CISCO SYSTEMS

Cisco CallManager
トラブルシューティング ガイド

Release 4.1(3)

Text Part Number: OL-7171-01-J

CONTENTS

FIGURES

このマニュアルについて

ここでは、このマニュアルの目的、対象読者、構成、および表記法について説明します。また、関連マニュアルを入手する方法についても説明します。

次のトピックについて取り上げます。

目的

『*Cisco CallManager トラブルシューティング ガイド*』では、Cisco CallManager のトラブルシューティングの手順について説明しています。このマニュアルは、Cisco CallManager システムで発生する可能性のあるすべてのトラブル事象を網羅しているわけではなく、Cisco Technical Assistance Center（TAC）で頻繁に扱っているトラブル事象やニュースグループから頻繁に問い合せのある質問を重点的に取り上げています。

対象読者

『*Cisco CallManager トラブルシューティング ガイド*』は、企業の管理者および従業員のために Cisco CallManager システムの管理を担当するネットワーク管理者を対象としています。テレフォニーおよび IP ネットワーキング テクノロジーに関する知識が必要です。

マニュアルの構成

表 1 は、このマニュアルの構成を示しています。

表 1　　このマニュアルの構成

章とタイトル	説明
第 1 章「トラブルシューティングの概要」	Cisco CallManager のトラブルシューティングに利用できるツールとリソースの概要を説明します。
第 2 章「トラブルシューティング ツール」	Cisco CallManager 4.0（またはそれ以降）の設定、監視、およびトラブルシューティングに使用するツールとユーティリティについて説明し、同じデータを何度もテストしたり再収集したりするのを避けるために情報収集に関する一般的なガイドラインを示します。
第 3 章「インストール、バックアップ、および復元の問題」	Cisco CallManager のインストール、バックアップ、または復元に関連する最も一般的な問題の解決方法について説明します。
第 4 章「Cisco CallManager システムの問題」	Cisco CallManager システムに関連する最も一般的な問題の解決方法について説明します。
第5章「ディレクトリの問題」	Cisco CallManager DC Directory（DCD）、Lightweight Directory Access Protocol（LDAP）ディレクトリ、または Microsoft Active Directory（AD）に関連する最も一般的な問題の解決方法について説明します。
第 6 章「デバイスの問題」	IP Phone とゲートウェイに関連する最も一般的な問題の解決方法について説明します。
第 7 章「ダイヤル プランとルーティングの問題」	ダイヤル プラン、ルート パーティション、およびコール検索スペース（コーリング サーチ スペース）に関連する最も一般的な問題の解決方法について説明します。
第 8 章「Cisco CallManager サービスの問題」	会議ブリッジやメディア終端点などのサービスに関連する最も一般的な問題の解決方法について説明します。

表 1　　このマニュアルの構成 （続き）

章とタイトル	説明
第 9 章「ボイス メッセージの問題」	ボイス メッセージに関連する最も一般的な問題の解決方法について説明します。
付録 A「TAC への問い合せ」	TAC に問い合せを行う際に必要となる情報について説明します。
付録 B「ケース スタディ：クラスタ内コール のトラブルシューティング」	同一クラスタ内にある 2 台の Cisco IP Phone 間のコール フローについて詳細に説明します。
付録 C「ケース スタディ：Cisco IP Phone と Cisco IOS Gateway 間のコールのトラブルシューティング」	ローカル PBX または Public Switched Telephone Network（PSTN; 公衆電話交換網）に接続された電話機に Cisco IOS Gateway を介してコールを発信する Cisco IP Phone について説明します。
付録 D「ケース スタディ：クラスタ間コールのトラブルシューティング」	異なるクラスタに配置された別の Cisco IP Phone にコールを発信する Cisco IP Phone について説明します。

関連マニュアル

Cisco IP Telephony 関連のアプリケーションと製品の詳細は、次の資料を参照してください。

- *Cisco CallManager API Troubleshooting Guide*
- *Cisco CallManager アドミニストレーション ガイド*
- *Cisco CallManager システム ガイド*
- *Cisco CallManager Serviceability アドミニストレーション ガイド*
- *Cisco CallManager 機能およびサービス ガイド*
- *Cisco CallManager Quick Start Guide*
- *Cisco CallManager Installation Instructions*
- *Cisco CallManager Backup and Restore Procedure*
- *Cisco CallManager Attendant Console ユーザ ガイド*
- *Cisco CallManager Multilevel Administration Access Guide*
- *Cisco CallManager Directory Services Guide*
- *Release Notes for Cisco CallManager*
- *Cisco CallManager Documentation Guide*
- *Hardware Configuration Guide for the Cisco Voice Gateway 200*
- *Software Configuration Guide for the Cisco Voice Gateway 200*
- *Cisco IP Phone アドミニストレーション ガイド for Cisco CallManager*
- *Cisco CallManager Bulk Administration Tool ユーザ ガイド*
- *Cisco Technical Solution Series: IP Telephony Solution Guide*
- *Guide to Cisco Systems VOIP Infrastructure Solution for SIP*

