QoS

Quality of Service の設定

QoS について

Quality of Service（QoS）とは、選択したネットワーク トラフィックにさまざまなテクノロジーに渡る優れたサービスを提供する、ネットワークの機能を意味します。QoS の主要な目的は、専用の帯域幅の確保、ジッタおよび遅延の制御（ある種のリアルタイム トラフィックや対話型トラフィックで必要）、および損失特性の改善などを優先的に処理することです。

コントローラでは次の 4 つの QoS レベルがサポートされています。

- Platinum/音声：無線を介して転送される音声のために高品質のサービスを保証します。
- Gold/ビデオ：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：クライアント用に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：ゲスト サービス用に最低帯域幅を提供します。

（注） VoIP クライアントは「Platinum」に設定する必要があります。

QoS プロファイルを使用して各 QoS レベルの帯域幅を設定してから、そのプロファイルを WLAN に適用できます。プロファイル設定は、その WLAN にアソシエートされたクライアントに組み込まれます。また、QoS ロールを作成して、通常ユーザとゲスト ユーザに異なる帯

域幅レベルを指定できます。QoS プロファイルと QoS ロールを設定するには、この項の手順に従ってください。QoS プロファイルを WLAN に割り当てるときは、ユニキャストおよびマルチキャスト トラフィックに対して最大およびデフォルトの QoS レベルを定義することもできます。

ワイヤレス レート制限は、アップストリームおよびダウンストリーム トラフィックの両方に定義できます。レート制限は SSID ごとに定義するか、または最大レート制限としてすべてのクライアントに対して指定できます（あるいは両方を行えます）。これらのレート制限は個別に設定できます。

Quality of Service プロファイルの設定

Platinum、Gold、Silver、および Bronze QoS プロファイルを設定できます。

QoS プロファイルの設定（GUI）

手順

ステップ 1 QoS プロファイルを設定できるように、802.11a および 802.11b/g ネットワークを無効にします。

無線ネットワークを無効にするには、[Wireless] > [802.11a/n/ac]（または [802.11b/g/n]） > [Network] の順に選択し、[802.11a（または 802.11b/g）Network Status] チェックボックスをオフにして、[Apply] をクリックします。

ステップ 2 [Wireless] > [QoS] > [Profiles] の順に選択して [QoS Profiles] ページを開きます。

ステップ 3 設定するプロファイルの名前をクリックして [Edit QoS Profile] ページを開きます。

ステップ 4 [Description] テキスト ボックスの内容を変更して、プロファイルの説明を変更します。

ステップ 5 次の手順で、ユーザごとのデータ レートを定義します。

a) [Average Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとの TCP トラフィックの平均データ レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

b) [Burst Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとの TCP トラフィックのピーク データ レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

（注） バースト データ レートは平均データ レート以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。

バースト データ レートを設定する前に平均データ レートを設定してください。

c) [Average Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとの UDP トラフィックの平均リアルタイム レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

（注） 平均リアルタイム レートがUDPトラフィック用に使用されているとき、平均データ レートはTCP トラフィックの測定に使用されます。すべてのエントリに対してキロビット/秒の単位で測定されます。平均データ レートと平均リアルタイム レートは、TCP や UDP などの上位層プロトコルに適用さているので、これらの値は異なる場合があります。これらの異なるレートの値は帯域幅に影響を与えません。

d) [Burst Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとの UDP トラフィックのピーク リアルタイム レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

（注） バースト リアルタイム レートは平均リアルタイム レート以上でなければなりません。それ以外の場合、QoSポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。

ステップ 6 次の手順で、SSID ごとのデータ レートを定義します。

a) [Average Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、SSID ごとの TCP トラフィックの平均データ レートを定義します。0 の値は、選択したQoSプロファイルで指定された値が有効であることを示します。

b) [Burst Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、SSID ごとの TCP トラフィックのピーク データ レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

（注） バースト データ レートは平均データ レート以上でなければなりません。それ以外の場合、QoSポリシーにより、WLANのトラフィックがブロックされることがあります。

c) [Average Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、SSID ごとの UDP トラフィックの平均リアルタイム レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

d) [Burst Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、SSID ごとの UDP トラフィックのピーク リアルタイム レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

（注） バースト リアルタイム レートは平均リアルタイム レート以上でなければなりません。それ以外の場合、QoSポリシーにより、WLANのトラフィックがブロックされることがあります。

ステップ 7 QoSプロファイルをWLANに割り当てる場合、ユニキャストおよびマルチキャスト トラフィックに対する最大およびデフォルトの QoS レベルを定義します。

a) [Maximum Priority] ドロップダウン リストから、WLAN 内で AP から任意のステーションに送信される任意のデータ フレームに対する最大 QoS 優先度を選択します。

たとえば、ビデオ アプリケーションをターゲットにした「gold」という名前の QoS プロファイルでは、デフォルトで最大優先度が video に設定されます。

b) [Unicast Default Priority] ドロップダウン リストから、WLAN 内で AP から非 WMM ステーションに送信されるユニキャスト データ フレームに対する QoS 優先度を選択します。

c) [Multicast Default Priority] ドロップダウン リストから、WLAN 内で AP からステーションに送信されるマルチキャスト データ フレームに対する QoS 優先度を選択します。

（注） 混合 WLAN 内の非 WMM クライアントに対してデフォルトのユニキャスト優先度を使用することはできません。

ステップ 8 [Protocol Type] ドロップダウン リストから [802.1p] を選択し、[802.1p Tag] テキスト ボックスに最大優先値を入力して、このプロファイルに該当するパケットに関連付けられる優先タグの最大値（0 ～ 7）を定義します。

タグが付けられるパケットには、CAPWAP データ パケット（アクセス ポイントとコントローラの間）や、コア ネットワークに向けて送信されるパケットなどがあります。

（注） 802.1p タギングが設定された QoS プロファイルが、コントローラ上のタグ付けなしのインターフェイスを使用する WLANに割り当てられると、クライアントトラフィックがブロックされます。

ステップ 9 [Apply] をクリックします。

ステップ 10 [Save Configuration] をクリックします。

ステップ 11 802.11 ネットワークを再度有効にします。

無線ネットワークを有効にするには、[Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [Network] の順に選択し、[802.11a（または 802.11b/g）Network Status] チェックボックスをオンにして、[Apply] をクリックします。

ステップ 12 [WLANs] を選択して、WLAN ID を選択し、それに新しい QoS プロファイルを適用します。

ステップ 13 [WLAN] > [Edit] ページで、[QoS]タブに移動し、[Quality of Service] ドロップダウンリストから [QoS Profile] タイプを選択します。QoS プロファイルは、WLAN 単位、無線単位、および AP ベース単位でコントローラに設定されたレート制限値を追加します。

たとえば、5 Mbps のアップストリーム レート制限が Silver タイプの QoS プロファイルに設定されている場合は、Silverプロファイルが割り当てられたすべての WLAN でトラフィックがその WLAN を適用可能な無線単位および AP 単位で 5 Mbps（wlan ごとに 5 Mbps）に制限されます。

ステップ 14 [Apply] をクリックします。

ステップ 15 [Save Configuration] をクリックします。

QoS プロファイルの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、802.11a および 802.11b/g ネットワークを無効にし、QoS プロファイルを設定できるようにします。

config 802.11{a | b} disable network

ステップ 2 次のコマンドを入力して、プロファイルの説明を変更します。

config qos description {**bronze** | **silver** | **gold** | **platinum** }*description*

ステップ 3 次のコマンドを入力して、ユーザまたはSSIDごとのTCPトラフィックの平均データ レートを定義します。

config qos average-data-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

（注） *rate* パラメータには、0 ～ 512,000 Kbps（両端の値を含む）の値を入力できます。値 0 を指定すると、QoS プロファイルに対する帯域幅の制限は行われません。

ステップ 4 このコマンドを入力して、ユーザまたは SSID ごとの TCP トラフィックのピーク データ レートを定義します。

config qos burst-data-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

ステップ 5 次のコマンドを入力して、ユーザまたは SSID ごとの UDP トラフィックの平均リアルタイム データ レートを定義します。

config qos average-realtime-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

ステップ 6 このコマンドを入力して、ユーザまたは SSID ごとの UDP トラフィックのピーク リアルタイム データ レートを定義します。

config qos burst-realtime-rate {**bronze** | **silver** | **gold** | **platinum**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

ステップ 7 QoS プロファイルを WLAN に割り当てる場合、次のコマンドを入力して、ユニキャストおよびマルチキャスト トラフィックに対する最大およびデフォルトの QoS レベルを定義します。

config qos priority {**bronze** | **gold** | **platinum** | **silver**} {*maximum priority*} {*default unicast priority*} {*default multicast priority*}

maximum priority、*default unicast priority*、および *default multicast priority* パラメータは、次のオプションの中から選択します。

