CHAPTER 4

# デバイスの問題

ここでは、Cisco Unified IP Phone、ゲートウェイ、および関連デバイスで発生する可能性がある、次のような一般的な問題について説明します。



## 音声品質

電話コール中に音声信号がなくなる、または歪むなどの音声品質の問題が発生する場合があります。

一般的な問題としては、音声が中断する（言葉が途切れるなど）、奇妙なノイズやエコーのような音声の歪みが生じる、水中で話しているような音または合成音のような音声品質になる、といった問題があります。片通話（2 人の間の会話で 1 人だけが聞くことができる）は、実際には音声品質の問題ではありませんが、この項で説明します。

次の項目の 1 つまたは複数で音声の問題が発生する場合があります。

- ゲートウェイ
- 電話機
- ネットワーク

ここでは、一般的な次の音声品質の問題について説明します。

# 音声の消失または歪み

### 症状

発生する可能性のある最も一般的な問題の 1 つに、音声信号の中断（不明瞭な会話や単語または文中の音節の消失としてよく説明される）があります。この問題の一般的な原因は、パケット損失およびジッタの 2 つです。パケット損失とは、音声パケットがドロップされたか、または使用するには到着が遅すぎたために、音声パケットが宛先に到着しないことを意味します。ジッタは、パケット到着時間の変動を示します。理想的な状況では、すべての Voice over IP（VoIP）パケットが、正確に 20 マイクロ秒（ms）ごとに 1 つの割合で到着します。これは、パケットがポイント A からポイント B に到達するためにかかる時間ではなく、単なるパケット到着時間の変動であることに注意してください。

### 考えられる原因

ネットワークには、可変遅延の原因が多数存在します。これらの原因には、制御できるものもあれば制御できないものもあります。パケット化された音声ネットワークの可変遅延は、完全には排除できません。電話機および他の音声対応デバイスの Digital Signal Processor（DSP; デジタル シグナル プロセッサ）は、可変遅延を予測して計画的に音声の一部をバッファに格納します。このデジッタ処理は、音声パケットが宛先に到着し、通常の音声ストリームに組み込まれる準備ができている場合にだけ実行されます。

Cisco Unified IP Phone モデル 7960 では、音声サンプルを 1 秒分バッファに格納できます。ジッタバッファには適応性があるため、パケットのバーストが受信された場合に、Cisco Unified IP Phone モデル 7960 ではジッタを制御するためにこれらのパケットを再生できます。ネットワーク管理者は、（特にコールが WAN を通過する場合は）quality-of-service（QoS）およびその他の手段をあらかじめ適用して、パケット到着時間の間の変動を最小化する必要があります。

一部のビデオ エンドポイントでは G.728 がサポートされていないため、G.728 を使用するとノイズが発生することがあります。G.729 などの別のコーデックを使用してください。

### 推奨処置

1. 音声の消失または歪みの問題が発生している場合は、最初にその音声のパスを分離します。コール音声ストリームのパスから個々のネットワーク デバイス（スイッチおよびルータ）を特定します。音声は、2 つの電話機間の場合もあれば、電話機とゲートウェイ間の場合もあり、また、複数のレッグ（電話機からトランスコーディング デバイスへのレッグやトランスコーディング デバイスから別の電話機へのレッグ）が存在する可能性もあります。問題が 2 つのサイト間だけで発生しているのか、特定のゲートウェイまたは特定のサブネットだけで発生しているのかなどを特定します。これにより、さらに注意して調べる必要があるデバイスの数を絞り込むことができます。
2. 次に、音声圧縮（Voice Activation Detection [VAD; 音声アクティブ化検出] とも呼ばれる）をディセーブルにします。このメカニズムは、無音状態になったときに音声を送信しないことで帯域幅を節約しますが、その結果、単語の最初の部分ではっきりとわかる、または許容できないクリッピングが発生することがあります。

   Cisco Unified Communications Manager の管理ページでサービスをディセーブルにして、[ システム（System）] > [ サービス パラメータ（Service Parameters）] を選択します。ここで、サーバおよび Cisco CallManager サービスを選択します。
3. Cisco Communications Manager クラスタ内のすべてのデバイスに対してディセーブルにするには、SilenceSuppression を **False** に設定します。または、SilenceSuppressionForGateways を **False** に設定することもできます。判断がつかない場合は、それぞれに値 **False** を選択して、両方ともオフにします。
4. ネットワーク アナライザを使用して（ネットワーク アナライザが使用可能な場合）、音声圧縮をディセーブルにしたときに、監視対象の 2 つの電話機間のコールに 1 秒当たり 50 個のパケット（または 20 ms ごとに 1 つのパケット）が含まれているかどうかを確認します。フィルタリングを適切に使用すると、過剰な数のパケットが損失または遅延していないかどうかを確認できます。

クリッピングの原因になるのは遅延そのものではなく、可変遅延だけです。次の表は完全なトレースを示していますが、ここで、音声パケット（RTP ヘッダーを含んでいる）間の到着時間が 20 ms になっていることに注意してください。低品質のコール（ジッタが多数存在するコールなど）では、到着時間に大きな差が出ます。

次の表は、完全なトレースを示しています。

| パケット番号 | 絶対時間（秒） | 差分時間（ミリ秒） |
|---|---|---|
| 1 | 0 | |
| 2 | 0.02 | 20 |
| 3 | 0.04 | 20 |
| 4 | 0.06 | 20 |
| 5 | 0.08 | 20 |

ネットワーク内のさまざまなポイントにパケット アナライザを配置すると、遅延が発生する場所の数を絞り込むのに役立ちます。アナライザを利用できない場合は、別の方法を使用する必要があります。音声パス内にある各デバイスのインターフェイス統計情報を調べてください。

診断 Call Detail Record（CDR; コール詳細レコード）には、音声品質の低いコールをトラッキングする別のツールが示されています。CDR の詳細については、『*CDR Analysis and Reporting Administration Guide*』を参照してください。

# Cisco Unified IP Phone の音声問題の修正

### 症状

音声の問題は、コールの進行中に発生します。

### 考えられる原因

高速インターフェイスを低速インターフェイスにつなぐデバイスは、遅延およびパケット損失の最も一般的な原因となります。たとえば、LAN に接続されている 100 MB のファースト イーサネット インターフェイスと、WAN に接続されている低速のフレームリレー インターフェイスがルータにあるとします。リモート サイトへの接続時にかぎって音声品質の低下が発生する場合、この問題の主な原因は次のとおりです。

- 音声トラフィックにデータ トラフィックよりも高い優先度を与えるように、ルータが正しく設定されていない。
- WAN でサポートするには多すぎる数のアクティブ コールが存在する（つまり、コール アドミッション制御で発信可能なコール数が制限されていない）。
- 物理的なポート エラーが発生している。
- WAN 自体で輻輳が発生している。

LAN で発生する最も一般的な問題は、ケーブル不良、インターフェイス不良、またはデバイスの設定不良（ポート速度やデュプレックスのミスマッチなど）が原因で発生する物理レベルのエラー（CRC エラーなど）です。トラフィックが、ハブなどの共有メディア デバイスを通過していないことを確認します。