表記法

このマニュアルは、次の表記法を使用しています。

表記法	説明
太字	コマンドおよびキーワードは、**太字**で示しています。
イタリック体	ユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{ x | y | z }	必ずどれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
ストリング	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。
`screen` フォント	システムが表示する端末セッションおよび情報は、`screen` フォントで示しています。
太字の `screen` フォント	ユーザが入力しなければならない情報は、太字の **`screen`** フォントで示しています。
イタリック体の `screen` フォント	ユーザが値を指定する引数は、イタリック体の *`screen`* フォントで示しています。
< >	パスワードのように出力されない文字は、かぎカッコで囲んで示しています。

（注）は、次のように表しています。

（注） 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

ワンポイント・アドバイスでは、次の表記法を使用しています。

ワンポイント・アドバイス　時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。

ヒントでは、次の表記法を使用しています。

ヒント　便利なヒントです。

注意は、次のように表しています。

注意　「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告は、次の表記法を使用しています。

警告　**「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の作業を行うときは、電気回路の危険性および一般的な事故防止対策に十分注意してください。**

技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。また、テクニカル サポートおよびその他のリソースを、さまざまな方法で入手することができます。ここでは、シスコ製品に関する技術情報を入手する方法について説明します。

Cisco.com

マニュアルの最新版は、次の URL で参照できます。

http://www.cisco.com/univercd/home/home.htm

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

また、シスコの Web サイトの各国語版へは、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスできます。

http://www.cisco.com/jp

マニュアルの発注方法（英語版）

英文マニュアルの発注方法については、次の URL にアクセスしてください。

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

シスコ製品の英文マニュアルは、次の方法で発注できます。

- Cisco.com（Cisco Direct Customers）に登録されている場合、Ordering Tool からシスコ製品の英文マニュアルを発注できます。次の URL にアクセスしてください。

  http://www.cisco.com/en/US/partner/ordering/index.shtml
- Cisco.com に登録されていない場合、製品を購入された代理店へお問い合せください。

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

http://www2.hipri.com/cisco/

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

http://www2.hipri.com/cisco/

なお、技術内容に関するお問い合せは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合せください。

テクニカル サポート

シスコと正式なサービス契約を交わしているすべてのお客様、パートナー、および代理店は、Cisco Technical Support で 24 時間テクニカル サポートを利用することができます。Cisco.com の Cisco Technical Support Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、Cisco Technical Assistance Center（TAC）のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合せください。

Cisco Technical Support Web サイト

Cisco Technical Support Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間 365 日、いつでも利用可能です。URL は次のとおりです。

http://www.cisco.com/techsupport

Cisco Technical Support Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます（S3：ネットワークに軽微な障害が発生した、S4：製品情報が必要である）。状況を入力すると、その状況を解決するための推奨手段が自動的に検索されます。これらの推奨手段で問題を解決できない場合は、Cisco TAC のエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合せください（S1：ネットワークがダウンした、S2：ネットワークの機能が著しく低下した）。S1 および S2 のサービス リクエストには、Cisco TAC のエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

http://www.cisco.com/techsupport/contacts

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1（S1）：ネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2（S2）：既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3（S3）：ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4（S4）：シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手方法

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

  http://www.cisco.com/go/marketplace/

- 『*Cisco Product Catalog*』には、シスコシステムズが提供するネットワーキング製品のほか、発注方法やカスタマー サポート サービスについての情報が記載されています。『*Cisco Product Catalog*』には、次の URL からアクセスしてください。

  http://cisco.com/univercd/cc/td/doc/pcat/

- Cisco Press では、ネットワーキング全般、トレーニング、および認定資格に関する書籍を広範囲にわたって出版しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版物やその他の情報を調べるには、次の URL から Cisco Press にアクセスしてください。

  http://www.ciscopress.com

- 『*Packet*』はシスコシステムズが発行する技術者向けの雑誌で、インターネットやネットワークへの投資を最大限に活用するために役立ちます。本誌は季刊誌として発行され、業界の最先端トレンド、最新テクノロジー、シスコ製品やソリューション情報が記載されています。また、ネットワーク構成およびトラブルシューティングに関するヒント、コンフィギュレーション例、カスタマー ケース スタディ、認定情報とトレーニング情報、および充実したオンライン サービスへのリンクの内容が含まれます。『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/packet