- besteffort
- background
- video
- voice

ステップ 8 次のコマンドを入力して、このプロファイルに該当するパケットに関連付けられる優先タグの最大値（0 ～ 7）を定義します。

config qos protocol-type {**bronze** | **silver** | **gold** | **platinum**} **dot1p**

config qos dot1p-tag {**bronze** | **silver** | **gold** | **platinum**} *tag*

タグが付けられるパケットには、CAPWAP データ パケット（アクセス ポイントとコントローラの間）や、コア ネットワークに向けて送信されるパケットなどがあります。

（注） 802.1p タギングは、有線パケットに対してのみ影響します。ワイヤレス パケットは、QoS プロファイルに設定された最大優先レベルによってのみ影響を受けます。

（注） 802.1p タギングが設定された QoS プロファイルが、コントローラ上のタグ付けなしのインターフェイスを使用する WLAN に割り当てられると、クライアント トラフィックがブロックされます。

ステップ 9 次のコマンドを入力して、802.11a および 802.11b/g ネットワークを有効にし、QoS プロファイルを設定できるようにします。

config 802.11{a | b} enable network

ステップ 10 次のコマンドを入力して、新しい QoS プロファイルを WLAN に適用します。

config wlan qos <WLAN ID> {bronze | silver | gold | platinum}

WLAN ごとの QoS プロファイル

QoS プロファイルについて

Cisco UWN ソリューション WLAN では、Platinum/音声、Gold/ビデオ、Silver/ベスト エフォート（デフォルト）、Bronze/バックグラウンドの 4 つのレベルの QoS をサポートしています。音声転送 WLAN で Platinum QoS を使用するよう設定したり、低帯域幅 WLAN で Bronze QoS を使用するよう割り当てたり、その他すべてのトラフィックに残りの QoS レベルを割り当てたりすることができます。

WLAN QoS レベルは、無線トラフィックの特定の 802.11e User Priority（UP）を定義します。この UP は、WMM 以外の有線トラフィックの優先順位を導出すると同時に、さまざまな優先レベルの WMM トラフィックを管理する際の上限値としても機能します。

ワイヤレス レート制限は、アップストリームおよびダウンストリーム トラフィックの両方に定義できます。レート制限は SSID ごとに定義するか、または最大レート制限としてすべてのクライアントに対して指定できます（あるいは両方を行えます）。これらのレート制限は個別に設定できます。

アクセス ポイントは、次の表の値に従ってこの QoS プロファイル固有の UP を使用することで、無線 LAN 上で確認可能な IP DSCP 値を導出します。

表 *1:* アクセス ポイントの *QoS* 変換値

AVVID トラフィック タイプ	AVVID IP DSCP	QoS プロファイル	AVVID 802.1p	IEEE 802.11e UP
ネットワーク制御	56（CS7）	Platinum	7	7

AVVID トラフィック タイプ	AVVID IP DSCP	QoS プロファイル	AVVID 802.1p	IEEE 802.11e UP
ネットワーク間制御（CAPWAP 制御、802.11 管理）	48（CS6）	Platinum	6	7
音声	46（EF）	Platinum	5	6
インタラクティブ ビデオ	34（AF41）	Gold	4	5
ミッションクリティカル	26（AF31）	Gold	3	4
トランザクション	18（AF21）	Silver	2	3
バルク データ	10（AF11）	Bronze	1	2
ベスト エフォート	0（BE）	Silver	0	0
スカベンジャー	2	Bronze	0	1

（注） 表に記載されていない DSCP 値に対する IEEE 802.11e UP 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 進数に相当する MSB（100）値で、これは 4 になります。DSCP 32 の 802.11e UP 値は 4 です。

WLAN への QoS プロファイルの割り当て（GUI）

始める前に

まだ設定していない場合は、「QoS プロファイルの設定（GUI）」セクションの指示に従って 1 つ以上の QoS プロファイルを設定してください。

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 QoS プロファイルを割り当てる WLAN の ID 番号をクリックします。

ステップ 3 [WLANs > Edit] ページが表示されたら、[QoS] タブを選択します。

ステップ 4 [Quality of Service（QoS）] ドロップダウン リストから、次のいずれかを選択します。

- Platinum (音声)
- **Gold（ビデオ）**

- **Silver（ベスト エフォート）**
- Bronze (バックグラウンド)

（注） Silver（ベスト エフォート）がデフォルト値です。

ステップ 5 データ レートをユーザ単位で定義するには、次の手順を実行します。

a) [Average Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、SSID ごとの TCP トラフィックの平均データ レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

b) [Burst Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、SSID ごとの TCP トラフィックのピーク データ レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

（注） バースト データ レートは平均データ レート以上でなければなりません。それ以外の場合、QoS ポリシーにより、WLAN のトラフィックがブロックされることがあります。

c) [Average Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、SSID ごとの UDP トラフィックの平均リアルタイム レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

d) [Burst Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、SSID ごとの UDP トラフィックのピーク リアルタイム レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

（注） バースト リアルタイム レートは平均リアルタイム レート以上でなければなりません。それ以外の場合、QoS ポリシーにより、WLAN のトラフィックがブロックされることがあります。

ステップ 6 データ レートを SSID 単位で定義するには、次の手順を実行します。

a) [Average Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとの TCP トラフィックの平均データ レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

b) [Burst Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとの TCP トラフィックのピーク データ レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

（注） バースト データ レートは平均データ レート以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。

バースト データ レートを設定する前に平均データ レートを設定してください。

c) [Average Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとの UDP トラフィックの平均リアルタイム レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

（注） 平均リアルタイム レートがUDPトラフィック用に使用されているとき、平均データ レートはTCPトラフィックの測定に使用されます。すべてのエントリに対してキロビット/秒の単位で測定されます。平均データ レートと平均リアルタイム レートは、TCPやUDPなどの上位層プロトコルに適用さているので、これらの値は異なる場合があります。これらの異なるレートの値は帯域幅に影響を与えません。

d) [Burst Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとの UDP トラフィックのピーク リアルタイム レートを定義します。0 の値は、選択した QoS プロファイルで指定された値が有効であることを示します。

（注） バースト リアルタイム レートは平均リアルタイム レート以上でなければなりません。それ以外の場合、QoSポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。

ステップ 7 設定を保存します。

WLAN への QoS プロファイルの割り当て（CLI）

まだ設定していない場合は、「QoS プロファイルの設定（CLI）」セクションの指示に従って 1 つ以上の QoS プロファイルを設定してください。

手順

ステップ 1 QoS プロファイルを WLAN に割り当てるには、次のコマンドを入力します。

config wlan qos*wlan_id*{**bronze** |**silver** |**gold** |**platinum**}

Silver がデフォルト値です。

ステップ 2 QoS プロファイルのレート制限パラメータを無効にするには、次のコマンドを入力します。

config wlan override-rate-limit *wlan-id* {**average-data-rate** | **average-realtime-rate** | **burst-data-rate** | **burst-realtime-rate**} {**per-ssid** | **per-client**} {**downstream** | **upstream**} *rate*

ステップ 3 **save config** コマンドを入力します。

ステップ 4 QoS プロファイルを WLAN に適切に割り当てたことを確認するには、次のコマンドを入力します。

show wlan *wlan_id*

以下に類似した情報が表示されます。

```
WLAN Identifier.................................. 1
Profile Name..................................... test
Network Name (SSID).............................. test
Status........................................... Enabled
MAC Filtering.................................... Disabled
Broadcast SSID................................... Enabled
AAA Policy Override.............................. Disabled
Number of Active Clients......................... 0
```

```
Exclusionlist.................................. Disabled
Session Timeout................................ 0
Interface...................................... management
WLAN ACL....................................... unconfigured
DHCP Server.................................... 1.100.163.24
DHCP Address Assignment Required............... Disabled
Quality of Service............................. Silver (best effort)
WMM............................................ Disabled
...
```

QoS のロール

Quality of Service ロールについて

QoS プロファイルを設定して WLAN に適用すると、その WLAN にアソシエートされたクライアントの帯域幅レベルが制限されます。複数の WLAN を同じ QoS プロファイルにマップできますが、通常ユーザ（従業員など）とゲストユーザの間で帯域幅のコンテンションが発生する可能性があります。ゲストユーザが通常ユーザと同じレベルの帯域幅を使用しないようにするには、異なる帯域幅コントラクト（恐らく下位）で QoS ロールを作成して、ゲスト ユーザに割り当てます。

ゲスト ユーザ用に最大 10 個の QoS ロールを設定できます。

（注） RADIUS サーバ上にゲスト ユーザ用のエントリを作成するように選択し、ゲスト ユーザをコントローラからローカル ユーザ データベースに追加するのではなく、Web 認証が実行される WLAN に対して RADIUS 認証を有効にする場合は、QoS ロールをその RADIUS サーバ自体に割り当てる必要があります。これを行うには、*Airespace-Guest-Role-Name* と呼ばれる「guest-role」Airespace 属性と属性識別子の値 11、および文字列のデータ型が、コントローラに設定されている「guest-role」の名前と一致し、RADIUS サーバに追加されている必要があります。この属性は、認証の際にコントローラへ送信されます。RADIUS サーバから返された名前付きのロールがコントローラ上で設定されている場合は、認証が正常に完了した後に、そのロールに関連付けられた帯域幅がゲスト ユーザに適用されます。