### 推奨処置

Cisco Unified IP Phone モデル 7960 には、発生する可能性がある音声問題の診断ツールが、もう 1 つ用意されています。

- アクティブ コールで *i* または **?** ボタンを 2 度素早く押すと、パケットの送受信に関する統計情報と、平均および最大ジッタ カウンタを含む情報画面が電話機に表示されます。

**（注）** このウィンドウでは、ジッタは、最後に到着した 5 パケットの平均に相当します。最大ジッタは平均ジッタの最大値を示します。

- トラフィックが予想よりも低速のネットワーク パスを通過しているという状況が発生することもあります。QoS が正しく設定されている場合、コール アドミッション制御が実行されていない可能性があります。トポロジに応じて、Cisco Unified Communications Manager の管理ページで [ロケーション（Locations）] の設定を使用するか、または Cisco IOS ルータをゲートキーパーとして使用することで、この制御を実行できます。いずれにしても、WAN 全体でサポートされている最大コール数を常に認識しておく必要があります。
- クラックル ノイズは音声品質の低下を示すもう 1 つの症状であり、電源モジュールの不具合や電話機周辺の何らかの強力な電気的干渉によって発生することがあります。電源モジュールを交換するか、電話機を移動します。
- ゲートウェイおよび電話機のロードを確認します。最新のソフトウェア ロード、新しいパッチ、または問題に関連のあるリリース ノートがないかどうかを www.cisco.com で確認します。

適切な修正を適用したあと、次の手順を実行して音声品質を確認します。

1. 「音声の消失または歪み」（P.4-2）の説明に従って無音圧縮をディセーブルにしてテストします。次に 2 つのサイト間でコールを発信します。コールを保留またはミュートの状態にしないでください。これを行うと、パケットの送信が停止してしまうためです。
2. WAN 全体の最大コール数が設定されている場合は、すべてのコールが許容可能な品質になります。
3. さらにもう 1 つコールを発信するとファースト ビジー音が返ってくることを、テストして確認します。

## エコー

### 症状

エコーは、生成された音声エネルギーがプライマリ信号パスに伝送され、遠端からの受信パスと連結されたときに発生します。このとき送話者には、自分自身の声がエコー パスの合計遅延時間分だけ遅れて聞こえます。

音声は反響することがあります。反響は、従来の音声ネットワークでも発生する可能性がありますが、遅延が小さいため認識されません。ユーザにとっては、エコーというよりも側音のように聞こえます。VoIP ネットワークでは、パケット化および圧縮が遅延の一因となるため、常にエコーが認識されます。

### 考えられる原因

エコーの原因は、常にアナログ コンポーネントおよび配線にあります。たとえば、IP パケットは、低い音声レベルまたはデジタル T1/E1 回線では、簡単に向きを変えてソースに戻ってくることはできません。例外が発生する可能性があるのは、片方の通話者が音量を非常に高くしたスピーカフォンを使用している場合など、音声ループが作成される状況だけです。

### 推奨処置

1. 問題の電話機でスピーカフォンを使用していないこと、およびヘッドセットの音量を適切なレベル（最大音声レベルの 50% から開始）に設定してあることを確認します。ほとんどの場合、問題は、デジタルまたはアナログ ゲートウェイ経由で PSTN に接続している場合に発生します。

#### ゲートウェイのテスト

2. 使用されているゲートウェイを特定します。デジタル ゲートウェイが使用されている場合は、送信方向（PSTN に向かう方向）にパディングを追加できます。信号の強度が弱いと反響エネルギーも小さくなるため、これによって問題が解決します。

   また、反響音がさらに小さくなるように受信レベルを調節できます。一度に少しずつ調節してください。信号を弱くしすぎると、両側で音声が聞こえなくなります。

3. または、通信事業者に問い合せて、回線を確認するよう要求することもできます。北米の一般的な T1/PRI 回線では、入力信号は -15 dB である必要があります。信号レベルが高すぎる場合（-5 dB など）、エコーが発生する可能性があります。

#### エコー ログの保持

4. エコーが発生したすべてのコールのログを保持する必要があります。

   問題が発生した時間、発信元の電話番号、および発信先の電話番号を記録します。ゲートウェイには 16 ms という固定値のエコー キャンセレーションが設定されています。

   反響音の遅延がこれよりも大きい場合、エコー キャンセラは正しく動作しません。この問題はローカル コールでは発生せず、長距離コールでは、セントラル オフィスのネットワークに組み込まれた外部のエコー キャンセラを使用する必要があります。このような事実が、エコーが発生するコールの外部電話番号を記録する必要がある理由の 1 つになっています。

#### ロードの確認

5. ゲートウェイおよび電話機のロードを確認します。最新のソフトウェア ロード、新しいパッチ、または問題に関連のあるリリース ノートがないかどうかを www.cisco.com で確認します。

## 片通話または無音声

### 症状

IP ステーションから Cisco IOS 音声ゲートウェイまたはルータ経由で電話コールが確立されている場合に、片方の通話者しか音声を受信しません（一方向通信）。

2 つの Cisco ゲートウェイ間でトールバイパス コールが確立されている場合に、片方の通話者しか音声を受信しません（一方向通信）。

### 考えられる原因

特に、Cisco IOS ゲートウェイ、ファイアウォール、またはルーティングが正しく設定されていないことや、デフォルト ゲートウェイの問題によって、この問題が発生する可能性があります。

### 推奨処置

#### Cisco IOS ゲートウェイまたはルータで IP ルーティングがイネーブルになっていることを確認

VG200 などの一部の Cisco IOS ゲートウェイでは、デフォルトで IP ルーティングがディセーブルになっています。これにより、片通話の問題が発生します。

**（注）** 次に進む前に、ルータで IP ルーティングがイネーブルになっている（つまり、グローバル コンフィギュレーション コマンド **no ip routing** を使用していない）ことを確認します。

IP ルーティングをイネーブルにするには、Cisco IOS ゲートウェイで次のグローバル コンフィギュレーション コマンドを入力します。

**voice-ios-gwy(config)#ip routing**

基本 IP ルーティングの確認

常に最初に基本 IP アクセスを確認するようにします。RTP ストリームはコネクションレス型であるため（UDP で転送される）、一方向のトラフィックは正常に実行されますが、逆方向はトラフィックが失われることがあります。

次の条件を確認してください。

- デフォルト ゲートウェイがエンド ステーションに設定されている。
- 上記のデフォルト ゲートウェイの IP ルートが宛先ネットワークにつながっている。

**（注）** 次に、さまざまな Cisco Unified IP Phone でデフォルト ルータまたはゲートウェイの設定を確認する方法を一覧します。

- Cisco Unified IP Phone モデル 7910 : [ 設定（Settings）] ボタンを押し、オプション 6 を選択して、[ デフォルト ルータ（Default Router）] フィールドが表示されるまで下向きの音量ボタンを押します。
- Cisco Unified IP Phone モデル 7960/40 : [ 設定（Settings）] ボタンを押し、オプション 3 を選択して、[ デフォルト ルータ（Default Router）] フィールドが表示されるまで下方向にスクロールします。
- Cisco Unified IP Phone モデル 2SP+/30VIP : **## を押してから、gtwy= が表示されるまで # を押します。