  日本語版『*Packet*』は、米国版『*Packet*』と日本版のオリジナル記事で構成されています。日本語版『*Packet*』には、次の URL からアクセスしてください。

  http://www.cisco.com/japanese/warp/public/3/jp/news/packet/

- 『*iQ Magazine*』はシスコシステムズの季刊誌で、成長企業が収益を上げ、業務を効率化し、サービスを拡大するためには技術をどのように利用したらよいかを学べるように構成されています。本誌では、実例とビジネス戦略を挙げて、成長企業が直面する問題とそれを解決するための技術を紹介し、読者が技術への投資に関して適切な決定を下せるよう配慮しています。『*iQ Magazine*』には、次の URL からアクセスしてください。

  http://www.cisco.com/go/iqmagazine

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。トレーニングの最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html

トラブルシューティングの概要

この章では、Cisco CallManager のトラブルシューティングで必要となる背景情報や使用できるリソースについて説明します。

この章では、次のトピックについて取り上げます。

Cisco CallManager

Cisco CallManager は、Cisco Architecture for Voice, Video and Integrated Data（AVVID）の一部である、企業向け Cisco IP テレフォニー ソリューションのソフトウェアベースのコール処理コンポーネントを提供します。

Cisco CallManager システムは、企業のテレフォニー機能を、IP Phone、メディア処理デバイス、voice-over-IP（VoIP）ゲートウェイ、マルチメディア アプリケーションなど、パケット テレフォニー デバイスにまで拡張します。

その他にも、統合メッセージング、マルチメディア会議、コラボラティブなコンタクト センター、対話型マルチメディア応答システムなど、データ、音声、ビデオの各サービスは、Cisco CallManager オープン テレフォニー アプリケーション プログラム インターフェイス（API）を介して情報を交換します。

Cisco CallManager システムには、音声会議や手動コンソール機能を実行するための統合音声アプリケーション群が組み込まれています。この音声アプリケーション群があるので、音声処理用の特別なハードウェアが不要となります。

保留、任意転送、自動転送、会議、複数回線の着信表示、自動ルート選択、短縮ダイヤル、最後にダイヤルした番号のリダイヤルなど、補助的な拡張サービスが IP Phone とゲートウェイに付加されます。Cisco CallManager はソフトウェア アプリケーションであるため、サーバ プラットフォームでソフトウェアをアップグレードするだけで、実稼働環境で機能を拡張できます。

IP ネットワークを介して Cisco CallManager とすべての Cisco IP Phone、ゲートウェイ、およびアプリケーションを分散させることにより、分散型の仮想テレフォニー ネットワークが構築されます。このアーキテクチャにより、システムのアベイラビリティとスケーラビリティが向上します。コール アドミッション制御により、帯域幅に制約のある WAN リンク全体で音声の quality of service（QoS; サービス品質）が保証され、WAN 帯域幅が使用できない場合は代わりの public switched telephone network（PSTN; 公衆電話交換網）のルートにコールが転送されます。

データベースへの Web ベースのインターフェイスである Cisco CallManager Administration により、リモート デバイスとリモート システムの設定機能およびサービサビリティが提供されます。また、このインターフェイスを使用して、ユーザおよび管理者が HTML ベースのオンライン ヘルプにアクセスすることもできます。

サービサビリティ

管理者は、Cisco CallManager Administration サービス ツールを使用して、システム問題のトラブルシューティングを行うことができます。この Web ベースのツール Serviceability は、次のサービスを提供します。

- アラーム：トラブルシューティングに備えて、Cisco CallManager サービスによって生成されたアラームとイベントを保存し、アラーム メッセージ定義を提供します。
- トレース：トラブルシューティングに備えて、Cisco CallManager サービスによって生成されたトレース情報をさまざまなログ ファイルに保存します。管理者は、トレース情報を設定、収集、および分析できます。
- Real-Time Monitoring Tool：Cisco CallManager クラスタ内のコンポーネントの動作をリアルタイムで監視します。
- Service Activation：Cisco CallManager サービスのアクティベーション ステータスを表示します。管理者は、Service Activation を使用して、サービスをアクティブおよび非アクティブにします。
- Control Center：Cisco CallManager サービスのステータスを表示します。管理者は、Control Center を使用して、サービスを開始および停止します。
- Quality Report Tool（QRT）：Cisco IP Phone 7940 と 7960 の音声品質および一般的な問題を報告するツールとして機能します。

Serviceability にアクセスするには、Cisco CallManager Administration ウィンドウのメニューバーから Applications を選択します。Cisco CallManager ソフトウェアをインストールすると、Serviceability が自動的にインストールされて使用できるようになります。

サービサビリティ ツールの詳細および設定手順については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』および『*Cisco CallManager Serviceability システム ガイド*』を参照してください。

ハードウェアおよびソフトウェアの互換性

すべての Cisco CallManager コンポーネントの互換バージョンについては、『*Cisco CallManager Compatibility Matrix*』を参照してください。

一般的な問題解決モデル

テレフォニーまたは IP ネットワーク環境でトラブルシューティングを行う場合は、症状を見極め、その症状を引き起こしていると考えられるすべての問題を洗い出し、症状がなくなるまで、考えられるそれぞれの問題を体系的に（可能性の高いものから順番に）排除していきます。

