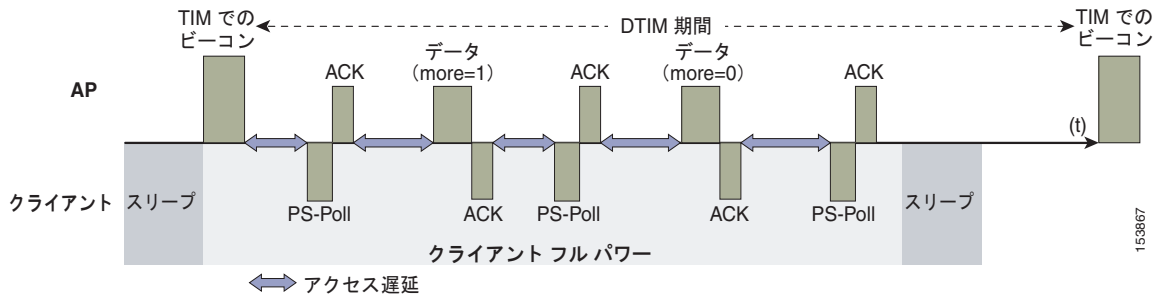
- U-APSD の第 1 の利点は、音声クライアントが AP との間で音声フレームの送受信を同期できることです。そのため、クライアントは音声フレームの各タプルの送受信間に省電力モードになることができます。U-APSD をサポートしているアクセスカテゴリ内で WLAN クライアントからフレームが送信されると、AP はその WLAN クライアントに対してキューイングされているそのアクセスカテゴリのあらゆるデータフレームの送信を開始します。U-APSD クライアントは、AP からサービス時間終了 (EOSP) ビットセットを含むフレームを受信するまで、AP の接続を待機し続けます。EOSP ビットセットによって、省電力モードに戻れることがクライアントに通知されま

す。このトリガーメカニズムでは、配信トラフィック通知メッセージ (DTIM) の間隔によって制御された間隔において、通常のビーコン方式の待機よりもクライアントの電源の使用を効率化できると見なされています。それは、音声の遅延要件とジッター要件により、無線 VoIP クライアントはコール中に省電力モードになれず、その結果通話時間が短縮されるか、DTIM 間隔が短くなり、結果として待機時間が短縮されてしまうためです。U-APSD を使用すれば、長い DTIM 間隔を使用して、コールの質を犠牲にせずにスタンバイ時間を最大限にできます。U-APSD 機能はアクセスカテゴリ全体で個別に適用できるため、AP で音声 AC に U-APSD を適用しつつ、他の AC では標準の省電力機能を使用できます。

- この機能の第 2 の利点は、コール キャパシティの増大です。AP からのデータ フレームをバッファされた伝送と、WLAN クライアントから取り込んだトリガリング データ フレームを組み合わせることで、IFS およびランダム バックオフなしで AP からのフレームを送信できます。これにより、コールによるコンテンションの発生が緩和されます。

図 5-11 では、標準 802.11 の省電力配信プロセスにおけるフレーム交換の例を示します。

図 5-11 標準のクライアント省電力



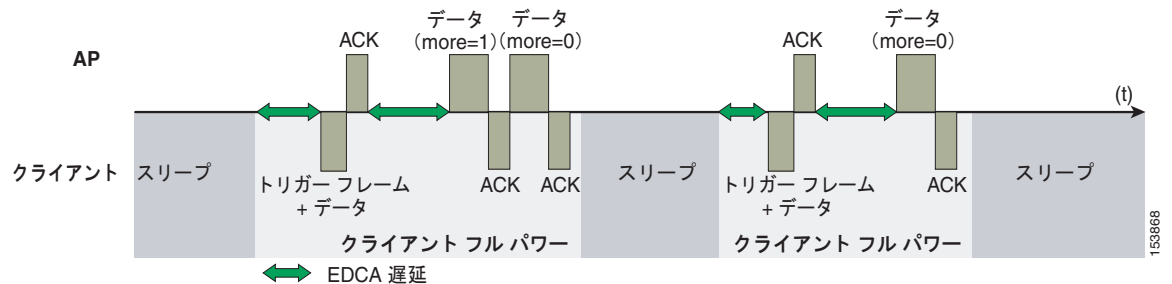
省電力モードにあるクライアントは、まず AP ビーコン内の TIM の存在を介して、AP でデータが待機していることを認識します。クライアントは、そのデータを取得するために AP を省電力ポーリング (PS-Poll) する必要があります。クライアントに送信されたデータが複数のフレームの送信を要求している場合、AP はそのことを送信済みデータ フレーム内に示します。このプロセスでは、クライアントはバッファされたすべてのデータを取得するまで、AP に省電力ポーリングを送信し続ける必要があります。

このことは 2 つの大きな問題点を提示しています。1 つ目の問題は、このプロセスが非常に非効率的で、PS ポーリング以外にも通常のデータ交換を要求し、DCF に関連する標準アクセス遅延を発生するということです。第 2 の問題点は、バッファ済みデータの取得が DTIM に依存しており、それによってビーコン間隔がさまざまに異なるということです。このことは、音声トラフィックに対してより重大な問題となります。標準のビーコン間隔は 100 ミリ秒であり、DTIM 間隔はこの整数の倍数となります。その結果、音声コールには通常は許容されないジッター レベルが発生し、音声端末は、音声コールの進行中、省電力モードをフル送信に切り替えて動作を受信します。これにより、許容できる音質を確保できますが、バッテリーの寿命は短くなります。Cisco 7921G Unified Wireless IP Phone では、ビーコンの TIM を待たずに PS ポーリング要求を生成できる PS ポーリング機能を提供することによって、この問題に対処しています。この機能により、7921G はフレームを送信したときにフレームのポーリングを実行し、その後、省電力モードに戻ることができます。この機能では U-APSD と同じ効率性は得られませんが、U-APSD を使用しない WLAN で 7921G のバッテリーの寿命を伸ばすことができます。

図 5-12 では、U-APSD を使用したトラフィック フローの例を示します。この場合、トラフィックを取得するためのトリガーは、クライアントによる AP へのトラフィック送信です。AP は、フレームを確認すると、データがキューイングされていることと、接続し続けなくてはならないことをクライアントに伝えます。その後 AP は、データをクライアントへ送信します。通常は TXOP バーストとして送信しますが、この場合は最初のフレームだけに EDCF アクセス遅延が発生します。すべての後続のフ

フレームは、応答フレームの後に直接送信されます。VoWLAN 実装では、AP でキューイングされている可能性があるフレームは 1 つのみです。VoWLAN クライアントは、そのフレームを AP から受信した後でスリープモードに入ることができます。