**（注）** Cisco DT24+ ゲートウェイの場合は、DHCP スコープを調べて、スコープに [ デフォルト ゲートウェイ（Default Gateway）]（003 ルータ）オプションがあることを確認します。003 ルータ パラメータによって、デバイスおよび PC の [ デフォルト ゲートウェイ（Default Gateway）] フィールドに値が入力されます。スコープ オプション 3 には、ゲートウェイのルーティングを行うルータ インターフェイスの IP アドレスが設定されている必要があります。

### Cisco IOS ゲートウェイまたはルータの特定の IP アドレスへの H.323 シグナリングのバインド

Cisco IOS ゲートウェイに複数のアクティブ IP インターフェイスがある場合、H.323 シグナリングの一部は送信元に 1 つの IP アドレスを使用し、その他の部分は別の送信元アドレスを参照することがあります。これにより、片通話になるなど、さまざまな問題が発生する可能性があります。

この問題を回避するには、H.323 シグナリングを特定の送信元アドレスにバインドします。この送信元アドレスは物理インターフェイスまたは仮想インターフェイスに割り当てることができます（ループバック）。インターフェイス コンフィギュレーション モードで使用するコマンド構文は、**h323-gateway voip bind srcaddr<ip address>** です。Cisco Unified Communications Manager が指す IP アドレスを持つインターフェイスで、このコマンドを設定します。

このコマンドは、Cisco IOS リリース 12.1.2T で導入され、『*Configuring H.323 Support for Virtual Interfaces*』で文書化されています。

**（注）** バージョン 12.2(6) には不具合があるため、実際にはこのソリューションで片通話の問題が発生する可能性があります。詳細については、Cisco ソフトウェア Bug Toolkit（登録されているお客様専用）で Bug ID CSCdw69681（登録されているお客様専用）を参照してください。

### Telco またはスイッチとの間で応答監視が正しく送受信されていることを確認

Telco またはスイッチに Cisco IOS ゲートウェイが接続されている実装では、Telco またはスイッチの背後にあるコール先のデバイスがコールに応答するときに、応答監視が正しく送信されることを確認します。応答監視の受信に失敗すると、Cisco IOS ゲートウェイは順方向の音声パスをカットスルー（オープン）せず、これにより片通話が発生します。これを回避するには、**voice rtp send-recv on** を設定する必要があります。

**voice rtp send-recv を使用した、Cisco IOS ゲートウェイまたはルータでの双方向通話の早期カットスルー**

RTP ストリームが開始するとすぐに、音声パスが逆方向に確立されます。順方向の音声パスは、Cisco IOS ゲートウェイがリモート エンドから Connect メッセージを受信するまでカットスルーされません。

場合によっては、RTP チャネルがオープンされたあとすぐに（Connect メッセージが受信される前に）双方向音声パスを確立する必要があります。これを実現するには、**voice rtp send-recv** グローバル コンフィギュレーション コマンドを使用します。

**Cisco IOS ゲートウェイまたはルータで、リンクバイリンク ベースで cRTP 設定を確認**

この問題は、トールバイパスなど、複数の Cisco IOS ルータまたはゲートウェイが音声パスに含まれ、Compressed RTP（cRTP; 圧縮 RTP）が使用されているシナリオに適用されます。cRTP、つまり RTP ヘッダー圧縮は、VoIP パケット ヘッダーを小さくして帯域幅を取り戻す方法です。cRTP は、VoIP パケット上の 40 バイトの IP/UDP/RTP ヘッダーを 1 パケット当たり 2 ～ 4 バイトに圧縮するため、G.729 で符号化されたコールで cRTP を使用すると、約 12KB の帯域幅が得られます。

cRTP はホップバイホップ ベースで実行され、ホップごとに圧縮解除および再圧縮が行われます。ルーティングを行うにはそれぞれのパケット ヘッダーを検査する必要があるため、IP リンクの両側で cRTP をイネーブルにします。

また、リンクの両端で cRTP が予想通りに機能していることを確認します。Cisco IOS のレベルは、スイッチング パスおよび cRTP の同時サポートに応じて異なります。

要約すると、次のような履歴になります。

- Cisco IOS ソフトウェア リリース 12.0.5T までは、cRTP はプロセス交換されます。
- Cisco IOS ソフトウェア リリース 12.0.7T では、cRTP に対するファースト スイッチングと Cisco express forwarding（CEF; シスコ エクスプレス フォワーディング）スイッチングのサポートが導入され、12.1.1T でも引き続きサポートされています。
- Cisco IOS ソフトウェア リリース 12.1.2T では、アルゴリズムによるパフォーマンス改善が導入されています。

Cisco IOS プラットフォーム（IOS リリース 12.1）を実行している場合、Bug ID CSCds08210（登録されているお客様専用）（「VoIP and FAX not working with RTP header compression ON」）が、使用している IOS バージョンに影響していないことを確認します。

**Cisco IOS ゲートウェイまたはルータの NAT に必要な最小ソフトウェア レベルの確認**

Network Address Translation（NAT; ネットワーク アドレス変換）を使用している場合は、最小ソフトウェア レベル要件を満たしている必要があります。初期バージョンの NAT では、Skinny プロトコル変換がサポートされていないため、片通話の問題が発生します。

NAT と Skinny を同時に使用するために必要な最小ソフトウェア レベルは、IOS ゲートウェイで NAT とともに Skinny および H.323v2 がサポートされている Cisco IOS ソフトウェア 12.1(5)T です。

**（注）** Cisco Unified Communications Manager で、Skinny シグナリング用にデフォルトの 2000 とは異なる TCP ポートを使用している場合、**ip nat service skinny tcp port<number>** グローバル コンフィギュレーション コマンドを使用して NAT ルータを調整する必要があります。

PIX ファイアウォールで NAT および Skinny を同時に使用するために必要な最小ソフトウェア レベルは 6.0 です。

（注）　これらのソフトウェア レベルは、ゲートキーパーのフル サポートに必要なすべての RAS メッセージをサポートしているわけではありません。ゲートキーパーのサポートは、このマニュアルの対象範囲外です。

### AS5350 および AS5400 での voice-fastpath のディセーブル化

Cisco IOS コマンド **voice-fastpath enable** は、AS5350 および AS5400 用の非表示のグローバル コンフィギュレーション コマンドで、デフォルトではイネーブルになっています。これをディセーブルにするには、**no voice-fastpath enable** グローバル コンフィギュレーション コマンドを使用します。

イネーブルの場合、このコマンドによって、特定のコール用にオープンされる論理チャネルの IP アドレスおよび UDP ポートがキャッシュされ、RTP ストリームはアプリケーション レイヤに到達できなくなり、それよりも下位のレイヤにパケットが転送されます。そのため、コール数の多いシナリオにおいて、CPU 使用率がわずかに減少します。