AAA パラメータがコントローラで処理される前に、WLAN に *Web* ポリシーのレイヤ 3 セキュリティが設定されていることを確認します。WLAN に *Web* ポリシーのレイヤ 3 セキュリティが設定されていない場合、AAA パラメータは無視されます。

QoS ロールの設定（GUI）

手順

ステップ 1 **[Wireless]** > **[QoS]** > **[Roles]** の順に選択して [QoS Roles for Guest Users] ページを開きます。

このページには、ゲスト ユーザ用の既存の QoS ロールが表示されます。

（注） QoS ロールを削除するには、そのロールの青いドロップダウン矢印の上にカーソルを置いて [Remove] を選択します。

ステップ 2 [New] をクリックして新しい QoS ロールを作成します。[QoS Role Name > New] ページが表示されます。

ステップ 3 [Role Name] テキスト ボックスに、新しい QoS ロールの名前を入力します。この名前は、QoS ユーザのロールを一意で識別できるように付けてください（Contractor、Vendor、など）。

ステップ 4 [Apply] をクリックします。

ステップ 5 QoS ロールの名前をクリックして、QoS ロールの帯域幅を編集します。[Edit QoS Role Data Rates] ページが表示されます。

（注） ユーザごとの帯域幅コントラクトの設定値の影響を受けるのは、ダウンストリーム方向（アクセスポイントからワイヤレス クライアントへ）の帯域幅の大きさのみです。アップストリーム トラフィック（クライアントからアクセス ポイントへ）の帯域幅には影響しません。

ステップ 6 [Average Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとの TCP トラフィックの平均データ レートを定義します。0 ～ 60,000Kbps（両端の値を含む）の値を入力できます。値に 0 を指定すると、QoS ロールに対する帯域幅の制限は行われません。

ステップ 7 [Burst Data Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとの TCP トラフィックのピーク データ レートを定義します。0 ～ 60,000Kbps（両端の値を含む）の値を入力できます。値に 0 を指定すると、QoS ロールに対する帯域幅の制限は行われません。

（注） バースト データ レートは平均データ レート以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。

バースト データ レートを設定する前に平均データ レートを設定してください。

ステップ 8 [Average Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとの UDP トラフィックの平均リアルタイム レートを定義します。0 ～ 60,000Kbps（両端の値を含む）の値を入力できます。値に 0 を指定すると、QoS ロールに対する帯域幅の制限は行われません。

ステップ 9 [Burst Real-Time Rate] テキスト ボックスに Kbps 単位でレートを入力して、ユーザごとの UDP トラフィックのピーク リアルタイム レートを定義します。0 ～ 60,000Kbps（両端の値を含む）の値を入力できます。値に 0 を指定すると、QoS ロールに対する帯域幅の制限は行われません。

（注） バーストリアルタイム レートは平均リアルタイム レート以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。

ステップ 10 [Apply] をクリックします。

ステップ 11 [Save Configuration] をクリックします。

ステップ 12 「コントローラに対するローカル ネットワーク ユーザの設定（GUI）」の項の説明に従って、QoS ロールをゲスト ユーザに適用します。

QoS ロールの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、ゲスト ユーザ用の QoS ロールを作成します。

config netuser guest-role create *role_name*

（注） QoS ロールを削除する場合は、**config netuser guest-role delete** *role_name* コマンドを入力します。

ステップ 2 次のコマンドを入力して、QoS ロール用の帯域幅コントラクトを設定します。

- **config netuser guest-role qos data-rate average-data-rate** *role_name rate*：TCP トラフィックの平均データ レートをユーザ単位で設定します。
- **config netuser guest-role qos data-rate burst-data-rate** *role_name rate*：TCP トラフィックのピーク データ レートをユーザ単位で設定します。

  （注） バースト データ レートは平均データ レート以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。

- **config netuser guest-role qos data-rate average-realtime-rate** *role_name rate*：UDP トラフィックの平均リアルタイム レートをユーザ単位で設定します。
- **config netuser guest-role qos data-rate burst-realtime-rate** *role_name rate*：UDP トラフィックのピーク リアルタイム レートをユーザ単位で設定します。

  （注） バースト リアルタイム レートは平均リアルタイム レート以上でなければなりません。それ以外の場合、QoS ポリシーにより、ワイヤレス クライアントとのトラフィックがブロックされることがあります。

（注） このコマンドの *role_name* パラメータには、新しい QoS ロールの名前を入力します。この名前は、QoS ユーザのロールを一意で識別できるように付けてください（Contractor、Vendor、など）。*rate* パラメータには、0 ～ 60,000 Kbps（両端の値を含む）の値を入力できます。値に 0 を指定すると、QoS ロールに対する帯域幅の制限は行われません。

ステップ 3 次のコマンドを入力して、ゲスト ユーザに QoS ロールを適用します。

config netuser guest-role apply *username role_name*

たとえば、*Contractor* のロールをゲスト ユーザ *jsmith* に適用するとします。

（注） ゲスト ユーザに QoS ロールを割り当てない場合は、[User Details] の [Role] テキスト ボックスにロールが "default" と表示されます。このユーザの帯域幅コントラクトは、WLAN の QoS プロファイルで定義されます。

（注） ゲスト ユーザの QoS ロールの割り当てを解除する場合は、**config netuser guest-role apply** *username* **default command** を入力します。今後、このユーザについては WLAN の QoS プロファイルで定義された帯域幅コントラクトが使用されます。

ステップ 4 次のコマンドを入力して、変更を保存します。

save config

ステップ 5 次のコマンドを入力して、現在の QoS ロールとそれらの帯域幅パラメータの一覧を表示します。

show netuser guest-roles

以下に類似した情報が表示されます。

```
Role Name..................................... Contractor
     Average Data Rate........................ 10
     Burst Data Rate.......................... 10
     Average Realtime Rate.................... 100
     Burst Realtime Rate...................... 100

Role Name..................................... Vendor
     Average Data Rate........................ unconfigured
     Burst Data Rate.......................... unconfigured
     Average Realtime Rate.................... unconfigured
     Burst Realtime Rate..................... unconfigured
```

QoS マッピングの設定

QoS マップについて

QoS マップ機能は、アプリケーション タイプと一致する適切な QoS マーキングがクライアントやアプリケーションによってマークされていない状況で QoS ポリシーを維持します。管理者は DiffServ コードポイント（DSCP）をユーザ優先度（UP）の値にマッピングすることができ、UP から Cisco WLC の DSCP にもマークすることができます。

QoS が有効な場合、QoS 機能は、フレームの AP がアドバタイズします。ネットワークとの関連付けや再度の関連付けの際、フレームを介して互換性のあるデバイスにマップが伝えられます。

QoS が無効な場合、Cisco WLC から AP とクライアントにデフォルトのマップが伝えられます。

この機能は、すべての Cisco AP モデルがサポートしています。

QoS マップの制約事項

- QoS マップ機能は Cisco WLC GUI では設定できません
- QoS マップはこの機能が無効な状態な場合にのみ設定できます。
- この機能は、801.11u 以外のサポート対象ハードウェアでは機能しません。QoS マップを持つフレームはこれらにクライアントに送信されませんが、これらのクライアントにより送信されたパケットは、設定した DSCP-UP マップに従います
- QoS マップが有効になる前にすべての UP 値を 0 ～ 7 の値で設定します
- 各ユーザ優先度の DSCP 範囲が重複していないことを確認します
- DSCP の上限値が DSCP の下限値以上であることを確認します
- 最大 21 個の例外を設定できます
- QoS マップを有効にする前にネットワークを無効にする必要があります

QoS マップの設定（GUI）

始める前に

QoS マップの設定を変更する場合は、QoS マップを無効にすることをお勧めします。QoS マップを無効にすると、DSCP 値は自動的にデフォルト値にリセットされます。

（注）
- 値を設定後、QoS マップを有効にするには、次の条件を満たす必要があります。
  - すべての UP 値を設定している。
  - UP 値の DSCP 範囲がオーバーラップしていない。たとえば、UP1 の値の範囲が 10 ～ 20 の場合は、その他の UP 値の範囲に 10 ～ 20 の数字を使用しないでください。

手順

ステップ 1 802.11a/n/ac ネットワークと 802.11b/g/n ネットワークを無効にして、QoS マップを設定できるようにします。

無線ネットワークを無効にするには、[Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [Network] を選択し、[802.11a（または 802.11b/g）Network Status] チェックボックスをオフにして [Apply] をクリックします。

ステップ 2 **[Wireless]** > **[QoS]** > **[QoS Map]** の順に選択して、[QoS map] ページを開きます。

ステップ 3 QoS マップ機能を無効にするには、次の手順を実行します。

1. [QoS Map] ドロップダウンリストから、[Disable] を選択します。
2. DSCP の例外値をリセットするには、[Default] オプションを選択します。