図 5-12 U-APSD



この方法は、以前の方式の短所を両方とも克服した、はるかに効率的な方法です。ポーリングのタイミングは、クライアントトラフィックにより制御されます。クライアントトラフィックは音声の場合には対称になるので、クライアントが 20 ミリ秒ごとにフレームを送信した場合、フレームの受信も 20 ミリ秒になると想定されます。それにより、発生する最大ジッターは $n * 100$ ミリ秒ではなく 20 ミリ秒になります。

TSpec アドミッション制御

Traffic Specification (TSpec) では、802.11e クライアントから AP へ、そのトラフィック要件に関する信号を送信できます。802.11e MAC 定義には、コンテンションベースの EDCA オプションと、送信権 (TXOP) によって提供される制御されたアクセス オプションという、アクセスを優先させるための 2 つのメカニズムがあります。クライアントがそのクライアント自体のトラフィック特性を指定できる TSpec 機能とはどのようなものかを説明する際、簡単に思い浮かぶのは、制御されたアクセスメカニズムが自動的に使用されるようになり、TSpec 要求に一致する特定の TXOP がクライアントに対して許可される、というものです。しかし、必ずしもそうとは限りません。TSpec 要求を使用して、EDCA のさまざまなアクセスカテゴリ (AC) の使用を制御することもできます。クライアントが特定の優先度タイプのトラフィックを送信できるようになる前に、TSpec メカニズムを使用してそれを要求しておく必要があります。たとえば、音声アクセスカテゴリを使用しようとしている WLAN クライアントデバイスは、最初にその AC 使用の要求を行う必要があります。AC の使用を TSpec 要求で制御するかどうかは、TSpec 要求により制御される音声 AC とビデオ AC で設定可能です。ベストエフォート AC とバックグラウンド AC については TSpec 要求なしで使用できます。802.11e Hybrid Coordinated Channel Access (HCCA) ではなく EDCA AC を使用して TSpec 要求を満たすことも、多くの場合可能です。これは、トラフィックパラメータが非常に単純なため、特定の TXOP を作成してアプリケーションの要求を満たさなくても、キャパシティを割り当てることによってパラメータを満たせるためです。

Add Traffic Stream (トラフィックストリームの追加)

Add Traffic Stream (ADDTs) 機能は、WLAN クライアントが AP へのアドミッション要求を実行する際に使用されます。アドミッション要求では、次の 2 つのいずれかの形式で TSpec 要求が AP に送信されます。

- ADDTs アクションフレーム：AP に関連付けられたクライアントが通話を開始または終了したときに作成されます。ADDTs には TSpec が含まれています。トラフィックストリームレートセット (TSRS) 情報要素 (IE) が含まれる場合もあります。

- アソシエーションおよび再アソシエーション メッセージ：ステーションがトラフィック ストリームをアソシエーションの一部として確立しようとする時、アソシエーション メッセージに 1 つまたは複数の TSpec および 1 つの TSRS IE が含まれることがあります。ステーションが別の AP にローミングすると、再アソシエーション メッセージに 1 つまたは複数の TSpec および 1 つの TSRS IE が含まれることがあります。

ADDTs には、トラフィック要求を説明する TSpec 要素が含まれます。Cisco 7921 WLAN 端末と Cisco AP の間の ADDTs 要求と応答の例については、[図 5-13](#) および [図 5-14](#) を参照してください。データ レートおよびフレーム サイズなど、トラフィックの要件を説明する主要なデータとは別に、TSpec 要素もクライアント デバイスが使用する最小物理レートを AP に伝えます。これにより、そのステーションがどのくらいの時間を消費してこの TSpec を送受信できるかを算出できるようになります。したがって、その TSpec を満たすリソースがあるかどうかを AP で算出できるようになります。TSpec アドミッション制御は、コールが開始されたときとローミングの要求中に、WLAN クライアントにより使用されます (ターゲット クライアントは VoIP 端末)。ローミングの際には、TSpec 要求が再アソシエーション要求に追加されます。

TSpec のサポートは、クライアントには必要ありません。ただし、WLAN が、音声またはビデオのコールアドミッション制御 (CAC) を使用して設定されている場合、TSpec をサポートしていないクライアントでは、ベスト エフォート型 QoS で音声またはビデオの packets を送信する必要があります ([「QoS プロファイル」\(P.5-18\)](#) を参照)。したがって、この WLAN が音声またはビデオの QoS レベルで設定され、CAC がイネーブルになっている場合、ADDTs ロジックを使用していないクライアントの正しい動作は、ベスト エフォート型にマーキングされた音声およびビデオ トラフィックを送信することです。TSpec 対応のクライアントに ADDTs 要求の拒否が存在していれば、Wi-Fi チャンネルの利用率は、設定された CAC 制限よりも高くなります。そのクライアントでは、音声パケットおよびビデオパケットがクライアントの仕様ごとにベスト エフォート型でマーキングされます。

図 5-13 ADDTS 要求のデコード

```

802.11 Management - Action
  Category Code: 17 WMM
  Action Code: 0 ADDTS Request
  Dialog Token: 1
  Status Code: 0 Admission Accepted
  VMO
  Element ID: 221 WMM
  Length: 61
  OUI: 00-50-F2
  OUI Type: 2
  OUI SubType: 2 TSPEC
  Version: 1
  TS Info: $00000000000000000000000011010011101100
            XXXXXXXX. .... Reserved
            .....0 ..... Schedule: Reserved
            .....00..... TSInfo Ack Policy: Normal IEEE 802.11 acknowledgement
            .....110..... UP: 6
            .....1..... FSB: Triggered
            .....0..... Aggregation: Reserved
            .....01..... AP: EDCA - Contention based channel access
            .....11..... Direction: Bi-directional
            .....0110. TID: EDCA: 6
            .....0 Traffic Type: Reserved
  Nominal MSDU Size: $00000000011001000
                    Size Might not be Fixed
                    Size: 200
  Maximum MSDU Size: 200
  Min Service Interval: 0
  Max Service Interval: 0
  Inactivity Interval: 0
  Suspension Interval: 4294967295
  Service Start Time: 0
  Min Data Rate: 80000
  Mean Data Rate: 80000 bits per second
  Peak Data Rate: 80000
  Max Burst Size: 0
  Delay Bound: 0
  Min PHY Rate: 12000000 bits per second
  Surplus Bandwidth Allowance: 1.2457
  Medium Time: 0 (units of 32 microsecond periods/second)
    
```