保留または転送などの補足サービスが使用されている場合、voice-fastpath コマンドを使用すると、ルータは、保留中のコールが再開されたあとや転送が完了したあとに生成された新しい論理チャネル情報を無視して、キャッシュされている IP アドレスおよび UDP ポートに音声を送ります。この問題を回避するには、論理チャネルの再定義が考慮され、音声が新しい IP アドレスと UDP ポートのペアに送られるように、トラフィックを常にアプリケーション レイヤに転送する必要があります。このような理由で、voice-fastpath をディセーブルにして補足サービスをサポートする必要があります。

### SoftPhone を使用した VPN IP アドレスの設定

Cisco IP SoftPhone には、Cisco Unified IP Phone モデル 7900 シリーズ電話機のように PC 動作を行う機能が備わっています。VPN を使用して会社のネットワークに接続するリモート ユーザは、片通話の問題を回避するためにさらに追加の設定を行う必要があります。

このソリューションでは、[ ネットワーク オーディオ設定（Network Audio Settings）] で、ネットワーク アダプタの IP アドレスの代わりに VPN IP アドレスを設定する必要があります。

### 検証

パケット フローの検証に役立つのが、**debug cch323 rtp** コマンドです。このコマンドは、ルータの送信パケット（X）と受信パケット（R）を表示します。大文字は、正しく実行された送信または受信を示し、小文字はドロップされたパケットを示します。次の例を参照してください。

```
voice-ios-gwy#debug cch323 rtp
RTP packet tracing is enabled
voice-ios-gwy#
voice-ios-gwy#
voice-ios-gwy#
voice-ios-gwy#
voice-ios-gwy#

!--- This is an unanswered outgoing call.
!--- Notice that voice path only cuts through in forward
!--- direction and that packets are dropped. Indeed,
!--- received packets are traffic from the IP phone to the PSTN
!--- phone. These will be dropped until the call is answered.

Mar 3 23:46:23.690: ****** cut through in FORWARD direction *****
XXXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXXrrrrrrrrrrrrrrrr
voice-ios-gwy#
voice-ios-gwy#

!--- This is an example of an answered call:

voice-ios-gwy#
```

```
voice-ios-gwy#
*Mar 3 23:53:26.570: ****** cut through in FORWARD direction *****
XXXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XXrrrrrXrXrXrXrXrXrXrXrXrXrXrXrrXXrrXrXrXrXrXrXXXXXXXXXXXXXXXXXrXXXXXXXXrXrXrXXrrXr
XrXrXrXrXrXrXrXrXXrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr

!-- At this point the remote end picks up the phone.

*Mar 3 23:53:30.378: ****** cut through in BOTH direction *****
XRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXR
XXRRXRXRXRXXRRXRXRXRXRXRXXRXRXRXRXRXRXRXRXXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XXRRRRRRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXXRRRXR

!-- End of conversation.
```

# コーデックおよびリージョンのミスマッチ

ユーザがオフフックしたときにリオーダー トーン（ビジー信号）を受信する場合は、リージョン間のコーデックの不一致によって発生している可能性があります。コールの両端で 1 つ以上の共通コーデック（G.711 など）がサポートされていることを確認します。サポートされていない場合は、トランスコーダを使用する必要があります。

リージョンは、他の個々のリージョンと併用可能なサポート コーデックの範囲を示します。すべてのデバイスがリージョンに属します。

**（注）** Cisco IOS ルータとのコーデック ネゴシエーションはサポートされていません。

たとえば、Region1<->Region2 = G.711 は、Region1 のデバイスと Region2 のデバイス間のコールで、G.711 または G.711 と同じかそれよりも少ない帯域幅を必要とする他のサポート コーデック（G.711、G.729、G.723 などのサポート コーデック）を使用できることを意味します。

**（注）** 各デバイス用にサポートされているコーデックは、次のとおりです。
Cisco Unified IP Phone モデル 7960：G.711A-law/mu-law、G.729、G729A、G.729Annex-B
Cisco Unified IP Phone SP12 シリーズおよび VIP 30：G.711a-law/mu-law、G.723.1
Cisco Access Gateway DE30 および DT-24+：G.711a-law/mu-law、G.723.1

# ロケーションおよび帯域幅

ユーザが番号をダイヤルしたあとにリオーダー トーンを受信する場合、コール エンド デバイスの片方のロケーションに対する Cisco Unified Communications Manager 帯域幅割り当てを超過したことが原因である可能性があります。Cisco Unified Communications Manager は、コールを発信する前にデバイスごとに使用可能な帯域幅を確認します。使用可能な帯域幅がない場合、Cisco Unified Communications Manager はコールをセットアップせず、ユーザはリオーダー トーンを受信します。

```
12:42:09.017 Cisco Communications Manager|Locations:Orig=1 BW=12Dest=0 BW=-1(-1 implies
infinite bw available)
12:42:09.017 Cisco Communications Manager|StationD - stationOutputCallState
tcpHandle=0x4f1ad98
12:42:09.017 Cisco Communications Manager|StationD - stationOutputCallInfo
CallingPartyName=,  CallingParty=5003, CalledPartyName=, CalledParty=5005,
tcpHandle=0x4f1ad98
12:42:09.017 Cisco Communications Manager|StationD - stationOutputStartTone:
37=ReorderTone tcpHandle=0x4f1ad98
```

コールが確立されると、Cisco Unified Communications Manager は、そのコールで使用されるコーデックに応じてロケーションから帯域幅を差し引きます。

- コールで G.711 を使用している場合、Cisco Unified Communications Manager は 80k を差し引きます。
- コールで G.723 を使用している場合、Cisco Unified Communications Manager は 24k を差し引きます。
- コールで G.729 を使用している場合、Cisco Unified Communications Manager は 24k を差し引きます。

# 電話機の問題

ここでは、次の電話機の問題について説明します。

- 「電話機のリセット」
- 「ドロップされたコール」
- 「電話機が登録されない」（P.4-12）

## 電話機のリセット

### 症状

電話機がリセットされます。

### 考えられる原因

電話機は次の 2 つの理由で電源が再投入されるか、またはリセットされます。

- Cisco Unified Communications Manager への接続中に TCP で障害が発生した。
- 電話機のキープアライブ メッセージに対する確認応答の受信に失敗した。

### 推奨処置

1. 電話機およびゲートウェイを調べて、最新のソフトウェア ロードを使用していることを確認します。
2. 最新のソフトウェア ロード、新しいパッチ、または問題に関連のあるリリース ノートがないかどうかを www.cisco.com で確認します。
3. Cisco Cisco Unified Real-Time Monitoring Tool の Syslog ビューアで、リセットされている電話機のインスタンスがないかどうかを確認します。電話機のリセットは情報イベントに相当します。
4. 電話機がリセットされた時間の前後で何らかのエラーが発生していないかどうかを調べます。
5. SDI トレースを開始し、リセットされている電話機に共通する特徴を識別して、問題を切り分けます。たとえば、これらの電話機がすべて同じサブネット、同じ VLAN などに配置されていないかどうかを確認します。トレースを調べて、次の点を確認します。