   [Default] オプションを選択すると、UP to DSCP テーブルと DSCP to UP テーブルの値が 255 にリセットされます。また、DSCP UP 例外が存在しなければ追加します。

ステップ 4 [UP to DSCP Map] を変更するには、次の手順を実行します。

1. [User Priority] ドロップダウンリストから値を選択します。
2. [DSCP Default]、[DSCP Start]、[DSCP End] の値を入力します。
3. [Modify] をクリックします。

ステップ 5 DSCP 例外を作成するには、次の手順を実行します。

1. [DSCP Exception] 値を入力します。
2. [User Priority] ドロップダウンリストから値を選択します。
3. [Add] をクリックします。

ステップ 6 DSCP 例外を削除するには、その DSCP 例外の青いドロップダウン矢印にマウス オーバーして、[Remove] をクリックします。

処理を確認するプロンプトが表示されたら、[OK] をクリックします。

ステップ 7 DSCP 例外リストをクリアするには、[Clear ALL] をクリックします。

ステップ 8 [Trust DSCP UpStream] チェックボックスをオン/オフして、アップストリーム パケットのマーキング有効または無効にします。

ステップ 9 QoS マップ機能を有効にするには、[QoS Map] ドロップダウンリストから [Enable] を選択します。

ステップ 10 [Apply] をクリックします。

ステップ 11 802.11 ネットワークを再度有効にします。

無線ネットワークを有効にするには、[Wireless] > [802.11a/n/ac] または [802.11b/g/n] > [Network] を選択し、[802.11a（または 802.11b/g）Network Status] チェックボックスをオンにします。

ステップ 12 設定を保存します。

QoS マップの設定（CLI）

手順

- 次のコマンドを入力して、有効化、無効化、デフォルト マップに戻します。

  config qos qos-map {**enable** | **disable** | **default**}

  default コマンドは、UP to DSCP テーブルと DSCP to UP テーブルをデフォルト値 (255) にリセットします。また、DSCP UP 例外が存在しなければ追加します。

- 次のコマンドを入力して、UP に対する DSCP 範囲を設定します。

  config qos qosmap up-to-dscp-map *up dscp-default dscp-start dscp-end*

  上記のコマンドは以下の状況で実行できます。

  - クライアントが QoS マップをサポートし、DSCP または UP を異常な値とクライアントでマークする場合
  - クライアントが QoS マップをサポートしていない場合。管理者は、特定の UP をクライアント パケットの DSCP アップストリームとダウンストリームにマッピングできます

- 次のコマンドを入力して、DSCP の例外を設定します。

  config qos qosmap dscp-up-to-exception *dscp up*

  上記のコマンドは、クライアントが DSCP を異常な値でマークする状況で実行できます。

- 次のコマンドを入力して、特定の DSCP 例外を削除します。

  config qos qosmap delete-dscp-exception *dscp*

  上記のコマンドは、特定の例外を QoS マップから削除する場合に実行できます。

- 次のコマンドを入力して、すべての例外を削除します。

  config qos qosmap clear-all

上記のコマンドは、すべての値をマップからクリアする必要がある場合に実行できます。

- 次のコマンドを入力して、クライアント DSCP を使用したアップストリーム パケットのマーキングを有効または無効にします。

  config qos qosmap trust-dscp-upstream {**enable** | **disable** }

  上記のコマンドは、クライアントが DSCP をマークして UP をマークしないか、UP を異常な値にマークする状況で実行できます。有効な状態では、AP で UP ではなく DSCP を使用してアップストリーム パケットをマークします。

- 次のコマンドを入力して、QoS マッピング設定を表示します。

  show qos qosmap

Fastlane QoS

Fastlane QoS の設定（CLI）

Fastlane QoS 機能は、iOS 10 以降のクライアントに向上した Quality of Service（QoS）処理を提供します。この機能はデフォルトで無効に設定されています。

（注） すべての WLAN とネットワークを無効にし、再度有効にするとサービスが中断されるため、あまり多くのクライアントが接続していないメンテナンス時のみこの機能を有効または無効にしてください。

Fastlane QoS の制約事項

- WLAN で Flex ローカル スイッチングが有効になっているときにデフォルト Flex AVC プロファイルがありません作成され、AUTOQOS AVC-プロファイル、中央スイッチング用に作成され、WLAN にマッピングとは異なり、WLAN にマッピングされています。

WLAN ごとの Fastlane QoS の有効化

WLAN ごとに Fastlane QoS 機能を有効にするには、**config qos fastlane enable** *wlan_id* コマンドを使用します。

config qos fastlane enable *wlan_id* コマンドを実行すると、ターゲットの WLAN で FastlaneQoS がアクティブになり、サポート対象の iOS 10 デバイスがそれぞれのプロファイルに含まれる QoS ホワイトリスト（存在する場合）をアクティブにできます。また、このコマンドにより次の表に記載されているコマンドが実行されます。

（注） コマンドが実行されると、Fastlane QoS 機能が有効になり、ターゲットの WLAN に適用されます。Fastlane QoS 機能に関連付けられているコマンドが、Fastlane QoS 機能が WLAN で有効な場合に失敗すると、QoS マップを除くすべての変更は元の値に戻ります。QoS マップ値は以前の設定値ではなく、デフォルト値に戻ります。また、新しい AVC プロファイルは削除されません。これは WLAN からのみ削除されます。

表 *2 : Fastlane QoS* を有効にするために実行されるコマンド

説明	コマンド
一時的に 802.11a および 802.11b ネットワークおよび WLAN を無効にします。	• **config 802.11a disable network** • **config 802.11b disable network** • **config wlan disable all**
Wi-Fi リンクを介したベスト エフォートのために、マークが付けられていない（ベスト エフォート）ユニキャスト パケット、およびマルチキャスト パケットを設定するための Platinum QoS プロファイルを設定します。	• **config qos priority platinum voice besteffort besteffort**
802.1p マーキングを無効にします（すべての有線マーキングは DSCP 対応です）。	• **config qos protocol-type platinum none**
UDP トラフィックの帯域幅制限を無効にします。	• **config qos average-realtime-rate platinum per-ssid downstream 0**
UDP のバーストの帯域幅制限を無効にします。	• **config qos burst-realtime-rate platinum per-ssid downstream 0**
5 GHz と 2.4 GHz の ACM を有効にします。	• **config 802.11a cac voice acm enable** • **config 802.11b cac voice acm enable**
5 GHz または 2.4 GHz 無線で使用可能な帯域幅の 50 % に音声トラフィックの割り当てを制限します。	• **config 802.11a cac voice max-bandwidth 50** • **config 802.11b cac voice max-bandwidth 50**
音声ユーザのローミング用に帯域幅の 6 % を割り当てます。	• **config 802.11a cac voice roam-bandwidth 6** • **config 802.11b cac voice roam-bandwidth 6**
EDCA パラメータの値を 802.11-2017 の推奨値に設定します。	• **config advanced 802.11b edca-parameter fastlane** • **config advanced 802.11a edca-parameter fastlane**

説明	コマンド
5 GHz と 2.4 GHz 優先帯域幅を有効にします。	• **config 802.11a exp-bwreq enable** • **config 802.11b exp-bwreq enable**
ユーザ優先度（UP）を DiffServ コードポイント（DSCP）マップへ設定します。	• **config qos qosmap disable** • **config qos qosmap default** • **config qos qosmap up-to-dscp-map 0 0 0 7** • **config qos qosmap up-to-dscp-map 1 8 8 15** • **config qos qosmap up-to-dscp-map 2 16 16 23** • **config qos qosmap up-to-dscp-map 3 24 24 31** • **config qos qosmap up-to-dscp-map 4 32 32 39** • **config qos qosmap up-to-dscp-map 5 34 40 47** • **config qos qosmap up-to-dscp-map 6 46 48 62** • **config qos qosmap up-to-dscp-map 7 56 63 63** • **config qos qosmap clear all**

説明	コマンド
DSCP 対 UP のマッピング例外を設定します。	

説明	コマンド
	• **config qos qosmap dscp-to-up-exception 56 0** • **config qos qosmap dscp-to-up-exception 48 0** • **config qos qosmap dscp-to-up-exception 46 6** • **config qos qosmap dscp-to-up-exception 44 6** • **config qos qosmap dscp-to-up-exception 40 5** • **config qos qosmap dscp-to-up-exception 38 4** • **config qos qosmap dscp-to-up-exception 36 4** • **config qos qosmap dscp-to-up-exception 34 4** • **config qos qosmap dscp-to-up-exception 32 5** • **config qos qosmap dscp-to-up-exception 30 4** • **config qos qosmap dscp-to-up-exception 28 4** • **config qos qosmap dscp-to-up-exception 26 4** • **config qos qosmap dscp-to-up-exception 24 4** • **config qos qosmap dscp-to-up-exception 22 3** • **config qos qosmap dscp-to-up-exception 20 3** • **config qos qosmap dscp-to-up-exception 18 3** • **config qos qosmap dscp-to-up-exception 16 0** • **config qos qosmap dscp-to-up-exception 14 2** • **config qos qosmap dscp-to-up-exception 12 2**