221940

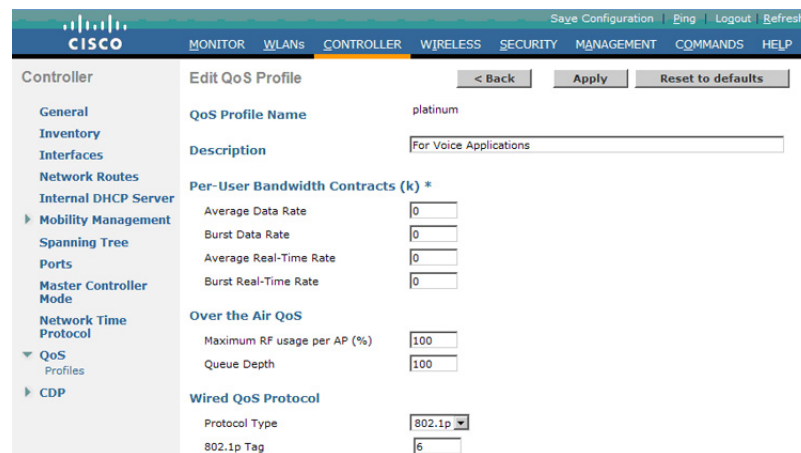
- プラチナ：音声アプリケーション
- シルバー：ベスト エフォート

図 5-15 QoS プロファイル オプション



図 5-16 に示すプロファイルごとに、帯域幅の契約、RF 使用制御、および許可された最大の 802.1P 分類を設定できます。

図 5-16 QoS プロファイルの設定



シスコでは通常、ユーザごとの帯域幅契約の設定はデフォルト値のままにして、802.11 WMM 機能を使用して差別化サービスを提供することを推奨します。

特定のプロファイルを使用する WLAN については、そのプロファイルの 802.1P 分類によって次の 2 つの重要なサービス クラス (CoS) の動作が制御されます。

- WLC から送信されるパケットに使用する CoS 値の決定

CoS パラメータの値を使用して、そのプロファイルを使用する WLAN のすべての CAPWAP (Control And Provisioning of Wireless Access Points) パケットの CoS がマーキングされます。たとえば、プラチナ QoS プロファイルを使用している WLAN の場合、802.1P マークが 6 なら、コントローラのアプリケーション マネージャ インターフェイスから送信される CAPWAP パケットは 5 の CoS としてマーキングされます。CoS は、Cisco QoS ベースライン推奨事項に準拠するよ

うに WLC で調整されます。設定に IEEE CoS のマーキングを維持することが重要である理由については、次に説明します。WLC へのネットワーク接続で DSCP ではなく CoS を信頼するように WLAN が設定されている場合、AP が受信する CAPWAP パケットの DSCP は CoS 値によって決まります。また、その結果として WLAN トラフィックの WMM 分類とキューイングが決まります。これは、フレームの WLAN WMM 分類が、そのフレームを伝送する CAPWAP パケットの DSCP 値から派生するためです。

- その WLAN に接続したクライアントが使用できる最大 CoS 値の決定

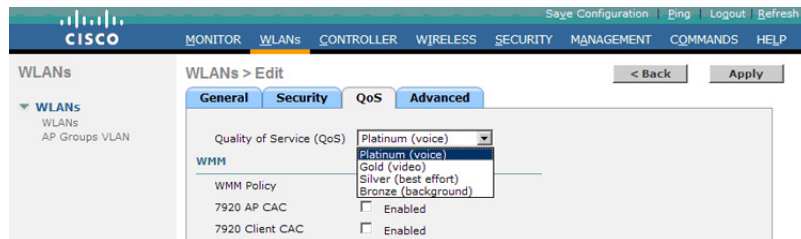
802.1P 分類によって、そのプロファイルを使用する WLAN で許可される最大 CoS 値が設定されます。

WMM の音声トラフィックは、CoS 6 で AP に着信し、CoS 6 に基づいて、このトラフィックに対して CoS から DSCP へのマッピングが AP で自動的に実行されます。WLC 設定の CoS 値が 6 未満の値に設定されている場合、この変更された値が AP の WLAN QoS プロファイルで使用されて、使用されている最大 CoS マーキングが設定されます。そしてそれにより、使用する WMM アドミッション制御 (AC) が設定されます。

重要な点は、Unified Wireless Network では常に IEEE 802.11e 分類の観点から考え、IEEE 分類と Cisco QoS ベースラインとの間の変換を Unified Wireless Network ソリューションで実行できるようにすることです。

WLAN はさまざまなデフォルト QoS プロファイルを使用して設定できます (図 5-17 を参照)。各 QoS プロファイルは、代表的な使用に対して注釈が付けられます。さらに、クライアントには、認証、許可、アカウントリング (AAA) を使用して ID に基づいて QoS プロファイルを割り当てることができます。一般的な企業で、クライアントに最適な QoS を提供するためには、ユーザごとの帯域幅契約や Over-the-Air QoS などの WLAN 展開パラメータをデフォルト値のままにしておき、WMM や有線 QoS などの標準 QoS メカニズムを使用する必要があります。

図 5-17 WLAN QoS プロファイル

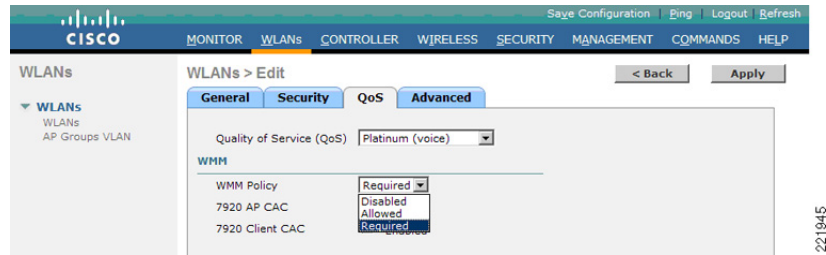


WMM ポリシー

QoS プロファイル以外に、WLAN ごとの WMM ポリシーによって追加の WMM オプションも制御できます (図 5-18 を参照)。WMM オプションには次のようなものがあります。

- [Disabled] : WLAN で WMM 機能はアドバタイズされず、WMM ネゴシエーションも許可されません。
- [Allowed] : WLAN で WMM クライアントと WMM 以外のクライアントが許可されます。
- [Required] : WMM 対応クライアントのみをこの WLAN にアソシエートできます。

図 5-18 WLAN WMM ポリシー



Voice over IP 電話

図 5-19 では、Cisco AP がアダプタイズする基本的な QoS Basis Service Set (QBSS) 情報要素 (IE) を示します。[Load] フィールドは、現在その AP のデータを送信するために使用されている有効な帯域幅の一部を示しています。