   リセットはコール中に発生しているのか、断続的に発生しているのか。

   電話機モデルに何らかの類似点があるか。
6. リセットが頻繁に発生している電話機でスニファ トレースを開始します。電話機がリセットされたあとトレースを調べて、TCP リトライが発生しているかどうかを確認します。発生している場合、ネットワークに問題があることを示しています。トレースには、電話機が 7 日ごとにリセットされているなど、リセットにおける何らかの一貫性が示されることがあります。これは、DHCP のリース期限切れが 7 日ごとに発生していることを示しています（この値はユーザ設定が可能で、たとえば 2 分ごとにすることができます）。

## ドロップされたコール

### 症状

ドロップされたコールが早期に終了します。

### 考えられる原因

ドロップされたコールの早期終了は、電話機やゲートウェイのリセット（「電話機のリセット」（P.4-10）を参照）、または不適切な PRI 設定などの回線の問題によって発生する可能性があります。

### 推奨処置

1. この問題が 1 つの電話機または電話機グループに特有のものであるかどうかを確認します。影響を受けている電話機が、すべて特定のサブネットまたはロケーションに存在していることがわかる場合があります。
2. Cisco Cisco Unified Real-Time Monitoring Tool（RTMT）の Syslog ビューアで、電話機またはゲートウェイがリセットされているかどうかを確認します。

   リセットされている電話機ごとに、警告メッセージおよびエラー メッセージが 1 つずつ表示されます。これは、電話機が Cisco Unified Communications Manager への TCP 接続を維持できないために、Cisco Unified Communications Manager によって接続がリセットされていることを示しています。この状況は、電話機の電源が切られたため、またはネットワークに問題があるために発生することがあります。問題が断続的に発生している場合、RTMT のパフォーマンス モニタリングを使用すると役立つことがあります。
3. 問題が特定のゲートウェイだけで発生しているように見える場合は、トレースをイネーブルにするか、Call Detail Record（CDR; コール詳細レコード）を表示するか、またはその両方を行います。CDR ファイルには、問題の原因特定に役立つ可能性のある cause of termination（CoT）が含まれています。CDR の詳細については、『*CDR Analysis and Reporting Administration Guide*』を参照してください。

4. コールのどちら側がハング アップしたのかに応じて、接続解除の理由値（origCause_value および destCause_value）を確認します。この値は、次の場所にある Q.931 接続解除原因コード（10 進表記）に対応しています。

   http://www.cisco.com/en/US/tech/tk801/tk379/technologies_tech_note09186a008012e95f.shtml

5. コールがゲートウェイから PSTN に送信されている場合、CDR を使用して、どちら側でコールがハング アップしているかを確認します。Cisco Unified Communications Manager でトレースをイネーブルにすると、ほぼ同じ情報を取得できます。トレース ツールは Cisco Unified Communications Manager のパフォーマンスに影響を与える可能性があるため、このオプションは最後の手段として使用するか、またはネットワークがまだ実稼動していない場合にだけ使用するようにします。

## 電話機が登録されない

### 症状

5000 を超える数の電話機を登録できません。

### 考えられる原因

Maximum Number of Registered Devices サービス パラメータがデフォルト値に設定されています。

### 推奨処置

各ノードの Maximum Number of Registered Devices サービス パラメータの値を適切な値に変更します。

# ゲートウェイの問題

ここでは、次のゲートウェイの問題について説明します。

- 「ゲートウェイのリオーダー トーン」
- 「ゲートウェイの登録障害」

## ゲートウェイのリオーダー トーン

### 症状

リオーダー トーンが発生します。

### 考えられる原因

ゲートウェイ経由でコールを発信するユーザは、制限されたコールを発信しようとした場合、またはブロックされている番号をコールしようとした場合に、リオーダー トーンを受信することがあります。リオーダー トーンは、ダイヤルされた番号がアウト オブ サービスになっている場合や、PSTN に機器またはサービスの問題がある場合に発生することがあります。

リオーダー トーンを発信しているデバイスが登録されていることを確認してください。また、ダイヤル プラン設定を調べて、コールが正しくルーティングされることを確認してください。

### 推奨処置

ゲートウェイ経由のリオーダー トーンをトラブルシューティングする手順は、次のとおりです。

1. ゲートウェイを調べて、最新のソフトウェア ロードを使用していることを確認します。
2. 最新のソフトウェア ロード、新しいパッチ、または問題に関連のあるリリース ノートがないかどうかを www.cisco.com で確認します。
3. SDI トレースを開始して、問題を再現します。リオーダー トーンは、Cisco Unified Communications Manager で許容可能なコール数が制限されている、ロケーションベースのアドミッション制御またはゲートキーパーベースのアドミッション制御に関わる設定の問題によって発生します。SDI トレースでコールを特定し、そのコールがルート パターンやコーリング サーチ スペース、またはその他の設定値によって意図的にブロックされたのかどうかを確認します。
4. リオーダー トーンは、コールが PSTN 経由で発信されている場合にも発生する可能性があります。SDI トレースを調べて、Q.931 メッセージ（特に接続解除メッセージ）がないかどうかを確認します。Q.931 接続解除メッセージが見つかった場合、接続解除の原因は相手側にあるため、こちら側では修正できないことを意味します。

## ゲートウェイの登録障害

ここでは、2 つの類似しているけれども同一ではないゲートウェイ カテゴリについて説明します。Cisco Access AS-X と AT-X および Cisco Access DT-24+ と DE-30+ は 1 つのカテゴリに属します。これらのゲートウェイは、Network Management Processor（NMP; ネットワーク管理プロセッサ）に直接接続されないスタンドアロン ユニットです。2 つめのカテゴリには、Analog Access WS-X6624 および Digital Access WS-X6608 が含まれます。これらのゲートウェイは、Catalyst 6000 シャーシにインストールされているブレードとして、制御およびステータス管理のために NMP に直接接続できます。

### 症状

登録の問題は、Cisco Unified Communications Manager のゲートウェイで発生する最も一般的な問題の 1 つです。

### 考えられる原因

登録は、さまざまな理由で失敗する可能性があります。

### 推奨処置

1. 最初に、ゲートウェイが開始され、実行されていることを確認します。すべてのゲートウェイに、ゲートウェイ ソフトウェアが正常に実行しているときには 1 秒間隔で点滅するハートビート LED があります。

   この LED が点滅していない場合、または非常に高速に点滅している場合は、ゲートウェイ ソフトウェアが実行していないことを示します。結果として、通常、ゲートウェイは自動的にリセットされます。また、2 ～ 3 分経っても登録処理が完了しない場合にゲートウェイがそれ自体でリセットするのは、正常な動作であると見なします。そのため、デバイスのリセット中にハートビート LED をたまたま確認したときに、10 ～ 15 秒経っても通常の点滅パターンが表示されない場合、ゲートウェイで重大な障害が発生しています。

   Cisco Access Analog ゲートウェイでは、前面パネルの右端に緑色のハートビート LED があります。Cisco Access Digital ゲートウェイでは、カードの左上端に赤い LED があります。Cisco Analog Access WS-X6624 では、ブレード内部（前面パネルからは見えない）の前面に近いカードの右端に緑色の LED があります。最後に、Digital Access WS-X6608 では、ブレードの 8 つのスパンのそれぞれに個別のハートビート LED があります。8 つの赤い LED は、背面に向かって約 3 分の 2 のところにカードを横切る形で（前面パネルからは見えない）配置されています。