次の手順は、問題解決プロセス用のガイドラインを示しています。

ステップ 1　ネットワークの問題を分析し、問題点を明確に記述します。症状および考えられる原因を明らかにします。

ステップ 2　問題の原因を特定するために役立つファクト（事実）を収集します。

ステップ 3　収集したファクトに基づいて、考えられる原因を検討します。

ステップ 4　その原因に基づいて、アクション　プランを作成します。最も可能性の高い問題から着手し、1 つの変数だけを操作するプランになるようにします。

ステップ 5　アクション　プランを実施します。テストして症状が消えたかどうかを確認しながら、各手順を慎重に実行します。

ステップ 6　結果を分析し、問題が解決したかどうかを確認します。問題が解決した場合、プロセスは完了です。

ステップ 7　問題が解決していない場合は、上記のリストで次に可能性の高い原因に基づいてアクション プランを作成します。ステップ 4 に戻り、問題が解決するまでプロセスを繰り返します。

アクション プランの実施中に何かを変更した場合は、必ずその変更を取り消してください。一度に 1 つの変数だけを変更してください。

（注）　一般的な対策（本書で説明しているもの、または環境に応じて独自に考案したもの）をすべて実施しても問題が解決しない場合は、Cisco TAC に連絡してください。

ネットワーク障害への事前準備

ネットワーク障害が発生したときにその回復を容易にするには、事前準備が重要です。ネットワーク障害への事前準備ができているかどうかを判断するには、次の質問に答えてください。

- ネットワーク上のすべてのデバイスの物理的な位置および接続方法を示した、インターネットワークの正確な物理および論理マップがありますか。また、ネットワーク アドレス、ネットワーク番号、およびサブネットワークを記述した論理マップがありますか。
- ネットワークに実装されているすべてのネットワーク　プロトコルのリストと、各プロトコルに関連付けられているネットワーク番号、サブネットワーク、ゾーン、およびエリアのリストがありますか。
- どのプロトコルがルーティングされているか、および各プロトコルについての正確かつ最新の設定情報を知っていますか。
- どのプロトコルがブリッジングされているかを知っていますか。そのブリッジに設定されているフィルタはありますか。その設定のコピーはありますか。そのコピーは Cisco CallManager に適用できますか。
- インターネットへの接続も含めて、外部ネットワークへのすべての接点を知っていますか。各外部ネットワーク接続について、使用されているルーティング プロトコルを知っていますか。
- 現在の問題とベースラインを比較できるように、通常のネットワーク動作およびパフォーマンスについて組織で文書化されていますか。

これらの質問に対して「はい」と答えることができる場合は、障害から迅速に回復できます。

IP テレフォニー ネットワーク

IP テレフォニー ネットワークのトラブルシューティングについては、『*Cisco Technical Solution Series: IP Telephony Solution Guide*』を参照してください。

その他の情報

参考資料

- *Cisco CallManager アドミニストレーション ガイド*
- *Cisco CallManager システム ガイド*
- *Cisco CallManager 機能およびサービス ガイド*
- *Cisco CallManager Serviceability アドミニストレーション ガイド*
- *Cisco CallManager Serviceability システム ガイド*
- *Cisco WebAttendant ユーザ ガイド*
- *BAT Administration Tool ユーザ ガイド*
- *Cisco CallManager Quick Start Guide*
- *Cisco CallManager インストレーション ガイド*
- *Cisco CallManager Attendant Console ユーザ ガイド*
- *Cisco IP Phone アドミニストレーション ガイド for Cisco CallManager*
- *Cisco VG248 Analog Phone Gateway ソフトウェア コンフィギュレーション ガイド*
- *Cisco Conference Connection Administration Guide*
- *Cisco IP Conference Station 7935 アドミニストレーション ガイド*
- *Cisco Technical Solution Series: IP Telephony Solution Guide*
- *Guide to Cisco Systems VOIP Infrastructure Solution for SIP*
- 次の URL にある CiscoWorks2000 のユーザ マニュアル

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/index.htm

CHAPTER 2

トラブルシューティング ツール

この章では、Cisco CallManager 4.0 の設定、監視、およびトラブルシューティングに使用するツールとユーティリティについて説明し、同じデータを何度もテストしたり再収集したりするのを避けるために情報収集に関する一般的なガイドラインを示します。

（注） 本書に示す URL サイトの中には、登録ユーザとしてログインしないとアクセスできないものもあります。

この章では、次のトピックについて取り上げます。

- Sniffer トレース
- デバッグ
- Cisco CallManager トラブルシューティング ツール
- トラブルシューティングのヒント
- その他の情報

Sniffer トレース

通常は、VLAN をスパンするように設定された Catalyst ポートまたはトラブル情報を含むポート（CatOS、Cat6K-IOS、XL-IOS）上で、ラップトップ、または sniffer を装備した他のデバイスを接続することにより、sniffer トレースを収集します。ポートが空いていない場合は、スイッチとデバイスの間に挿入されているハブ上で、sniffer を装備したデバイスを接続します。