説明	コマンド
	• **config qos qosmap dscp-to-up-exception 10 2** • **config qos qosmap dscp-to-up-exception 8 1**
DSCP-Trust（新しい QoS マップ）を有効にします。	• **config qos qosmap trust-dscp-upstream enable** • **config qos qosmap enable**
Application Visibility and Control（AVC）プロファイルを作成します。	• **config avc profile AUTOQOS-AVC-PROFILE create**
音声アプリケーションおよびサブコンポーネントを Expedited Forwarding（EF; 完全優先転送）にマーキングするよう AVC を設定します（DSCP 46）。	• **config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-phone-audio mark 46** • **config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-jabber-audio mark 46** • **config avc profile AUTOQOS-AVC-PROFILE rule add application ms-lync-audio mark 46** • **config avc profile AUTOQOS-AVC-PROFILE rule add application citrix-audio mark 46**
マルチメディア会議アプリケーションを相対的優先転送（AF）41 にマーキングするよう AVC を設定します（DSCP 34）。	• **config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-phone-video mark 34** • **config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-jabber-video mark 34** • **config avc profile AUTOQOS-AVC-PROFILE rule add application ms-lync-video mark 34** • **config avc profile AUTOQOS-AVC-PROFILE rule add application webex-media mark 34**

説明	コマンド
マルチメディア ストリーミング アプリケーションを AF31 にマーキングするよう AVC を設定します（DSCP 26）。	• **config avc profile AUTOQOS-AVC-PROFILE rule add application citrix mark 26** • **config avc profile AUTOQOS-AVC-PROFILE rule add application pcoip mark 26** • **config avc profile AUTOQOS-AVC-PROFILE rule add application vnc mark 26** • **config avc profile AUTOQOS-AVC-PROFILE rule add application vnc-http mark 26**
シグナリング プロトコルを CS3 にマーキングするよう AVC を設定します（DSCP 24）。	• **config avc profile AUTOQOS-AVC-PROFILE rule add application skinny mark 24** • **config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-jabber-control mark 24** • **config avc profile AUTOQOS-AVC-PROFILE rule add application sip mark 24** • **config avc profile AUTOQOS-AVC-PROFILE rule add application sip-tls mark 24**
トランザクションデータ アプリケーションを AF21 にマーキングするよう AVC を設定します（DSCP 18）。	• **config avc profile AUTOQOS-AVC-PROFILE rule add application cisco-jabber-im mark 18** • **config avc profile AUTOQOS-AVC-PROFILE rule add application ms-office-web-apps mark 18** • **config avc profile AUTOQOS-AVC-PROFILE rule add application salesforce mark 18** • **config avc profile AUTOQOS-AVC-PROFILE rule add application sap mark 18**

説明	コマンド
OAM アプリケーションを CS2 にマーキングするよう AVC を設定します（DSCP 16）。	• **config avc profile AUTOQOS-AVC-PROFILE rule add application dhcp mark 16** • **config avc profile AUTOQOS-AVC-PROFILE rule add application dns mark 16** • **config avc profile AUTOQOS-AVC-PROFILE rule add application ntp mark 16** • **config avc profile AUTOQOS-AVC-PROFILE rule add application snmp mark 16**
バルク データ アプリケーションを AF11 にマーキングするよう AVC を設定します（DSCP 10）。	• **config avc profile AUTOQOS-AVC-PROFILE rule add application ftp mark 10** • **config avc profile AUTOQOS-AVC-PROFILE rule add application ftp-data mark 10** • **config avc profile AUTOQOS-AVC-PROFILE rule add application ftps-data mark 10** • **config avc profile AUTOQOS-AVC-PROFILE rule add application cifs mark 10**
スカベンジャのアプリケーションをCS1にマーキングするよう AVC を設定します（DSCP 8）。	• **config avc profile AUTOQOS-AVC-PROFILE rule add application netflix mark 8** • **config avc profile AUTOQOS-AVC-PROFILE rule add application youtube mark 8** • **config avc profile AUTOQOS-AVC-PROFILE rule add application skype mark 8** • **config avc profile AUTOQOS-AVC-PROFILE rule add application bittorrent mark 8**
Platinum QoS プロファイルを WLAN に適用します。	• **config wlan qos** *wlan_id* **platinum**

説明	コマンド
AVC の表示が WLAN で有効な場合、AVC プロファイル AUTOQOS-AVC-PROFILE を WLAN ID *wlan-id* に適用します。	• **config wlan avc** *wlan_id***profile AUTOQOS-AVC-PROFILE enable**
802.11a および 802.11b ネットワークと WLAN を再度有効にします。	• **config 802.11a enable network** • **config 802.11b enable network** • **config wlan enable all**

WLAN での Fastlane QoS の無効化

WLAN の Fastlane QoS を無効にするには、**config qos fastlane disable** *wlan_id* コマンドを使用します。

ターゲット WLAN の Fastlane を無効にすると、サポート対象 iOS 10 デバイスはその WLAN に対する QoS ホワイトリストの使用を停止します。ターゲット WLAN の Fastlane を無効にすると、WLAN の設定も QoS のデフォルト値にもどります（次の表を参照）。

（注） Fastlane QoS 機能が WLAN ごとに無効になると、すべての値がデフォルト状態に戻ります。ただし、WLAN の状態は以前の状態に戻ります。

WLAN で Fastlane QoS を無効にし、メディア ストリームが有効の場合、Silver プロファイルを QoS に有効にする前に無効になります。

表 *3 : WLAN* で *Fastlane QoS* を無効にするために実行されるコマンド

説明	コマンド
WLAN設定を変更するためにWLANを無効にします。 （注） コール スヌーピングおよび KTS が有効になっている場合、それらは無効になります。	• **config wlan disable** *wlan_id*
Silver（デフォルト）QoS プロファイルを WLAN に適用します。	• **config wlan qos** *wlan_id* **silver**
接続されている場合、WLAN ID *wlan-id* から AVC プロファイル AUTOQOS-AVC-PROFILE を削除します。	• **config wlan avc** *wlan_id* **profile AUTOQOS-AVC-PROFILE disable**

説明	コマンド
WLANを以前の状態に戻します（WLANが有効な状態だった場合、有効な状態に戻り、WLAN が無効な状態だった場合、無効な状態に戻ります）。	• **config wlan enable** *wlan_id*

Fastlane QoS のグローバルな無効化

Fastlane QoS をグローバルに無効にするには、**config qos fastlane disable global** コマンドを使用します。

Fastlane QoS 機能をグローバルに無効にすると、WLC QoS の設定は次の表に示されているデフォルト値に戻ります。

（注） **config qos fastlane disable global** コマンドを実行する前に、すべての WLAN で Fastlane QoS を無効にする必要があります。

Fastlane QoS 機能に関連付けられたコマンドがグローバルに有効な場合に、失敗する場合、すべての変更は元の値に戻ります。ただし、QoSマップは以前の設定値ではなく、デフォルト値に戻ります。

表 *4 : Fastlane QoS* をグローバルに無効にするために実行されるコマンド

説明	コマンド
QoSプロファイルに変更を加えるため、802.11aと802.11bネットワークを一時的に無効にします。	• **config 802.11a disable network** • **config 802.11b disable network**
QoS プロファイルに変更を加えるため、すべての WLAN を無効にします。	• **config wlan disable all**
PlatinumQoSプロファイルをデフォルトのQoS設定に戻します。	• **config qos priority platinum voice voice voice** • **config qos protocol-type platinum none** • **config qos average-realtime-rate platinum per-ssid downstream 0** • **config qos burst-realtime-rate platinum per-ssid downstream 0**

説明	コマンド
2.4 GHz と 5 GHz の ACM を無効にします。また、ビデオCACをデフォルト値に戻します。	• **config 802.11a cac voice acm disable** • **config 802.11b cac voice acm disable** • **config 802.11a cac video max-bandwidth 5** • **config 802.11b cac video max-bandwidth 5**
音声トラフィックを 2.4 GHz と 5 GHz の合計帯域幅のデフォルト値に制限します。	• **config 802.11a cac voice max-bandwidth 75** • **config 802.11b cac voice max-bandwidth 75**
音声ユーザのローミング帯域幅をデフォルト値に戻します。	• **config 802.11a cac voice roam-bandwidth 6** • **config 802.11b cac voice roam-bandwidth 6**
EDCAパラメータをデフォルト値に戻します。	• **config advanced 802.11b edca-parameter wmm-default** • **config advanced 802.11a edca-parameter wmm-default**
5 GHz と 2.4 GHz 優先帯域幅を無効にします。	• **config 802.11a exp-bwreq disable** • **config 802.11b exp-bwreq disable**
UP 対 DSCP マップを無効にします。	• **config qos qosmap disable** • **config qos qosmap default**
802.11a および 802.11b ネットワークを再度有効にします。	• **config 802.11a enable network** • **config 802.11b enable network**
WLANを以前の状態に戻します（WLANが有効な状態だった場合は有効な状態に戻り、WLAN が無効な状態だった場合は無効な状態に戻ります）。	**config wlan enable *wlan-id***