2. ゲートウェイが自身の IP アドレスを受信していることを確認します。スタンドアロン ゲートウェイは、DHCP または BOOTP を使用して自身の IP アドレスを受信する必要があります。Catalyst ゲートウェイは、DHCP や BOOTP を使用して、または NMP による手動設定で、自身の IP アドレスを受信することがあります。
3. DHCP サーバにアクセスできる場合、スタンドアロン ゲートウェイを確認する最善の方法は、デバイスに未処理の IP アドレス リースがないかどうかを確認することです。ゲートウェイがサーバ上に表示される場合、この方法はよい目安になりますが、決定的ではありません。DHCP サーバでリースを削除します。
4. ゲートウェイをリセットします。
5. 2 ～ 3 分以内にゲートウェイがリースとともにサーバに再表示される場合、このエリアではすべてが正常に動作します。再表示されない場合、ゲートウェイは DHCP サーバに接続できないか（ルータが正しく設定され、DHCP ブロードキャストに転送されていないこと、およびサーバが実行されていることを確認してください）、または肯定応答を受信できません（IP アドレス プールが枯渇していないことを確認してください）。
6. このような確認を行っても答えが得られない場合は、スニファ トレースを使用して問題を特定します。
7. Catalyst 6000 ゲートウェイの場合、NMP がゲートウェイと確実に通信できることを確認する必要があります。これを確認するには、NMP から内部 IP アドレスに **ping** します。

   IP アドレスには次の形式が使用されます。

   ```
   127.1.module.port

   For example, for port 1 on module 7, you would enter
   Console (enable) ping 127.1.7.1
   127.1.7.1 is alive
   ```

8. ping が機能している場合、**show port** コマンドを使用すると IP アドレス情報が表示されます。IP アドレス情報および TFTP IP アドレスが正しいことを確認します。
9. ゲートウェイが有効な DHCP 情報の取得に失敗している場合は、tracy ユーティリティ（Cisco TAC で提供）を使用して問題を特定します。
10. TAC からこのユーティリティを取得したあと、Cat6000 Command Line Interface（CLI; コマンドライン インターフェイス）から次のコマンドを発行します。

    **tracy_start** *mod port*

    この例では、WS-X6624 はモジュール 7 に相当し、860 プロセッサが 1 つしかないため、これがポート 1 になります。コマンド **tracy_start 7 1** を発行します。

    ゲートウェイ ボード自体の 860 コンソール ポートから実際に出力される結果は次のとおりです。ただし、tracy コマンドの出力は 860 コンソール ポートのリモート コピーです。

    ```
          |             |
          |             |
        | | |         | | |
       | | | | |     | | | | |
    | | | | | |:.:| | | | | | |:..
    C i s c o   S y s t e m s
    CAT6K Analog Gateway (ELVIS)
    APP Version : A0020300, DSP Version : A0030300, Built Jun  1 2000 16:33:01

    ELVIS>> 00:00:00.020 (XA) MAC Addr : 00-10-7B-00-13-DE
    00:00:00.050 NMPTask:got message from XA Task
    00:00:00.050 (NMP) Open TCP Connection ip:7f010101
    00:00:00.050 NMPTask:Send Module Slot Info
    00:00:00.060 NMPTask:get DIAGCMD
    ```

```
00:00:00.160 (DSP) Test Begin -> Mask<0x00FFFFFF>
00:00:01.260 (DSP) Test Complete -> Results<0x00FFFFFF/0x00FFFFFF>
00:00:01.260 NMPTask:get VLANCONFIG
00:00:02.870 (CFG) Starting DHCP
00:00:02.870 (CFG) Booting DHCP for dynamic configuration.
00:00:06.570 (CFG) DHCP Request or Discovery Sent, DHCPState = INIT_REBOOT
00:00:06.570 (CFG) DHCP Server Response Processed, DHCPState = INIT_REBOOT
00:00:06.780 (CFG) IP Configuration Change!  Restarting now...
00:00:10.480 (CFG) DHCP Request or Discovery Sent, DHCPState = INIT
00:00:14:480 (CFG) DHCP Timeout Waiting on Server, DHCPState = INIT
00:00:22:480 (CFG) DHCP Timeout Waiting on Server, DHCPState = INIT
00:00:38:480 (CFG) DHCP Timeout Waiting on Server, DHCPState = INIT
```

このタイムアウト メッセージが延々とスクロール表示される場合は、DHCP サーバへの接続に問題があります。

11. 最初に、Catalyst 6000 ゲートウェイ ポートが正しい VLAN 内にあることを確認します。

    この情報は、**show port** コマンドを使用して取得した情報に含まれています。

12. DHCP サーバが Catalyst 6000 ゲートウェイと同じ VLAN に配置されていない場合、DHCP 要求を DHCP サーバに転送するように適切な IP ヘルパー アドレスが設定されていることを確認します。ゲートウェイは、VLAN 番号が変更されたあと、ゲートウェイがリセットされるまで、INIT 状態のままになる可能性があります。

13. INIT 状態になっている場合は、ゲートウェイをリセットします。860 がリセットされるたびに tracy セッションが失われるため、次のコマンドを発行して既存のセッションを閉じ、新しいセッションを再確立する必要があります。

    **tracy_close** *mod port*

    **tracy_start** *mod port*

14. それでもまだ **DHCPState = INIT** メッセージが表示される場合は、DHCP サーバが正しく動作しているかどうかを確認します。

15. 正しく動作している場合は、スニファ トレースを開始して、要求が送信されているかどうか、およびサーバが応答しているかどうかを確認します。

    DHCP が正しく動作している場合は、tracy デバッグ ユーティリティを使用できるようにする IP アドレスがゲートウェイに割り当てられます。このユーティリティには、Catalyst ゲートウェイ用に設定された NMP コマンドの組み込み機能が含まれており、Windows 98/NT/2000 で実行するヘルパー アプリケーションとしてスタンドアロン ゲートウェイに使用できます。

16. ヘルパー アプリケーションとして tracy ユーティリティを使用するには、割り当てられている IP アドレスを使用してゲートウェイに接続します。この tracy アプリケーションはすべてのゲートウェイで動作し、ゲートウェイごとに個別のトレース ウィンドウを提供して（一度に最大 8 つのトレースが可能）、指定されたファイルにトレースを直接記録できるようにします。

17. TFTP サーバの IP アドレスがゲートウェイに正しく提供されていることを確認します。DHCP は、通常、オプション 66（名前または IP アドレス）、オプション 150（IP アドレス限定）、または si_addr（IP アドレス限定）で DHCP を提供します。サーバに複数のオプションが設定されている場合、si_addr はオプション 150 に優先し、オプション 150 はオプション 66 に優先します。

    オプション 66 で TFTP サーバの DNS_NAME が提供される場合、DNS サーバの IP アドレスは DHCP で指定されている必要があり、さらにオプション 66 で入力された名前は正しい TFTP サーバの IP アドレスに解決される必要があります。NMP では DHCP をディセーブルにするように Catalyst ゲートウェイを設定できます。その場合、NMP オペレータはコンソールで、TFTP サーバ アドレスなどの設定パラメータをすべて手動で入力する必要があります。