ヒント　TAC では Sniffer Pro ソフトウェアが広く使用されているため、TAC エンジニアがトレースを簡単に読み取って解釈できるように、このソフトウェアを使用することをお勧めします。

関係するすべての機器（IP Phone、ゲートウェイ、Cisco CallManager など）の IP アドレスと MAC アドレスを用意しておいてください。

デバッグ

debug 特権 EXEC コマンドからの出力には、プロトコル ステータスやネットワーク アクティビティ全般に関連するさまざまなインターネットワーキング イベントについての診断情報が記載されています。

デバッグ出力をファイルに取り込むことができるように、ターミナル エミュレータ ソフトウェア（HyperTerminal など）を設定します。HyperTerminal では、**Transfer** をクリックし、**Capture Text** をクリックして、適切なオプションを選択します。

IOS 音声ゲートウェイのデバッグを実行する前に、ゲートウェイ上で `service timestamps debug datetime msec` がグローバルに設定されていることを確認します。

（注）　営業時間中にライブ環境でデバッグを収集しないでください。

営業時間外にデバッグを収集することをお勧めします。ライブ環境でデバッグを収集する必要がある場合は、`no logging console` および `logging buffered` を設定します。デバッグを収集するには、**`show log`** を使用します。

デバッグは長くなることがあるため、直接コンソール ポートで（デフォルト **`logging console`**）またはバッファで（**`logging buffer`**）デバッグを収集します。Telnet セッションを介してデバッグを収集すると、デバイスのパフォーマンスが低下して、デバッグが不完全となり、デバッグを再収集する必要が生じることがあります。

デバッグを停止するには、**`no debug all`** または **`undebug all`** コマンドを使用します。**`show debug`** コマンドを使用して、デバッグがオフになっていることを確認してください。

Cisco CallManager トラブルシューティング ツール

さまざまな Cisco CallManager システムを監視および分析するために Cisco CallManager Serviceability が提供する、次のようなタイプのツールの詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』および『*Cisco CallManager Serviceability システム ガイド*』を参照してください。

表 2-1　Serviceability ツール

用語	定義
Real-Time Monitoring Tool	この用語は、Cisco CallManager デバイスおよびパフォーマンス カウンタに関するリアルタイム情報を提供する、Serviceability 内のプログラムを示します。
アラーム	管理者は、アラームを使用して、Cisco CallManager システムの実行時のステータスや状態を確認します。アラームには、説明や推奨される処置など、システムの問題に関する情報が含まれています。
アラーム カタログ	この用語は、Cisco CallManager サービスのすべてのアラーム定義を含むファイルを示します。Serviceability は、アラーム タイプに固有の複数のアラーム カタログをサポートしています。
アラーム定義	管理者は、アラーム定義データベースを検索して、アラーム情報を見つけます。アラーム定義には、アラームの説明および推奨される処置が含まれています。
アラーム イベント レベル	管理者は、アラームに含まれる情報のレベルを決定します。レベルの範囲は、システムに関する一般的な情報から、デバッグだけを目的とした情報にまで及びます。
アラーム フィルタ	管理者は、アラームに含まれる情報のレベル、およびアラーム 情報が保存される場所を決定します。
アラーム モニタ	Cisco CallManager Serviceability では、モニタと呼ばれるさまざまな宛先（Windows 2000 イベント ビューア、CCM トレース、SDL トレース、SNMP トラップ、および SysLog）にアラームを送信できます。

表 2-1　Serviceability ツール（続き）

用語	定義
アラート通知	管理者は、Real-Time Monitoring Tool を使用して、パフォーマンス カウンタおよびゲートウェイ ポート（チャネル）のアラート通知を設定します。リアルタイム モニタリングでは、電子メールまたはシステム通知（ポップアップ）ウィンドウで管理者にアラートが送信されます。
カテゴリ タブ	管理者は、トラブルシューティングの目的で、リアルタイム モニタリングに特定のモニタリング ウィンドウを設定します。管理者は、カテゴリ タブを使用して、その特定のウィンドウを作成します。
チャート ビュー	Performance Monitoring ウィンドウでは、デフォルトで、チャート ビューにパフォーマンス カウンタが表示されます。チャート ビューでは、カウンタ情報がグラフィカルに表示されます。
Cisco CallManager サービス	Cisco CallManager は、TFTP、CTI、Music On Hold（MOH; 保留音楽）など、特定の機能を実行するソフトウェアの形で、多くのサービスをサポートしています。
Control Center	Serviceability の Control Center ツールを使用すると、管理者は、Cisco CallManager サービスのステータスを表示したり、Cisco Callmanager サービスを開始および停止できます。
デバッグ トレース レベル	管理者は、トレースに含まれる情報のレベルを決定します。レベルの範囲は、一般的なエラーから、デバッグだけを目的とした詳細なエラーにまで及びます。
デバイス モニタリング	リアルタイム モニタリングでは、電話機やゲートウェイなど、Cisco CallManager デバイスに関するリアルタイム情報が表示されます。
Device Monitoring ウィンドウ	Real-Time Monitoring Tool がデバイスのパフォーマンスを監視しているときに、Real-Time Monitoring Tool ウィンドウの右側にデバイスのパフォーマンス情報が表示されます。
デバイス名に基づくトレース モニタリング	管理者は、Cisco CallManager および Cisco CTIManager サービスのトレース パラメータを設定することにより、選択したデバイスに関するトレース情報を取得します。