Fastlane QoS の設定（GUI）

手順

ステップ 1 [WLANs] を選択して、[WLANs] ウィンドウを開きます。

ステップ 2 [QoS] を選択して、[WLANs] > [Edit] ウィンドウを開きます。

ステップ 3 [Fastlane] ドロップダウン リストから、Fastlane QoS を有効または無効にします。

ステップ 4 [Apply] をクリックして設定値を保存します。

Fastlane QoS のグローバルな無効化（GUI）

手順

ステップ 1 [Wireless] > [Advanced] > [QoS] > [Fastlane] の順に選択して、[Fastlane Configuration] ウィンドウを開きます。

ステップ 2 [Revert Fastlane AutoQoS global parameters to defaults] で [Apply] をクリックし、Fastlane をグローバルに無効にします。

メディアと EDCA

アグレッシブ ロード バランシング

アグレッシブ ロード バランシングの 設定について

コントローラ上でアグレッシブ ロード バランシングを有効にすると、ワイヤレス クライアントの負荷を Lightweight アクセス ポイント間で分散することができます。アグレッシブ ロード バランシングはコントローラを使用して有効にできます。

（注） クライアントの負荷は、同じコントローラ上のアクセス ポイント間で分散されます。別のコントローラ上のアクセス ポイントとの間では、ロード バランシングは行われません。

ワイヤレス クライアントが Lightweight アクセス ポイントへのアソシエートを試みると、アソシエーション応答パケットとともに 802.11 応答パケットがクライアントに送信されます。この 802.11 応答パケットの中にステータス コード 17 があります。コード 17 は AP がビジー状態であることを示します。AP のしきい値に達成しなければ、AP からは「success」を示すアソシエーション応答は返りません。AP 使用率のしきい値を超えると、コード 17（AP ビジー）が返り、処理能力に余裕がある別の AP がクライアント要求を受け取ります。

たとえば、AP1 上のクライアント数が、AP2 のクライアント数とロード バランシング ウィンドウの和を上回っている場合は、AP1 の負荷は AP2 よりも高いと判断されます。クライアントが AP1 にアソシエートしようとすると、ステータス コード 17 が含まれている 802.11 応答パケットがクライアントに送信されます。アクセス ポイントの負荷が高いことがこのステータス コードからわかるので、クライアントは別のアクセス ポイントへのアソシエーションを試みます。

コントローラは、クライアントアソシエーションを10回まで拒否するように設定できます（クライアントがアソシエーションを 11 回試みた場合、11 回目の試行時にアソシエーションが許可されます）。また、特定の WLAN 上でロード バランシングを有効にするか、無効にするかも指定できます。これは、特定のクライアント グループ（遅延に敏感な音声クライアントなど）に対してロード バランシングを無効にする場合に便利です。

（注） 300 ミリ秒を超えて遅延を設定すると、音声クライアントは認証しません。これを避けるには、中央認証（CCKM による WLAN のローカル スイッチング）を設定し、さらに AP と WLC 間に遅延 600 ms（UP と DOWN それぞれ 300 ms）の Pagent ルータを設定して、音声クライアントをアソシエートします

パッシブ スキャン クライアントは、ロード バランシングが有効か無効かに関係なく、AP に関連付けられます。

（注） Cisco 600 シリーズ OfficeExtend アクセス ポイントはクライアント ロード バランシングをサポートしません。

7.4 リリースでは、FlexConnect アクセス ポイントはクライアント ロードバランシングをサポートします。

隣接 AP の WAN インターフェイスの使用率を分析するようにコントローラを設定して、負荷が軽い AP 間のクライアントをロード バランスすることができます。これを設定するには、ロード バランシングしきい値を定義します。しきい値を定義することによって、WAN インターフェイスの使用率（%）を測定できます。たとえば、50 というしきい値を設定すると、AP-WAN インターフェイスで 50% 以上の使用率を検出した場合にロード バランシングがトリガされます。

（注） FlexConnect AP の場合は、アソシエーションがローカルに処理されます。ロードバランシングの判断は、Cisco WLC で行われます。FlexConnect AP は、Cisco WLC の計算結果を確認する前に、まず、クライアントに応答を返します。FlexConnect AP がスタンドアロン モードの場合は、ロード バランシングが適用されません。

FlexConnect AP は、ローカル モードの AP と同様にロード バランシング用のステータス 17 で（再）アソシエーション応答を送信しません。代わりに、ステータス 0（成功）で（再）アソシエーションを送信してから、理由 5 で認証解除を送信します。

アグレッシブなロード バランシングの設定（GUI）

手順

ステップ 1 **[Wireless]** > **[Advanced]** > **[Load Balancing]** を選択して、[Load Balancing] ページを開きます。

ステップ 2 [Client Window Size] テキスト ボックスに、1 ～ 20 の値を入力します。

このウィンドウ サイズは、アクセス ポイントの負荷が高すぎてそれ以上はクライアント アソシエーションを受け付けることができないかどうかを判断するアルゴリズムで使用されます。

ロード バランシング ウィンドウ + 最も負荷が低いアクセス ポイント上のクライアント アソシエーション数 = ロード バランシングしきい値

特定のクライアント デバイスからアクセス可能なアクセス ポイントが複数ある場合に、アクセス ポイントはそれぞれ、アソシエートしているクライアントの数が異なります。クライアントの数が最も少ないアクセス ポイントは、負荷が最も低くなります。クライアント ウィンドウ サイズと、負荷が最も低いアクセス ポイント上のクライアント数の合計がしきい値となります。クライアント アソシエーションの数がこの閾値を超えるアクセス ポイントはビジー状態であるとみなされ、クライアントがアソシエートできるのは、クライアント数が閾値を下回るアクセス ポイントだけとなります。

ステップ 3 [Maximum Denial Count] テキスト ボックスに、0 ～ 10 の値を入力します。

拒否数は、ロード バランシング中のアソシエーション拒否の最大数を設定します。

ステップ 4 [Apply] をクリックします。

ステップ 5 [Save Configuration] をクリックします。

ステップ 6 特定の WLAN 上でアグレッシブ ロード バランシングを有効または無効にするには、次の手順を実行します。

a) **[WLANs]** > **[WLAN ID]** を選択します。[WLANs > Edit] ページが表示されます。
b) [Advanced] タブで、[Client Load Balancing] チェックボックスをオンまたはオフにします。
c) [Apply] をクリックします。
d) [Save Configuration] をクリックします。

アグレッシブなロード バランシングの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、アグレッシブ ロード バランシング用のクライアント ウィンドウを設定します。

config load-balancing window *client_count*

client_count パラメータには、0 ～ 20 の範囲内の値を入力できます。

ステップ 2 次のコマンドを入力して、ロード バランシング用の拒否回数を設定します。

config load-balancing denial *denial_count*

denial_count パラメータには、1 ～ 10 の範囲内の値を入力できます。

ステップ 3 次のコマンドを入力して、変更を保存します。

save config

ステップ 4 次のコマンドを入力して、特定の WLAN 上のアグレッシブ ロード バランシングを有効または無効にします。

config wlan load-balance allow {**enable** | **disable**} *wlan_ID*

wlan_ID パラメータには、1 ～ 512 の範囲内の値を入力できます。

ステップ 5 次のコマンドを入力して、設定を確認します。

show load-balancing

ステップ 6 次のコマンドを入力して、変更を保存します。

save config

ステップ 7 次のコマンドを入力して、WLAN のロード バランシング モードを設定します。

config wlan load-balance mode {*client-count* | *uplink-usage*} *wlan-id*

この機能では、APがコントローラにアップリンクの使用状況の統計情報を定期的にアップロードする必要があります。次のコマンドを入力して、これらの統計を確認してください。

show ap stats system *cisco-AP*

メディア セッションとスヌーピング

メディア セッション スヌーピングおよびレポートについて

この機能により、アクセス ポイントは Session Initiation Protocol（SIP）の音声コールの確立、終了、および失敗を検出し、それをコントローラおよびCisco Prime Infrastructureにレポートできます。各 WLAN に対して、Voice over IP （VoIP）のスヌーピングおよびレポートを有効または無効にできます。

VoIP Media Session Aware（MSA）スヌーピングを有効にすると、この WLAN をアドバタイズするアクセス ポイント無線は、SIP RFC 3261 に準拠する SIP 音声パケットを検索します。非 RFC 3261 準拠の SIP 音声パケットや Skinny Call Control Protocol（SCCP）音声パケットは検索しません。ポート番号 5060 に宛てた、またはポート番号 5060 からの SIP パケット（標準的な SIP シグナリング ポート）はいずれも、詳細検査の対象として考慮されます。アクセス ポイントでは、Wi-Fi Multimedia（WMM）クライアントと非 WMM クライアントがコールを確立している段階、コールがアクティブになった段階、コールの終了処理の段階を追跡します。両方のクライアント タイプのアップストリーム パケット分類は、アクセス ポイントで行われます。ダウンストリーム パケット分類は、WMM クライアントはコントローラで、非 WMM クライ