    また、ゲートウェイは常に DNS を使用して名前 CiscoCM1 を解決しようとします。解決に成功した場合、CiscoCM1 の IP アドレスは、NMP で DHCP がディセーブルになっていても、DHCP サーバまたは NMP が TFTP サーバ アドレスとして示すすべてに優先します。

18. tracy ユーティリティを使用すると、ゲートウェイにある現在の TFTP サーバの IP アドレスを確認できます。次のコマンドを入力して、設定タスク番号を取得します。

```
TaskID: 0
Cmd:    show tl
```

config または CFG を含む行を探して、対応する番号を次の行（Cisco Access Digital ゲートウェイなど）の taskID として使用します。次の例では、テキスト行を太字にすることで説明されているメッセージをわかりやすくしています。実際の出力では、テキストは太字で表示されません。これらの例は WS-X6624 モデルの出力です。DHCP 情報をダンプするコマンドは次のとおりです。

```
TaskID: 6
Cmd:     show dhcp
```

19. これで、TFTP サーバの IP アドレスが表示されます。この IP アドレスが正しくない場合は、表示された DHCP オプションおよび他の情報が正しいかどうかを確認します。

20. TFTP アドレスが正しい場合、ゲートウェイが TFTP サーバから自身の設定ファイルを取得していることを確認します。tracy 出力に次の情報が表示された場合、TFTP サービスが正しく動作していないか、またはゲートウェイが Cisco Unified Communications Manager で設定されていないことがあります。

```
00:09:05.620 (CFG) Requesting SAA00107B0013DE.cnf File From TFTP Server
00:09:18.620 (CFG) TFTP Error: Timeout Awaiting Server Response for .cnf File!
```

ゲートウェイは、設定ファイルを取得していない場合に、TFTP サーバと同じ IP アドレスに接続しようとします。この試みは、ゲートウェイで冗長 Cisco Unified Communications Manager のリストを受信する必要があるクラスタ環境でないかぎり、成功します。

21. カードが TFTP 情報を正しく取得していない場合、Cisco Unified Communications Manager の TFTP サービスを調べて、このサービスが動作していることを確認します。

22. Cisco Unified Communications Manager の TFTP トレースを確認します。

Cisco Unified Communications Manager でゲートウェイが正しく設定されていない場合は、別の一般的な問題が発生します。典型的なエラーとしては、ゲートウェイに不正な MAC アドレスが入力されている場合があります。この場合、Catalyst 6000 ゲートウェイでは、次のメッセージが 2 分ごとに NMP コンソールに表示されます。

```
2000 Apr 14 19:24:08 %SYS-4-MODHPRESET:Host process (860) 7/1 got reset asynchronously
2000 Apr 14 19:26:05 %SYS-4-MODHPRESET:Host process (860) 7/1 got reset asynchronously
2000 Apr 14 19:28:02 %SYS-4-MODHPRESET:Host process (860) 7/1 got reset asynchronously

The following example shows what the tracy output would look like if the gateway is
not in the Cisco CallManager database:
00:00:01.670 (CFG) Booting DHCP for dynamic configuration.
00:00:05.370 (CFG) DHCP Request or Discovery Sent, DHCPState = INIT_REBOOT
00:00:05.370 (CFG) DHCP Server Response Processed, DHCPState = BOUND
00:00:05.370 (CFG) Requesting DNS Resolution of CiscoCM1
00:00:05.370 (CFG) DNS Error on Resolving TFTP Server Name.
00:00:05.370 (CFG) TFTP Server IP Set by DHCP Option 150 = 10.123.9.2
00:00:05.370 (CFG) Requesting SAA00107B0013DE.cnf File From TFTP Server
00:00:05.370 (CFG) TFTP Error: .cnf File Not Found!
00:00:05.370 (CFG) Requesting SAADefault.cnf File From TFTP Server
00:00:05.380 (CFG) .cnf File Received and Parsed Successfully.
00:00:05.380 (CFG) Updating Configuration ROM...
00:00:05.610 GMSG: GWEvent = CFG_DONE --> GWState = SrchActive
00:00:05.610 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState = AttemptingSocket
00:00:05.610 GMSG: Attempting TCP socket with CM 10.123.9.2
00:00:05.610 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = BackupUnified CM
00:00:05.610 GMSG: GWEvent = SOCKET_ACK --> GWState = RegActive
00:00:05.610 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState = SentRegister
00:00:05.680 GMSG: CCM#0 CPEvent = CLOSED --> CPState = NoTCPSocket
```

```
00:00:05.680 GMSG: GWEvent = DISCONNECT --> GWState = Rollover
00:00:20.600 GMSG: GWEvent = TIMEOUT --> GWState = SrchActive
00:00:20.600 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState = AttemptingSocket
00:00:20.600 GMSG: Attempting TCP socket with CM 10.123.9.2
00:00:20.600 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = Backup CCM
```

他に発生する可能性がある登録の問題としては、ロード情報が正しくない、またはロード ファイルが破損しているといった問題もあります。問題は、TFTP サーバが動作していない場合にも発生する可能性があります。このような場合、ファイルが見つからないという TFTP サーバからの報告が、tracy によって次のように表示されます。

```
00:00:07.390 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState = SentRegister
00:00:08.010 GMSG: TFTP Request for application load A0021300
00:00:08.010 GMSG: CCM#0 CPEvent = LOADID --> CPState = AppLoadRequest
00:00:08.010 GMSG: ***TFTP Error: File Not Found***
00:00:08.010 GMSG: CCM#0 CPEvent = LOAD_UPDATE --> CPState = LoadResponse
```