表 2-1　Serviceability ツール（続き）

用語	定義
Monitoring Objects ウィンドウ	Real-Time Monitoring Tool ウィンドウの左側には、クラスタに対応する、Cisco CallManager 関連のオブジェクトおよびカウンタまたはデバイスが表示されます。表示される情報は、ウィンドウでアクティブになっているタブによって異なります。
オブジェクトとカウンタ	Windows 2000 は、さまざまなオブジェクトおよびカウンタに関する情報を含むパフォーマンス データを提供します。オブジェクトとは、Cisco IP Phone や Cisco CallManager System Performance など、特定のデバイスまたは機能に関する同様のカウンタを論理グループにまとめたものです。カウンタは、システム パフォーマンスのさまざまな側面を測定します。カウンタは、登録されている電話機の数、試行されたコール、進行中のコールなど、統計情報を測定します。Real-Time Monitoring Tool は、これらのカウンタによって生成されるリアルタイムの統計情報を監視します。
パフォーマンス モニタリング	Real-Time Monitoring Tool には、パフォーマンス カウンタに関するリアルタイム情報が表示されます。パフォーマンス カウンタは、システム固有のものも Cisco CallManager 固有のものもあります。
Performance Monitoring ウィンドウ	Real-Time Monitoring Tool がカウンタを監視しているときに、Real-Time Monitoring Tool ウィンドウの右側にカウンタの統計情報が表示されます。
CCM トレース ログ ファイル（以前は SDI トレース）	すべての Cisco CallManager サービスには、デフォルトのトレース ログ ファイルが含まれています。システムは、サービスからの system diagnostic interface（SDI）情報をトレースし、実行時のイベントおよびトレースをログ ファイルに記録します。
SDL トレース ログ ファイル	このファイルには、Cisco CallManager や Cisco CTIManager などのサービスからのコール処理情報が含まれています。システムは、コールの signal distribution layer（SDL）をトレースし、状態遷移をログ ファイルに記録します。 （注）　ほとんどの場合は、Cisco Technical Assistance Center（TAC）から要求された場合にだけ、SDL トレースを収集します。

表 2-1　Serviceability ツール（続き）

用語	定義
サービス ステータス アイコン	Control Center には、サーバ上のサービスのステータスを示す 3 つのアイコンが表示されます。 • 四角は、停止しているサービスを示します。 • 矢印は、実行中のサービスを示します。 • 疑問符は、状態が不明なサービスを示します。
トレース	管理者およびシスコのエンジニアは、トレース ファイルを使用して、Cisco CallManager サービスの問題に関する特定の情報を取得します。
トレース分析	このプログラムは、結果をフィルタリングできる形式でトレース情報を提供します。
トレース ログ ファイル	Cisco CallManager Serviceability は、設定されているトレース情報をこのファイルに送信します。CCM と SDL という 2 つのタイプのトレース ログ ファイルがあります。
ウィンドウ ステータス バー	Real-Time Monitoring Tool ウィンドウの右下隅には、ウィンドウ ステータス バーが表示されます。このステータス バーには、Preferences、Cluster Information、Resource Usage、About、および Help という 5 つのアイコンが表示されます。
Quality Report Tool	この用語は、Cisco CallManager Serviceability に含まれる、音声品質および一般的な問題を報告するユーティリティを示します。

Cisco Secure Telnet

Cisco Secure Telnet を使用すると、Cisco Service Engineer（CSE; シスコ サービス エンジニア）は、ファイアウォールを介してお客様のサイトの Cisco CallManager ノードに透過的にアクセスできます。Cisco Secure Telnet は、強力な暗号化を使用して、シスコシステムズ内の特別な Telnet クライアントを、お客様のファイアウォールの内側にある Telnet デーモンに接続できます。このセキュアな接続により、ファイアウォールを変更せずに、お客様の Cisco CallManager ノードの監視およびトラブルシューティングをリモートで行うことができます。