図 5-19 QBSS 情報要素

1 オクテット	1 オクテット	4 バイト
要素 ID (11)	長さ	負荷

特定の状況でサポートする必要のある QBSS IE は、次の 3 つです。

- 旧 QBSS : Draft 6 (pre-standard)
- 新 QBSS : Draft 13 802.11e (standard)
- 新分散型 CAC 負荷の IE : シスコの情報要素

使用する QBSS は WLAN 上の WMM および Cisco 792x VoIP 電話の設定に依存します。

図 5-20 で示しているとおり、792x 電話のサポートは、WLC WLAN 構成のコンポーネントです。これにより、AP にビーコンの適切な QBSS 要素を含めることができます。Cisco 792x 電話など QoS 要件のある WLAN クライアントは、これらのアダプタイズされた QoS パラメータを使用して、アソシエートすべき最良の AP を決定します。

WLC は、クライアント コール アドミッション制御 (CAC) 制限を使用して 792x 電話をサポートします。このサポートには次の機能があります。

- クライアント CAC 制限 : 7920 は、クライアントに設定されたコール アドミッション制御設定を使用します。これは、2.01 以前の古い 7920 コードをサポートします。
- AP CAC 制限 : 7920 は、WLAN アダプタイズメントから習得した CAC 設定を使用します。

WMM、クライアント CAC 制限、および AP CAC 制限のさまざまな組み合わせにより、次のようなさまざまな QBSS IE が送信されます。

- WMM だけがイネーブルの場合、IE 番号 2 (802.11e 標準) QBSS Load IE がビーコン応答とプローブ応答で送信されます。
- 7920 クライアント CAC 制限がサポートされる場合、IE 番号 1 (以前の標準 QBSS IE) が 802.11b/g 無線のビーコン応答とプローブ応答で送信されます。

- 7920 AP CAC 制限がサポートされる場合、IE 番号 3 QBSS IE が bg 無線のビーコンとプローブ応答で送信されます。



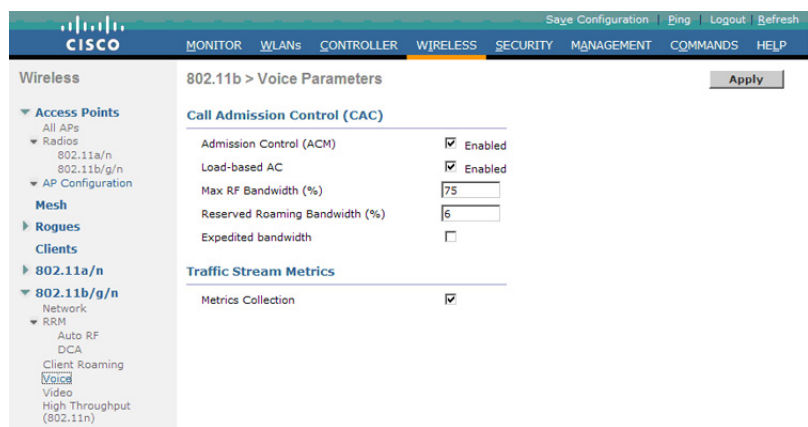
(注)

さまざまな QBSS IE が同じ ID を使用するので、これらの 3 つの QBSS は相互に排他的です。たとえば、ビーコン応答およびプローブ応答には 1 つの QBSS IE のみを含めることができます。

アドミッション制御パラメータ

図 5-20 では、コントローラの音声パラメータ設定の設定画面の例を示しています。

図 5-20 音声パラメータの設定



CAC パラメータは、無線が対応でき、通常の ADDTS 要求により VoWLAN コールを開始させることができる、[Max RF Bandwidth (%)] を含みます。この値の範囲は、チャンネル帯域幅の 5～85% です。

[Reserved Roaming Bandwidth (%)] は、アソシエーションまたは再アソシエーション時の ADDTS に応答できるようにどれだけのキャパシティを取っておくか、また通話中の VoWLAN クライアントのうちのどれがその AP にローミングしようとしているかを指定します。

これらのパラメータに基づいてアドミッション制御を有効にするには、[Admission Control (ACM)] チェックボックスをオンにします。それによって、AP のキャパシティに基づくアドミッション制御が有効になりますが、エリア内の他の AP のチャンネル負荷の影響の可能性は考慮されません。キャパシティ計算にこのチャンネル負荷を算入するには、[Load-Based AC] チェックボックスと [Admission Control (ACM)] チェックボックスの両方をオンにします。



(注)

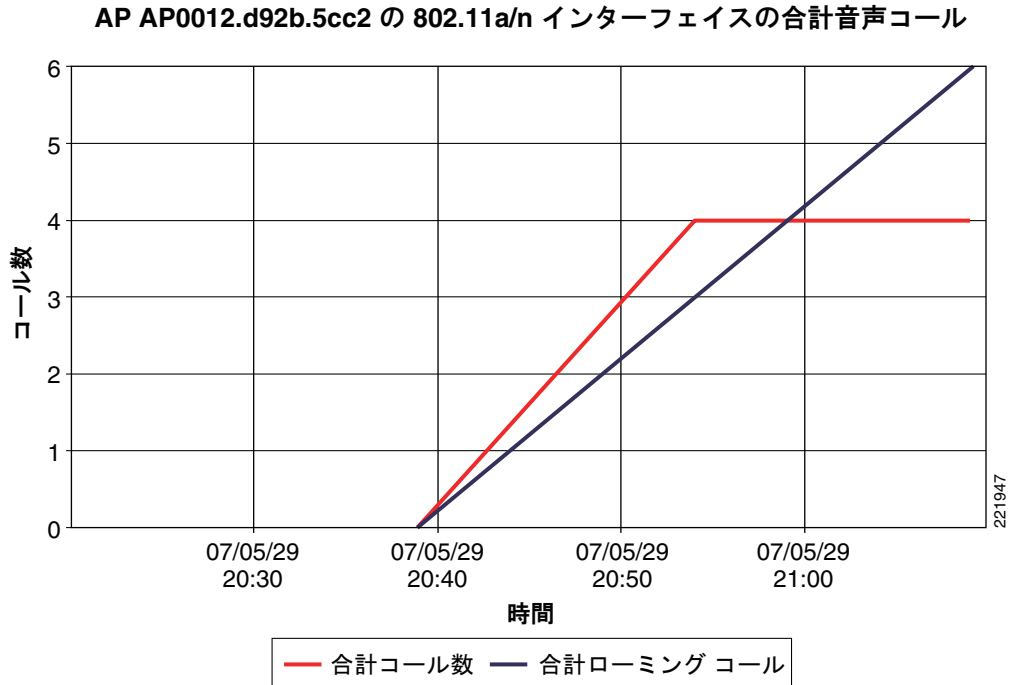
音声およびビデオの負荷ベースの CAC は非メッシュ AP に適用されます。メッシュ AP の場合は、静的な CAC のみが適用されます。