アントはアクセス ポイントで行われます。アクセス ポイントは、コールの確立、終了、失敗など、主要なコール イベントをコントローラと Cisco Prime Infrastructure に通知します。

VoIP MSA コールに関する詳細な情報がコントローラによって提供されます。コールが失敗した場合、コントローラはトラブルシューティングで有用なタイムスタンプ、障害の原因（GUI で）、およびエラー コード（CLI で）が含まれるトラップ ログを生成します。コールが成功した場合、追跡用にコール数とコール時間を表示します。Cisco Prime Infrastructure の [Event] ページに、失敗した VoIP コール情報が表示されます。

メディア セッション スヌーピングおよびレポートの制約事項

コントローラ ソフトウェア リリース 6.0 以降では、Voice over IP（VoIP）Media Session Aware（MSA）スヌーピングおよびレポートをサポートしています。

メディア セッション スヌーピングの設定（GUI）

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 メディア セッション スヌーピングを設定する WLAN の ID 番号をクリックします。

ステップ 3 [WLANs > Edit] ページで [Advanced] タブをクリックします。

ステップ 4 [Voice] の下の [Media Session Snooping] チェックボックスをオンしてメディア セッション スヌーピングを有効にするか、オフにしてこの機能を無効にします。デフォルト値はオフです。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Save Configuration] をクリックします。

ステップ 7 次の手順で、アクセス ポイント無線の VoIP 統計情報を表示します。

a) [Monitor] > [Access Points] > [Radios] > [802.11a/n/ac] または [802.11b/g/n] の順に選択して、[802.11a/n/ac（または 802.11b/g/n）Radios] ページを開きます。

b) 右にスクロールし、VoIP 統計を表示したいアクセス ポイントの [Detail] リンクをクリックします。[Radio > Statistics] ページが表示されます。

[VoIP Stats] セクションには、このアクセスポイント無線について、音声コールの累積の数と長さが表示されます。音声コールが正常に発信されるとエントリが自動的に追加され、コントローラからアクセス ポイントが解除されるとエントリが削除されます。

ステップ 8 [Management] > [SNMP] > [Trap Logs] の順に選択して、コールが失敗した場合に生成されるトラップを表示します。[Trap Logs] ページが表示されます。

たとえば、図のログ 0 はコールが失敗したことを示しています。ログでは、コールの日時、障害の内容、障害発生の原因が示されます。

メディア セッション スヌーピングの設定（CLI）

手順

ステップ 1 特定の WLAN で VoIP スヌーピングを有効または無効にするには、次のコマンドを入力します。

config wlan call-snoop {**enable** | **disable**} *wlan_id*

ステップ 2 次のコマンドを入力して、変更を保存します。

save config

ステップ 3 特定の WLAN のメディア セッション スヌーピングのステータスを表示するには、次のコマンドを入力します。

show wlan *wlan_id*

以下に類似した情報が表示されます。

```
WLAN Identifier.................................. 1
Profile Name..................................... wpa2-psk
Network Name (SSID).............................. wpa2-psk
Status........................................... Enabled
...
 FlexConnect Local Switching...................... Disabled
    FlexConnect Learn IP Address..................... Enabled
    Infrastructure MFP protection.............. Enabled (Global Infrastructure MFP
Disabled)
 Client MFP..................................... Optional
    Tkip MIC Countermeasure Hold-down Timer....... 60
Call Snooping.................................... Enabled
```

ステップ 4 メディア セッション スヌーピングが有効であり、コールがアクティブである場合の MSA クライアントのコール情報を表示するには、次のコマンドを入力します。

show call-control client callInfo *client_MAC_address*

以下に類似した情報が表示されます。

```
Uplink IP/port..................................... 192.11.1.71 / 23870
Downlonk IP/port................................... 192.12.1.47 / 2070
UP................................................. 6
Calling Party...................................... sip:1054
Called Party....................................... sip:1000
Call ID............................................ 58635b00-850161b7-14853-1501a8
Number of calls for given client is.............. 1
```

ステップ 5 コールが成功した場合のメトリックまたはコールが失敗した場合に生成されるトラップを表示するには、次のコマンドを入力します。

show call-control ap {**802.11a** | **802.11b**} *Cisco_AP* {**metrics** | **traps**}

show call-control ap {**802.11a** | **802.11b**} *Cisco_AP* **metrics** を入力すると、次のような情報が表示されます。

```
Total Call Duration in Seconds.................. 120
Number of Calls................................. 10
```

show call-control ap {**802.11a** | **802.11b**} *Cisco_AP* **traps** を入力すると、次のような情報が表示されます。

```
Number of traps sent in one min................. 2
Last SIP error code............................. 404
Last sent trap timestamp..................... Jun 20 10:05:06
```

トラブルシューティングに役立つように、このコマンドの出力には失敗したコールすべてのエラー コードが示されます。次の表では、失敗したコールの考えられるエラー コードについて説明します。

表 *5 :* 失敗した *Voice over IP*（*VoIP*）コールのエラー コード

エラー コード	整数	説明
1	unknown	不明なエラー。
400	badRequest	構文が不正であるため要求を認識できませんでした。
401	unauthorized	要求にはユーザ認証が必要です。
402	paymentRequired	将来的な使用のために予約されています。
403	forbidden	サーバは要求を認識しましたが、実行を拒否しています。
404	notFound	サーバは、このユーザが Request-URI に指定されたドメインに存在しないという情報を持っています。
405	methodNotallowed	Request-Line で指定されたメソッドが認識されているものの、Request-URI で指定されたアドレスでは許可されていません。

エラー コード	整数	説明
406	notAcceptabl	要求によって指定されたリソースは、送信された要求内の [Accept] ヘッダー テキストボックスによって許容されないコンテンツ特性を持つ応答エンティティしか生成できません。
407	proxyAuthenticationRequired	クライアントは、最初にプロキシで認証される必要があります。
408	requestTimeout	サーバは、時間内にユーザのロケーションを確認できなかったため、適切な時間内に応答を作成できませんでした。
409	conflict	リソースの現在の状態と競合したために、要求を完了できませんでした。
410	gone	要求されたリソースがサーバで使用できず、転送アドレスが不明です。
411	lengthRequired	要求のエンティティ自体が、サーバが処理を想定しているサイズ、または処理できるサイズより大きいため、サーバが要求の処理を拒否しています。
413	requestEntityTooLarge	要求のエンティティ自体が、サーバが処理を想定しているサイズ、または処理できるサイズより大きいため、サーバが要求の処理を拒否しています。
414	requestURITooLarge	Request-URI がサーバが解釈を想定している長さよりも長いために、サーバが要求の処理を拒否しています。

エラー コード	整数	説明
415	unsupportedMediaType	要求されたメソッドについて、要求のメッセージ本文の形式がサーバでサポートされていないために、サーバが要求の処理を拒否しています。
420	badExtension	Proxy-Require または Require ヘッダー テキスト ボックスで指定されたプロトコル拡張が、サーバで認識されませんでした。
480	temporarilyNotAvailable	着信側のエンド システムが正常に通信できるものの、着信側が現在、利用不能です。
481	callLegDoesNotExist	User-Agent Server（UAS; ユーザ エージェント サーバ）が既存のダイアログまたはトランザクションと一致していない要求を受け取りました。
482	loopDetected	サーバはループを検出しました。
483	tooManyHops	サーバは Max-Forwards ヘッダー テキスト ボックスの値が 0 である要求を受信しました。
484	addressIncomplete	サーバは Request-URI が不完全である要求を受信しました。
485	ambiguous	Request-URI があいまいです。
486	busy	着信側のエンド システムは正常に接続されましたが、着信側は現在、このエンド システムで追加のコールを受け入れようとしないか、受け入れることができません。
500	internalServerError	サーバで、要求の処理を妨げる予期しない状態が発生しました。

エラー コード	整数	説明
501	notImplemented	サーバは要求を処理するために必要な機能をサポートしていません。
502	badGateway	ゲートウェイまたはプロキシとして機能しているサーバが、要求を処理するためにアクセスしたダウンストリームサーバから無効な応答を受信しました。
503	serviceUnavailable	一時的な過負荷またはメンテナンスのために、サーバが一時的に要求を処理できなくなっています。
504	serverTimeout	サーバは、要求を処理するためにアクセスした外部サーバから時間内に応答を受信しませんでした。
505	versionNotSupported	サーバは、要求で使用されたSIPプロトコルのバージョンをサポートしていないか、サポートを拒否しています。
600	busyEverywhere	着信側のエンド システムは正常に接続されましたが、着信側はこの時点でビジーであるか、コールに応答しようとしていません。
603	decline	着信側のマシンは正常に接続されましたが、ユーザが参加しようとしていないか、参加できません。
604	doesNotExistAnywhere	サーバには、Request-URIで示されたユーザが存在しないという情報があります。