（注）　シスコでは、お客様の承諾を得た場合にだけこのサービスを提供します。作業を開始する場合は、お客様のサイトでネットワーク管理者のご協力をお願いしています。

コマンドライン ツール

コマンドライン ツールは、トラブルシューティングに役立ちます。使用できるコマンドライン ツールは次のとおりです。

- **show**：Cisco CallManager データベースの内容、.ini 設定ファイル、メモリ統計情報、および Windows 診断情報を表示します。DOS シェルまたは Telnet セッションから Cisco CallManager に対して実行します。
- **nslookup** *hostname*：ホスト名から IP アドレスへの解決を確認します。
- **netstat** - **a | more**：正しいポート番号でのソケット受信を確認します。
- **ping** *hostname*：IP を介してマシンに到達できることを確認します。
- **net start**：サービスが実行されているかどうかを確認します。

Show コマンド

システム メモリ統計情報および Windows 診断情報の内容を表示するには、Show コマンドライン ツールを使用します。Show コマンドは、DOS シェルから実行でき、Telnet サーバ ソフトウェアが使用可能である場合は Telnet セッションから実行することもできます。出力データは、コンソールに表示することも、テキスト ファイルとして保存することもできます。

（注）　show コマンドは、出力に \Temp ディレクトリ内の一時ファイルを使用するため、ディスク スペースにこのファイルを格納するための十分な余裕があることを確認してください。必要な量は、ユーザ数や使用されているデバイス数、システムによって使用されているデータベースのサイズなど、さまざまな要因によって変わります。

また、Telnet サーバ ソフトウェアが使用可能である場合は、Telnet セッションから **show.exe** を実行することもできます。

show コマンドの構文は、次のとおりです。

show [**-f** <*filename*>] [**-c** <*column width*>] [**-w** <*console width*>] [**-v**] [*command*]

表 2-2 に、**show** コマンドがサポートするオプションを示します。

表 2-2　Show コマンドのオプション

コマンド	説明
-f <*filename*>	レポートを出力するファイル名
-c <*col width*>	データベース レポートの各カラムの幅（デフォルトは 15）
-w <*con width*>	データベース レポート領域の幅（デフォルトは 80）
-v	冗長モード

show コマンドでは、次のパラメータを使用します。

- **?**：ヘルプ メッセージを表示します。
- **db**：設定データベースを表示します。
- **db tables**：データベース テーブル名を表示します。
- **db t** <*tablename*>：データベース テーブルの内容を表示します。
- inst [apps | elem | all]：インストールされているアプリケーションと要素に関する情報を表示します。
- **isdn [cluster | local | specific]**：ゲートウェイの D チャネルのステータスを表示します。
- **ps**：ローカル システム上で実行されているすべてのプロセスを表示します。
- **win**：Windows の診断を報告します。**win** パラメータを指定すると、システム統計情報、ストレージ情報、ソフトウェア環境、要約統計情報などが表示されます。

（注）　**Show win** は、Windows システム情報の取得に大量の CPU リソースを消費し、表示に長時間かかります。このコマンドは、Cisco CallManager がビジー状態でない場合にだけ実行してください。

- **tech** | (**none**)：データベースおよび Windows システムの情報を報告します。

（注）　**Show tech** は、パラメータを指定しない show コマンドと同じ複数レポート出力を提供します。

例：

```
show -f output.txt -v -w480 db
show tech
show db t ProcessNode
```

show コマンドの詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。

Cisco CallManager システム パフォーマンス モニタリング

ローカルまたはリモートにある任意の Cisco CallManager インストレーションのシステムおよびデバイスの統計情報を収集して表示するには、Windows 2000 Performance を使用します。この管理ツールを使用すると、各コンポーネントの動作を学習しなくても、システムを十分に理解できます。このツールは、一般的な情報と特定の情報の両方をリアルタイムで報告します。

Cisco CallManager のパラメータを追加した後、システムによって生成された統計情報を Cisco CallManager で表示する条件を定義できます。

Performance の詳細については、Microsoft Windows 2000 のマニュアルを参照してください。

Path Analysis の動作

Path Analysis は診断アプリケーションで、ネットワーク上の指定された 2 ポイント間の接続性をトレースします。Path Analysis は、これらのポイント間を流れるパケットが通る物理パスと論理パス（レイヤ 2 とレイヤ 3）の両方を分析します。

コールの完了後、PathTool は、発信側と着信側の電話番号を指定して、音声パケットのルートをトレースします。このトレースは、Cisco IP Phone、ステーション ゲートウェイに接続されているアナログ デバイス、トランク ゲートウェイ（アナログまたはデジタル）のうち、任意のエンドポイント間のコールに適用されます。

詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。

システム ログ管理プロセス

システム ログ管理プロセスは他のネットワーク管理システムに適合させることもできますが、シスコ デバイスからの Syslog メッセージの管理には、CiscoWorks2000 Resource Manager Essentials に付属の Cisco Syslog Analysis が最適です。