SIP CAC のサポートには、スタティックまたは負荷ベースの CAC が必要です。スタティック CAC を使用している場合は、SIP CAC のサポートにより、AP でのコールの数を設定できます。通常、Wi-Fi チャンネル上のコールのサブスクリプションによって品質が影響を受けないようにするためにコール数を管理する方法としては、ダイナミックな負荷分散型アプローチの方が優れています。

[Voice Parameters] ウィンドウ (図 5-20) の [Metrics Collection] オプションで、Cisco Prime Infrastructure で使用するために音声またはビデオ コールでデータを収集するかどうかを指定します。

図 5-21 では、Cisco Prime Infrastructure で使用できる音声統計レポートの一例を示します。この例では、1 つの AP の無線で確立されたコールと、その AP にローミングしたコール数を示しています。このレポートおよび他の音声統計は、スケジュール設定するか、または要求に応じて（一時的に）使用できるほか、Cisco Prime Infrastructure でのグラフィック表示やファイルへの書き込みが可能です。

図 5-21 Cisco Prime Infrastructure の音声統計



(注)

CAC は、音声とビデオの QoS プロファイルに対してのみ実行されます。

図 5-21 では、音声 CAC のコール用に予約されている帯域幅の割合が小さい場合の影響を示します。4 つのコールに対して十分な帯域幅が予約されましたが、コールは他の Wi-Fi チャンネルにローミングすることが可能でした。図 5-22 では、メディア ストリーミング用の CAC オプションを示します。最大 RF 帯域幅は音声、ビデオおよびメディア ストリーミングの間で共有されます。[Voice]、[Video] および [Media] タブにはそれぞれ固有の最大 RF 帯域幅があります。この最大 RF 帯域幅を合計して、Wi-Fi チャンネルのメディアの完全な帯域幅予約の総計を得ます。各タブのフィールドには 85% という最大値が表示されていますが、全体的な最大 RF 帯域幅値は実際には 3 つすべてのフィールドの合計です。[Voice] タブの最大 RF 帯域幅が 85% に設定されている場合、[Video] タブと [Media] タブでは [Max RF Bandwidth] フィールドをゼロに設定する必要があります。音声、ビデオ、データすべての CAC の動作に帯域幅を必要とする場合、各タブのフィールドを 25% に設定します。そうすると、メディアのチャンネル帯域幅の制限が 75% になります。それぞれのメディアのタイプに帯域幅の 4 分の 1 を割り当て、データに帯域幅の 4 分の 1 を割り当てるわけです。

図 5-22 WLC の [802.11a (5 GHz) Media] ウィンドウ



ビデオ用 CAC は、音声 CAC と似た動作をします。ビデオ用 CAC の目的は、実行中のビデオ コールの品質が Wi-Fi チャンネルに追加されたビデオによる悪影響を受けないよう、ビデオ コールの量を制限することです。



(注) この件やその他の設定オプションの詳細については、WLC のコンフィギュレーション ガイドを参照してください。

TSpec アドミッション制御の影響

TSpec アドミッション制御の目的は、WLAN へのクライアント アクセスを拒否することではなく、優先度の高いリソースを保護することです。したがって、TSpec アドミッション制御を使用していないクライアントが、そのトラフィックをブロックされることはありません。トラフィックを送信しようとしたときに、単にトラフィックが再分類されるだけです（保護されたアドミッション制御においてそのクライアントが WMM に準拠したトラフィック送信する場合は不適切）。

表 5-5 および表 5-6 では、アクセス制御が有効である場合の分類への影響を、トラフィック ストリームが確立されているかどうかに基づいて示しています。

表 5-5 アップストリーム トラフィック

AC 有効	確立されたトラフィック ストリーム	トラフィック ストリームなし
無効	動作に変化なく、パケットは従来どおりネットワークに送信されます。ユーザ優先度 (UP) は max = WLAN QoS 設定に制限されます。	動作に変化なく、パケットは従来どおりネットワークに送信されます。UP は max = WLAN QoS 設定に制限されます。
有効	動作に変化なく、パケットは従来どおりネットワークに送信されます。UP は max = WLAN QoS 設定に制限されます。	パケットが WMM クライアントのネットワークに入る前に、パケットが BE (CoS および DSCP の両方) に対してリマークされます。WMM 以外のクライアントについては、WLAN QoS と共にパケットが送信されます。

表 5-6 ダウンストリーム トラフィック

AC 有効	確立されたトラフィック ストリーム	トラフィック ストリームなし
無効	変更なし	変更なし
有効	変更なし	WMM クライアントの BE に対して UP をリマークします。WMM 以外のクライアントに対しては、WLAN QoS を使用します。

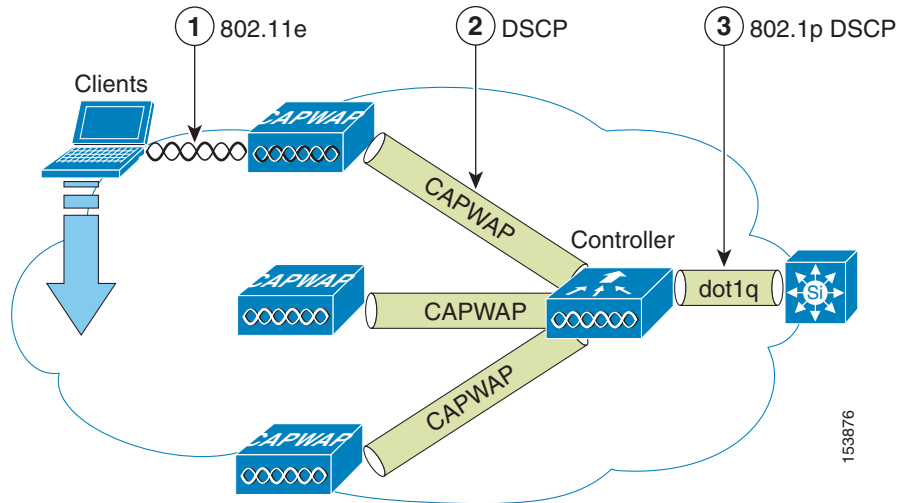
802.11e、802.1P および DSCP のマッピング

Unified Wireless Network 内の WLAN データは CAPWAP (IP UDP パケット) を介してトンネリングされます。WLAN フレームに適用された QoS 分類を維持するため、WLC は DSCP と CoS の間の分類のマッピングプロセスを使用します。たとえば、WLAN クライアントから WMM で分類されたトラフィックが送信された場合、このトラフィック フレームには 802.1P 分類が含まれています。AP はこの分類を DSCP 値に変換する必要があります。それによって、このフレームを伝送する CAPWAP パケットが WLC へ達するまでの間、適切な優先度で確実に処理されるようになります。これに類似したプロセスは、AP に行く CAPWAP パケットに対して WLC でも発生する必要があります。