この場合、実際のロード名は A0020300 ですが、ゲートウェイはアプリケーション ロード A0021300 を要求しています。Catalyst 6000 ゲートウェイでは、新しいアプリケーション ロードで対応する DSP ロードの取得も必要になる場合に、同じ問題が発生する可能性があります。新しい DSP ロードが見つからない場合、同様のメッセージが表示されます。

```
ELVIS>> 00:00:00.020 (XA) MAC Addr : 00-10-7B-00-13-DE
00:00:00.050 NMPTask:got message from XA Task
00:00:00.050 (NMP) Open TCP Connection ip:7f010101
00:00:00.050 NMPTask:Send Module Slot Info
00:00:00.060 NMPTask:get DIAGCMD
00:00:00.160 (DSP) Test Begin -> Mask<0x00FFFFFF>
00:00:01.260 (DSP) Test Complete -> Results<0x00FFFFFF/0x00FFFFFF>
00:00:01.260 NMPTask:get VLANCONFIG
00:00:02.030 (CFG) Starting DHCP
00:00:02.030 (CFG) Booting DHCP for dynamic configuration.
00:00:05.730 (CFG) DHCP Request or Discovery Sent, DHCPState = INIT_REBOOT
00:00:05.730 (CFG) DHCP Server Response Processed, DHCPState = BOUND
00:00:05.730 (CFG) Requesting DNS Resolution of CiscoCM1
00:00:05.730 (CFG) DNS Error on Resolving TFTP Server Name.
00:00:05.730 (CFG) TFTP Server IP Set by DHCP Option 150 = 10.123.9.2
00:00:05.730 (CFG) Requesting SAA00107B0013DE.cnf File From TFTP Server
00:00:05.730 (CFG) .cnf File Received and Parsed Successfully.
00:00:05.730 GMSG: GWEvent = CFG_DONE --> GWState = SrchActive
00:00:05.730 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState = AttemptingSocket
00:00:05.730 GMSG: Attempting TCP socket with CM 10.123.9.2
00:00:05.730 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = Backup CCM
00:00:05.730 GMSG: GWEvent = SOCKET_ACK --> GWState = RegActive
00:00:05.730 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState = SentRegister
00:00:06.320 GMSG: CCM#0 CPEvent = LOADID --> CPState = LoadResponse
00:01:36.300 GMSG: CCM#0 CPEvent = TIMEOUT --> CPState = BadUnified CM
00:01:36.300 GMSG: GWEvent = DISCONNECT --> GWState = Rollover
00:01:46.870 GMSG: CCM#0 CPEvent = CLOSED --> CPState = NoTCPSocket
00:01:51.300 GMSG: GWEvent = TIMEOUT --> GWState = SrchActive
00:01:51.300 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState = AttemptingSocket
00:01:51.300 GMSG: Attempting TCP socket with CM 10.123.9.2
00:01:51.300 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = Backup CCM
00:01:51.300 GMSG: GWEvent = SOCKET_ACK --> GWState = RegActive
00:01:51.300 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState = SentRegister
00:01:51.890 GMSG: Unified CM#0 CPEvent = LOADID --> CPState = LoadResponse
```

ここで異なるのは、ゲートウェイが **LoadResponse** 段階のままになり、最終的にはタイムアウトすることです。この問題は、Cisco Unified Communications Manager の管理ページの [デバイスのデフォルト（Device Defaults）] エリアでロード ファイル名を修正することにより解決できます。

# ゲートキーパーの問題

ゲートキーパーのトラブルシューティングを開始する前に、ネットワーク内に IP 接続が存在することを確認します。ここでは、IP 接続が存在するという前提で、次の情報を使用してゲートキーパーのコールをトラブルシューティングします。


- 「アドミッション拒否」（P.4-18）
- 「登録拒否」（P.4-18）


## アドミッション拒否

### 症状

Cisco Unified Communications Manager がゲートキーパーに登録されているにもかかわらず電話コールを送信できない場合、システムによって Admission Reject（ARJ; アドミッション拒否）が発行されます。

### 考えられる原因

ゲートキーパーによって ARJ が発行される場合、ゲートキーパーの設定の問題に注目する必要があります。

### 推奨処置

1. Cisco Unified Communications Manager からゲートキーパーへの IP 接続を確認します。
2. ゲートキーパーのステータスを表示して、ゲートキーパーがアップ状態であることを確認します。
3. ゾーン サブセットがゲートキーパーに定義されていることを確認します。定義されている場合、Cisco Unified Communications Manager のサブネットが、許可されているサブネットに含まれていることを確認します。
4. Cisco Unified Communications Manager とゲートキーパーの設定間で、テクノロジー プレフィクスが一致していることを確認します。
5. 帯域幅の設定を確認します。

## 登録拒否

### 症状

Cisco Unified Communications Manager をゲートキーパーに登録できない場合、システムによって Registration Reject（RRJ; 登録拒否）が発行されます。

### 考えられる原因

ゲートキーパーによって RRJ が発行されている場合、ゲートキーパーの設定の問題に注目する必要があります。

### 推奨処置

1. Cisco Unified Communications Manager からゲートキーパーへの IP 接続を確認します。
2. ゲートキーパーのステータスを表示して、ゲートキーパーがアップ状態であることを確認します。
3. ゾーン サブセットがゲートキーパーに定義されていることを確認します。定義されている場合、ゲートウェイのサブネットが、許可されているサブネットに含まれていることを確認します。

# Restart_Ack に Channel IE が含まれていない場合に B チャネルがロック状態のままになる

### 症状

Cisco Unified Communications Manager システムで ie=channel not available という理由付きの Release Complete を受信すると、システムは Restart を送信してこのチャネルをアイドル状態に戻します。

### 考えられる原因

Restart では、Channel IE を使用して、再起動する必要があるチャネルを指定します。ネットワークが Channel IE を含まない Restart_Ack で応答してきた場合、システムはこのチャネルをロック状態のままにします。一方、ネットワーク側では、同じチャネルがアイドル状態に戻されます。

その結果、ネットワークから着信コール用にこのチャネルが要求されることになります。

チャネルは Cisco Unified Communications Manager サーバでロックされるため、Cisco Unified Communications Manager はこのチャネルのすべてのコール要求を解放します。

この動作は、UK の多数のサイトで、ゲートウェイが E1 ブレードの場合に発生します（2600/3600 で MGCP バックホールが使用されている場合にも同じ動作が発生する可能性が高くなります）。

グレア状態は Release Complete の原因となることがあります。

この状態は、大量のコールが発生するサイトで頻繁に発生します。

ネットワークでの B チャネル選択がトップダウンまたはボトムアップの場合、上位または下位の B チャネルが解放されるまで、着信コールはすべて失敗します（アクティブ コールがクリアされた場合）。

B チャネル選択が特定の時間のラウンドロビンである場合、E1 ブレードの B チャネルがすべてロックされることになります。

### 推奨処置

E1 ポートをリセットします。

検証

B チャネルがアイドル状態に戻ります。

# 不正なデバイス登録ステータスが表示される

### 症状

Cisco Unified CM の管理のデバイス ウィンドウに、不正なデバイス登録ステータスが表示されます。

### 考えられる原因

Cisco RIS Data Collector サービスによって、現在のデバイス登録ステータスが Cisco Unified CM の管理ウィンドウに表示されます。ステータスが表示されない場合、次のいずれかの原因が存在することがあります。

Cisco RIS Data Collector サービスが実行していない、または応答していない。

ネットワーク接続の問題または DNS 名前解決の問題が存在しているため、Cisco Unified CM の管理で Cisco RIS Data Collector サービスとの通信を確立できない。

### 推奨処置

1. Cisco Unified Serviceability を使用して、Cisco RIS Data Collector サービスが実行していることを確認します。サービスが実行している場合は、サービスを再起動します。サービス ステータスの確認およびサービスの再起動に関する詳細は、『*Cisco Unified Serviceability Administration Guide*』を参照してください。
2. 次の点を確認します。
   - DNS サーバが適切に設定され、使用可能になっている。
   - ホスト ファイルに、Cisco Unified Communications Manager サーバに対する適切なマッピングが含まれている。
   - クラスタ内の Cisco Unified Communications Manager サーバに DNS 解決の問題がない。
   - ローカル サーバ名をホストファイルに追加して、ipconfig /flushdns、ipconfig /registerdns、iisrest を実行している。

**（注）** DNS 解決を確認するには、nslookup ツールでクラスタ内のサーバのホスト名を解決できることを確認します。