エラー コード	整数	説明
606	notAcceptable	ユーザのエージェントは正常に接続されましたが、セッションの説明の一部（要求されるメディア、帯域幅、アドレス指定形式など）が受け入れられませんでした。

（注） メディア セッション スヌーピングに関する問題が発生した場合は、**debug call-control** {**all** | **event**} {**enable** | **disable**} コマンドを入力して、すべてのメディア セッション スヌーピング メッセージまたはイベントをデバッグしてください。

QoS Enhanced BSS

Cisco 7921 および 7920 Wireless IP Phone で QoS Enhanced BSS を使用するための前提条件

Cisco 7921 および 7920 Wireless IP Phone をコントローラで使用する場合は、次のガイドラインに従ってください。

- 各コントローラで、アグレッシブなロードバランシングが無効にされている必要があります。無効化されていない場合、電話による初期ローミングが失敗し、オーディオパスが中断されることがあります。
- ダイナミック伝送パワーコントロール（DTPC）情報要素（IE）は、**config 802.11b dtpc enable** コマンドを使用して有効にする必要があります。DTPC IE は、アクセスポイントがその送信電力で情報をブロードキャストすることを可能にする、ビーコンおよびプローブの情報要素です。7921 または 7920 電話は、この情報を使用して、その送信電力を、アソシエート先のアクセスポイントと同じレベルに自動的に調整します。このようにして、両方のデバイスが同じレベルで送信するようになります。
- 7921 と 7920 電話のおよびコントローラの両方で、Cisco Centralized Key Management（CCKM）高速ローミングがサポートされます。
- WEP を設定する際、コントローラおよび 7921 または 7920 電話によって、用語上の違いがあります。7921 または 7920 で 128 ビット WEP を使用する場合は、コントローラを 104 ビットに設定してください。
- スタンドアロンの 7921 電話では、load-based の CAC が有効にされ、また WLAN 上で WMM Policy が Required に設定されている必要があります。
- コントローラでは、ファームウェア バージョン 1.1.1 を使用して 7921 電話から送られるトラフィック分類（TCLAS）がサポートされます。この機能により、7921 電話への音声ストリームを正しく分類することができます。

• 1242 シリーズ アクセス ポイントの 802.11a 無線で 7921 電話を使用する場合は、24-Mbps データ レートを Supported に設定して、それよりも小さい Mandatory データ レート（12 Mbps など）を選択します。さもないと、電話の音声品質が低下するおそれがあります。

QoS Enhanced BSS について

QoS Enhanced Basis Service Set（QBSS）情報要素（IE）により、アクセス ポイントはそのチャネル使用率を無線デバイスに通知できます。チャネル使用率が高いアクセス ポイントではリアルタイム トラフィックを効率的に処理できないため、7921 または 7920 電話では、QBSS 値を使用して、他のアクセス ポイントにアソシエートするべきかどうかが判断されます。次の 2 つのモードで QBSS を有効にできます。

• 802.11E QBSS 規格を満たすデバイス（Cisco 7921 IP Phone など）をサポートしている、Wi-Fi Multimedia（WMM）モード

• 802.11b/g ネットワーク上で Cisco 7920 IP Phone をサポートしている 7920 サポート モード

  7920 サポート モードには、次の 2 つのオプションが含まれています。

  • Call Admission Control（CAC; コール アドミッション制御）がクライアント デバイス上で設定され、クライアント デバイスによってアドバタイズされている必要がある 7920 電話のサポート（通常、旧式の 7920 電話）

  • CAC がアクセス ポイント上で設定され、アクセス ポイントによってアドバタイズされている必要がある 7920 電話のサポート（通常、新式の 7920 電話）

    アクセス ポイントで制御される CAC が有効になっている場合、アクセス ポイントは、シスコが所有する CAC Information Element（IE;情報要素）を送信し、標準の QBSS IE を送信しません。

QoS Enhanced BSS の制約事項

• OEAP 600 シリーズ アクセス ポイントでは、CAC はサポートされません。

• デフォルトで、QBSS は無効になっています。

• 7920 電話は、CAC 機能が制限された、非 WMM 電話です。電話は、アソシエート先のアクセス ポイントのチャネル使用率を確認し、それをアクセス ポイントからビーコンにより通知されたしきい値と比較します。チャネル使用率がしきい値より低い場合は、7920 は電話をかけます。対照的に、7921 電話は、完全な機能を備えた WMM 電話で、Traffic Specifications（TSPEC）を使用して、電話をかける前に音声キューにアクセスします。7921 電話は、load-based の CAC と適切に連動します。load-based の CAC では、音声に取り分けられたチャネルの割合を使用して、それに応じて通話を制限しようとします。

  7921 電話は WMM をサポートし、7920 電話はサポートしないため、これらの電話を混合環境で使用する場合に両方の電話を適切に設定していないと、キャパシティと音声品質の問題が生じる可能性があります。7921 および 7920 電話の両方を有効にして同じネットワーク上で共存させるには、load-based の CAC と 7920 AP CAC の両方がコントローラで有効

にされ、WMM Policy が Allowed に設定されていることを確認してください。7921 ユーザより、7920 ユーザの方が多い場合に、これらの設定は特に重要になります。

- 音声をサポートしているすべての無線ネットワークでは、ベンダーに関係なく、コントローラ GUI または CLI を使用して、アグレッシブ ロード バランシングを常にオフにすることを推奨します。アグレッシブ ロードバランシングがオンになっていると、ハンドセットが最初の再アソシエーション試行で拒否されたとき、音声クライアントはローミングすると可聴アーティファクトを聞くことができます。

QBSS の設定（GUI）

手順

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 WMM モードを設定する WLAN の ID 番号をクリックします。

ステップ 3 [WLANs > Edit] ページが表示されたら、[QoS] タブを選択して [WLANs > Edit（QoS）] ページを開きます。

ステップ 4 7921 電話および WMM 規格を満たすその他のデバイスに対して WMM モードを有効にするかどうかに応じて、[WMM Policy] ドロップダウン リストから次のオプションのいずれかを選択してください。

- [Disabled]：WLAN 上で WMM を無効にします。これはデフォルト値です。
- [Allowed]：WLAN 上でクライアント デバイスに WMM の使用を許可します。
- [Required]：クライアント デバイスで WMM の使用を必須にします。WMM をサポートしていないデバイスは WLAN に接続できません。

ステップ 5 アクセス ポイントで制御される CAC を必要とする電話で 7920 サポート モードを有効にする場合は、[7920 AP CAC] チェックボックスをオンにします。デフォルト値はオフです。

ステップ 6 クライアントで制御される CAC を必要とする電話で 7920 サポート モードを有効にする場合は、[7920 Client CAC] チェックボックスをオンにします。デフォルト値はオフです。

（注） 1 つの WLAN で、WMM モードとクライアントにより制御された CAC モードの両方を有効にすることはできません。

ステップ 7 [Apply] をクリックして、変更を確定します。

ステップ 8 [Save Configuration] をクリックして、変更を保存します。

QBSS の設定（CLI）

手順

ステップ 1 QBSS サポートを追加する WLAN の ID 番号を決定するには、次のコマンドを入力します。

show wlan summary

ステップ 2 次のコマンドを入力して、WLAN を無効にします。

config wlan disable *wlan_id*

ステップ 3 7921 電話および WMM 規格を満たすその他のデバイスで WMM モードを設定するには、次のコマンドを入力します。

config wlan wmm {**disabled** | **allowed** | **required**} *wlan_id*

値は次のとおりです。

- **disabled** は、WLAN 上の WMM モードを無効にします。
- **allowed** は、WLAN 上のクライアント デバイスに WMM の使用を許可します。
- **required** は、クライアント デバイスに WMM の使用を要求します。WMM をサポートしていないデバイスは WLAN に接続できません。

ステップ 4 クライアントで制御される CAC を必要とする電話で 7920 サポート モードを有効または無効にするには、次のコマンドを入力します。

config wlan 7920-support client-cac-limit {**enable** | **disable**} *wlan_id*

（注） 1 つの WLAN で、WMM モードとクライアントにより制御された CAC モードの両方を有効にすることはできません。

ステップ 5 アクセス ポイントで制御される CAC を必要とする電話で 7920 サポート モードを有効または無効にするには、次のコマンドを入力します。

config wlan 7920-support ap-cac-limit {**enable** | **disable**} *wlan_id*

ステップ 6 次のコマンドを入力して、WLAN を再び有効にします。

config wlan enable *wlan_id*

ステップ 7 次のコマンドを入力して、変更を保存します。

save config

ステップ 8 WLAN が有効であり、[Dot11-Phone Mode (7920)] テキスト ボックスがコンパクト モードに設定されていることを確認するには、次のコマンドを入力します。

show wlan *wlan_id*