WMM 以外のクライアントからのトラフィックを分類するメカニズムも必要です。それによって、WMM 以外のクライアントの CAPWAP パケットにも AP および WLC によって適切な DSCP 分類 (「分類に関する考慮事項」(P.5-32) を参照) が割り当てられます。

図 5-23 では、CAPWAP WLAN ネットワークのさまざまな分類メカニズムを示します。

図 5-23 WMM と 802.1P との関係



複数の分類メカニズムとクライアントの機能には、複数の戦略が必要です。戦略とは次のようなものです。

- CAPWAP 制御フレームには優先順位が必要です。CAPWAP 制御フレームは CS6 (IP ルーティングクラス) の DSCP 分類でマーク付けされます。
- WMM を有効化したクライアントは、WLC への CAPWAP パケットに対する該当 DSCP 分類へマップされたフレームの分類が割り当てられています。このマッピングは、QoS ベースラインへの準拠に必要な変更を除いて、IEEE CoS から DSCP へのマッピングの標準に従っています。この DSCP 値は、WLC において、WLC インターフェイスから発信される 802.1Q フレーム上で CoS 値に変換されます。
- WMM 以外のクライアントには、その WLAN のデフォルトの QoS プロファイルに一致するように設定された CAPWAP トンネルの DSCP があります。792x 電話をサポートする WLAN の QoS プロファイルがプラチナに設定されている場合、その AP WLAN からのデータ フレーム パケットについても EF の DSCP 分類となります。
- WLC からの CAPWAP データ パケットには、WLC へ送信された有線データ パケットの DSCP によって決定される DSCP 分類があります。AP から WMM クライアントへのフレーム送信時に使用される 802.11.e 分類は、DSCP 分類を WMM 分類へ変換する AP テーブルによって決定されます。



(注) AP から WLAN クライアントに送信されるトラフィックに使用される WMM 分類は、CAPWAP パケットの DSCP 値に基づき、含まれている IP パケットの DSCP 値には基づきません。そのため、エンドツーエンドの QoS システムの整備が重要になります。

QoS ベースラインの優先度のマッピング

CAPWAP AP と WLC で QoS ベースラインの変換が実行されることによって、表 5-7 で示すとおり、WMM 値は IEEE 値ではなく適切な QoS ベースライン DSCP 値にマッピングされます。

表 5-7 アクセス ポイントの QoS 変換値¹

AVVID 802.1 UP ベースのトラフィック タイプ	AVVID IP DSCP	AVVID 802.1p UP	IEEE 802.11e UP
ネットワーク制御	-	7	-
ネットワーク間制御 (CAPWAP 制御、802.11 管理)	48	6	7
音声	46 (EF)	5	6
ビデオ	34 (AF41)	4	5
音声管理	26 (AF31)	3	4
バックグラウンド (ゴールド)	18 (AF21)	2	2
バックグラウンド (ゴールド)	20 (AF22)	2	2
バックグラウンド (ゴールド)	22 (AF23)	2	2
バックグラウンド (シルバー)	10 (AF11)	1	1
バックグラウンド (シルバー)	12 (AF12)	1	1
バックグラウンド (シルバー)	14 (AF13)	1	1
ベスト エフォート	0 (BE)	0	0、3
バックグラウンド	2	0	1
バックグラウンド	4	0	1
バックグラウンド	6	0	1

1. 表に記載されていない DSCP 値に対する IEEE 802.11e UP (ユーザ優先度) 値は、DSCP の上位 (MSB) 3 ビットを考慮して算出されます。たとえば、DSCP 32 (バイナリ 100 000) に対する IEEE 802.11e UP 値は、10 進数に変換される MSB (100) 値で、これは 4 になります。DSCP 32 の 802.11e UP 値は 4 です。

CAPWAP ベースの AP への QoS 機能の展開

WLAN QoS を AP に展開する場合には、次の事項を検討します。

- 有線 CAPWAP AP は、レイヤ 2 CoS (802.1P) 情報の読み書きを実行します。WLC と AP はレイヤ 3 分類 (DSCP) 情報に依存して、WLAN クライアントのトラフィック分類を伝達します。この DSCP 値は中間ルータによって変更される可能性があるため、宛先が受信するレイヤ 2 分類は、CAPWAP トラフィックの送信元でマーキングされたレイヤ 2 分類を示していないことがあります。
- AP では NULL VLAN ID は使用されなくなりました。そのため、レイヤ 2 CAPWAP は、事実上 QoS をサポートしていません。これは、AP が 802.1P/Q タグを送らず、レイヤ 2 CAPWAP にはフォールバックする外部 DSCP がいないためです。
- AP では、フレームを再分類するのではなく、CoS 値または WLAN プロファイルに基づいて優先度を決定します。
- 無線出力ポートに限り EDCF に類似したキューイングを実行します。
- AP では、イーサネット出力ポートでのみ FIFO キューイングを実行します。

WAN QoS と FlexConnect

WLC に転送されるデータトラフィックがある WLAN の場合、動作はハイブリッドリモートエッジ FlexConnect AP 以外の AP と同じです。WMM トラフィックがある、ローカルにスイッチされた WLAN の場合、FlexConnect AP でアップストリームトラフィックに対して dot1q VLAN タグに dot1p 値がマーキングされます。これはネイティブでないタグ付きの VLAN 上でのみ発生します。

ダウンストリーム トラフィックの場合、FlexConnect AP はイーサネット側から受信した dot1q タグを使用して、ローカルにスイッチされた VLAN の無線で WMM 値に対してキューイングとマーキングを行います。

WLAN QoS プロファイルは、アップストリームとダウンストリーム パケットに適用されます。ダウンストリーム トラフィックの場合、デフォルトの WLAN 値より高い 802.1P 値を受信したときには、デフォルトの WLAN 値が使用されます。アップストリームの場合、クライアントがデフォルト WLAN 値より高い WMM 値を送信したときには、デフォルトの WLAN 値が使用されます。WMM 以外のトラフィックの場合、AP からのクライアント フレームには CoS マーキングはありません。

無線 QoS の展開に関するガイドライン

有線ネットワークにおける QoS 展開のルールが、WLAN での QoS 展開にも適用されます。QoS 展開でまず最も重要なガイドラインは、自分のトラフィックを理解することです。プロトコル、遅延に対するアプリケーションの影響度、およびトラフィックの帯域幅について理解してください。QoS によって帯域幅が増えるわけではなく、帯域幅の割り当てに対する制御が強化されるだけです。

LAN スイッチにおける QoS の設定例

AP スイッチの設定

AP スイッチの QoS 設定は、AP から渡される CAPWAP パケットの DSCP を信頼する必要があるため、比較的単純です。AP から送られてくる CAPWAP フレームには CoS のマーキングはありません。次にこの設定の例を示します。この設定では分類のみ行っていることに注意してください。ローカルの QoS ポリシーに応じて、キューイング コマンドを追加できます。

```
interface GigabitEthernet1/0/1
  switchport access vlan 100
  switchport mode access
  mls qos trust dscp
  spanning-tree portfast
end
```

AP DSCP 値を信頼するという点においては、アクセス スイッチは WLC によりその AP に対して設定されたポリシーを信頼しています。クライアント トラフィックに割り当てられた最大 DSCP 値は、その AP 上で WLAN に割り当てられた QoS ポリシーに基づきます。

WLC スイッチの設定

WLC に接続されたスイッチでの QoS 分類決定は、AP に接続されたスイッチの場合よりも少々複雑です。これは、WLC から送られてくるトラフィックの DSCP を信頼するか、CoS を信頼するかの選択が可能のためです。この決定を行う際は、次のことを考慮してください。

- WLC から発信されるトラフィックは、アップストリーム（WLC またはネットワークに送信）か、またはダウンストリーム（AP および WLAN クライアントに送信）です。ダウンストリーム トラフィックは CAPWAP でカプセル化されたものです。アップストリーム トラフィックは、WLC から発信された、CAPWAP でカプセル化またはカプセル開放された WLAN クライアント トラフィックです。
- CAPWAP パケットの DSCP 値は WLC 上の QoS ポリシーによって制御されます。（CAPWAP トンネル ヘッダーによってカプセル化された）WLAN クライアント トラフィックに設定されている DSCP 値は、WLAN クライアントによって設定された値から変更されていません。

- WLC から発信されるフレームの CoS 値は、アップストリームかダウンストリームか、カプセル化かカプセル開放かの別にかかわらず、WLC の QoS ポリシーによって設定されます。

次の例では、WLC の設定の CoS を信頼することを選択しています。これは、この場合、WLAN QoS を集中的に管理できるため、WLC 設定の他に WLC スイッチ接続で追加のポリシーを管理する必要がないためです。

```
interface GigabitEthernet1/0/13
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 11-13,60,61
  switchport mode trunk
  mls qos trust cos
end
```

より詳細な制御が必要な場合は、WLAN クライアントの VLAN 上で QoS 分類ポリシーを実装してください。

トラフィック シェーピング、Over-the-Air QoS および WMM クライアント

トラフィック シェーピングと Over-the-Air QoS は、WLAN WMM 機能がない場合には便利なツールですが、802.11 トラフィックの優先順位付けには直接対応していません。WMM クライアントまたは 792x 端末をサポートする WLAN では、これらのクライアントの WLAN QoS メカニズムに頼ってください。これらの WLAN には、トラフィック シェーピングも Over-the-Air QoS も適用しないでください。

WLAN 音声とシスコの電話機

Cisco Unified Communications エンドポイントのデータ シートは、次のページで入手できます。

http://www.cisco.com/en/US/prod/voicesw/ps6788/ip_phones.html

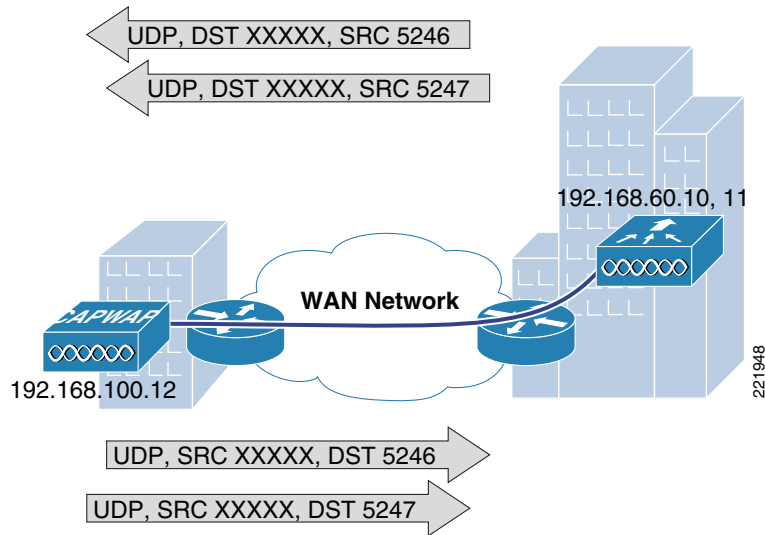
Cisco Jabber の一般的な概要については、次のページを参照してください。

<http://www.cisco.com/web/products/voice/jabber.html>

WAN 接続を介した CAPWAP

ここでは、[図 5-24](#) で示すように CAPWAP AP が WAN リンク上に展開されている場合の QoS 戦略について説明します。

図 5-24 WAN 上の CAPWAP トラフィック



CAPWAP のトラフィック分類

CAPWAP AP は一般的に、次の 2 種類に分類できます。

- CAPWAP コントロールトラフィック：UDP ポート 5246 で識別
- CAPWAP 802.11 トラフィック：UDP ポート 5247 で識別

CAPWAP コントロールトラフィック

CAPWAP コントロールトラフィックはさらに、次の 2 種類に分類できます。

- 初期化トラフィック：CAPWAP AP がブートして CAPWAP システムに接続するときに生成されます。たとえば、コントローラの検出、AP 設定、AP ファームウェアの更新によって生成されるトラフィックなどです。



(注) コントローラからの CAPWAP イメージパケットはベストエフォートとしてマーキングされますが、その確認応答は CS6 としてマーキングされます。この場合、スライディングウィンドウプロトコルが使用されないため、各追加パケットは確認応答を受信してからでないとは送信されないことに注意してください。このタイプのハンドシェイクでは、WAN からのファイルのダウンロードの影響が最小化されます。

- バックグラウンドトラフィック：WLAN ネットワークのメンバとして動作している CAPWAP AP によって生成されます。たとえば、CAPWAP ハートビート、無線リソース管理 (RRM)、不正 AP 測定値などです。バックグラウンド CAPWAP コントロールトラフィックは、CS6 としてマーキングされます。

図 5-24 では、初期 CAPWAP コントロールメッセージの例を示します。初期 CAPWAP コントロールメッセージのリストには、次のものが含まれています。

- CAPWAP discovery メッセージ
- CAPWAP join メッセージ

- CAPWAP コンフィギュレーション メッセージ
- 初期 CAPWAP RRM メッセージ

図 5-25 WISM-2 での CAPWAP 検出要求

```

Frame 5: 162 bytes on wire (1296 bits), 162 bytes captured (1296 bits)
Ethernet II, Src: Cisco_3a:ff:61 (c4:7d:4f:3a:ff:61), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 10.30.0.130 (10.30.0.130), Dst: 255.255.255.255 (255.255.255.255)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00)
  Total Length: 148
  Identification: 0x0011 (3777)
  Flags: 0x02 (Don't Fragment)
  Fragment offset: 0
  Time to live: 255
  Protocol: UDP (17)
  Header checksum: 0x65e8 [correct]
  Source: 10.30.0.130 (10.30.0.130)
  Destination: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: 45048 (45048), Dst Port: capwap-control (5246)
  Source port: 45048 (45048)
  Destination port: capwap-control (5246)
  Length: 128
  Checksum: 0x0000 (none)
Control And Provisioning of Wireless Access Points
  Preamble
  Version: 0
  Type: CAPWAP Header (0)
  Header
  Header Length: 4
  Radio ID: 0
  wireless Binding ID: IEEE 802.11 (1)
  Header flags
  Fragment ID: 0
  Fragment offset: 0
  Reserved: 0
  MAC length: 6
  MAC address: Cisco_49:fe:40 (04:fe:7f:49:fe:40)
  Padding for 4 Byte Alignment: 40
  Control Header

```

CAPWAP 802.11 トラフィック

CAPWAP 802.11 コントロール トラフィックは一般的に、次の 2 つの追加タイプに分類されます。

- 802.11 管理フレーム：プローブ要求やアソシエーション要求および応答などの 802.11 管理フレームは、自動的に CS6 の DSCP として分類されます。
- 802.11 データ フレーム：クライアント データとクライアントからの 802.1X データは、WLAN の QoS 設定に従って分類されますが、WLC から送信される 802.1X フレームを含むパケットは CS4 としてマーキングされます。802.11 データ トラフィック分類は、WLAN 設定に適用されている QoS に依存します。また、自動設定はされません。WLAN データ トラフィックのデフォルトの分類はベストエフォートです。

分類に関する考慮事項

CAPWAP コントロール トラフィックに使用される DSCP 分類は CS6 (IP ルーティング クラス) です。これはボーダー ゲートウェイ プロトコル (BGP)、Open Shortest Path First (OSPF)、Enhanced Interior Gateway Routing Protocol (EIGRP) などの IP ルーティング プロトコルを対象としています。

現在の CAPWAP DSCP 分類では、WLAN システムにとって最適な分類を表現していますが、ユーザ自身の QoS ポリシーやニーズと一致しない可能性があります。

特に、WLAN ネットワークで生成される CS6 に分類されるトラフィックの量を最小限に抑えたい場合があります。場合によっては、プローブ要求などのクライアント アクティビティによる CS6 トラフィックの生成を停止させる必要があります。これを実行するための最も簡単な方法は、CAPWAP 802.11 CS6 トラフィックを、より QoS 優先度の低い DSCP 値に再分類することです。CAPWAP UDP の使用ポートが CAPWAP データの使用ポートと異なるため、ディープ パケット インスペクションの助けを借りなくても、DSCP のデフォルトのマーキングによって、このトラフィックをマーキングしなおすことができます。

また場合によっては、CAPWAP 初期化トラフィックがルーティング トラフィックに絶対に影響しないようにする必要があります。これを実行するための最も簡単な方法は、バックグラウンド レートを超えた CAPWAP コントロール トラフィックに対して、優先度の低いマーキングをすることです。

ルータの設定例

ここでは、CS6 の再マーキングや CAPWAP コントロール トラフィックの負荷に対処する場合のガイドラインとして使用できるルータ設定の例を示します。

この例では、192.168.101.0/24 サブネット上で CAPWAP AP を使用し、AP マネージャを持つ 2 つの WLC を 192.168.60.11 と 192.168.62.11 で使用しています。

クライアントが生成した CS6 パケットの再マーキング

次の例では、CS6 としてマーキングされた CAPWAP データ パケットを、より適切な値である CS3 にマーキングしなおすための設定例を示します。この再マーキングにより、ネットワーク制御のレベルではなくコール制御のレベルで、トラフィックの分類がより適切な分類に変更されます。

```
class-map match-all CAPWAPDATA6
  match access-group 110
  match dscp cs6
!
policy-map CAPWAPDATA6
  class CAPWAPDATA6
    set dscp cs3
!
interface FastEthernet0
  ip address 192.168.203.1 255.255.255.252
  service-policy input CAPWAPDATA6
!
access-list 110 remark CAPWAP Data
access-list 110 permit udp 192.168.101.0 0.0.0.255 host 192.168.60.11 eq 5247
access-list 110 permit udp 192.168.101.0 0.0.0.255 host 192.168.62.11 eq 5247
access-list 111 remark CAPWAP Control
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.60.11 eq 5246
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.62.11 eq 5246
```


定義済みのレートを越えた CAPWAP コントロール トラフィックの DSCP の変更

次の例では、WAN サイトから送られる CAPWAP コントロール トラフィックのレートを制限して、CS6 としてマーキングされたコントロール トラフィックがルーティング トラフィックに及ぼす影響を最小化するための設定例を示します。レート制限の設定では、非準拠のトラフィックがドロップされるのではなく、単に再分類されることに注意してください。



(注)

この設定は例であり、推奨ではありません。普通の状況では、WAN 接続を介した AP の展開の設計ガイドラインに従っていれば、CAPWAP コントロール トラフィックが WAN ルーティング プロトコル接続に影響する可能性はほとんどありません。

```
interface Serial0
  ip address 192.168.202.2 255.255.255.252
  rate-limit output access-group 111 8000 3000 6000 conform-action transmit exceed-action
  set-dscp-transmit 26
access-list 111 remark CAPWAP Control
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.60.11 eq 5246
access-list 111 permit udp 192.168.101.0 0.0.0.255 host 192.168.62.11 eq 5246
!
```

WLAN QoS と 802.11e の詳細については、『*IEEE 802.11 Handbook: A Designer's Companion 2nd Edition*』（Bob O'Hara/Al Petrick 著）を参照してください。ISBN: 978-0-7381-4449-8