Cisco Syslog Analyzer は、Cisco Syslog Analysis のコンポーネントとして機能し、複数のアプリケーションのシステム ログの共通ストレージおよび分析を提供します。もう 1 つの主要コンポーネントである Syslog Analyzer Collector は、Cisco CallManager サーバからログ メッセージを収集します。

これら 2 つのシスコ アプリケーションは連動し、Cisco IP テレフォニー ソリューション用の集中システム ロギング サービスを提供します。

詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。

簡易ネットワーク管理プロトコルのサポート

network management system（NMS; ネットワーク管理システム）は、業界標準のインターフェイスである SNMP を使用して、ネットワーク デバイス間で管理情報を交換します。TCP/IP プロトコル スイートの一部である SNMP を使用すると、管理者はリモートでネットワーク パフォーマンスを管理し、ネットワークの問題を検出して解決し、ネットワークの拡張を計画できます。

SNMP で管理されるネットワークは、管理対象デバイス、エージェント、およびネットワーク管理システムという 3 つの主要コンポーネントで構成されます。

- 管理対象デバイスとは、SNMP エージェントを含み、管理対象ネットワークに常駐するネットワーク ノードです。管理対象デバイスは、管理情報を収集して格納し、SNMP を使用してその情報を使用できるようにします。
- エージェントは、ネットワーク管理ソフトウェアとして、管理対象デバイスに常駐します。エージェントは、管理情報をローカルで認識し、その情報を SNMP と互換性のある形式に変換します。
- ネットワーク管理システムは、SNMP 管理アプリケーションと、そのアプリケーションを実行するコンピュータで構成されます。NMS は、管理対象デバイスを監視および制御するアプリケーションを実行します。NMS は、ネットワーク管理に必要な処理リソースおよびメモリ リソースの大部分を提供します。次の NMS は Cisco CallManager と互換性があります。
  - CiscoWorks2000
  - HP OpenView
  - SNMP および Cisco CallManager SNMP インターフェイスをサポートするサードパーティ製アプリケーション

詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』および『*Cisco CallManager Serviceability システム ガイド*』を参照してください。

CiscoWorks2000

CiscoWorks2000 は、Cisco CallManager を含め、すべてのシスコ デバイスに最適なネットワーク管理システムとして機能します。CiscoWorks2000 は Cisco CallManager にバンドルされていないため、別途購入する必要があります。次のツールを CiscoWorks2000 と併用すると、リモート サービサビリティが得られます。

- システム ログ
- Path Analysis
- シスコ検出プロトコル（CDP）
- 簡易ネットワーク管理プロトコル

CiscoWorks2000 の詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』、および次の URL にある CiscoWorks2000 のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/index.htm

シスコ検出プロトコル（CDP）のサポート

シスコ検出プロトコル（CDP）のサポートにより、CiscoWorks2000 で、Cisco CallManager サーバを検出および管理できます。

CiscoWorks2000 の詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』、および次の URL にある CiscoWorks2000 のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/index.htm

SQL クエリー アナライザ

SQL クエリー アナライザは、ロケーションに関連付けられているデバイス（エンドポイント、IP Phone、ゲートウェイなど）を検出します。SQL クエリーを使用するには、次の手順を実行します。

（注）　Cisco CallManager Configuration ウィンドウの Location フィールドに **None** という値が表示される場合は、デバイスが特定のロケーションに割り当てられていません。ロケーションに割り当てられていないデバイスは、SQL クエリーによって返されません。

手順

ステップ 1　Cisco CallManager サーバの Windows 2000 サーバ コンソールで **Start > Programs > Microsoft SQL Server > Query Analyzer** を選択し、SQL Server クエリー アナライザ アプリケーションを実行します。

Connect to SQL Server ウィンドウが表示されます（SQL Query Analyzer ウィンドウは、バックグラウンドで淡色表示されます）。

ステップ 2　SQL Server フィールドに、ピリオドを入力します。

ステップ 3　**Start SQL Server if it is Stopped** オプションをオフにします。

ステップ 4　**Windows Authentication** ボタンをクリックします。

ステップ 5　**OK** をクリックします。

ステップ 6　Query (local) ウィンドウが表示されます（SQL Query Analyzer ウィンドウは、バックグラウンドで淡色表示されます）。

ステップ 7　DB フィールドで、ドロップダウン矢印をクリックし、最も大きい番号の Cisco CallManager データベースを選択します。

Cisco CallManager データベースには、**CCM03xx**（**xx** はデータベースの番号）という形式のラベルが付いています。

ステップ 8　Query (local) ウィンドウ本体に、次の SQL クエリーを入力します。

```
SELECT Device.name, Device.description
FROM Device, Location
WHERE Device.fkLocation=Location.pkid
AND Location.name="enter location name between these quotes"
```

ステップ 9　メインの Query Analyzer ウィンドウから **Query > Execute** を選択し、クエリーを実行します。

ツールバーで緑の矢印をクリックするか、**F5** キーを押して、クエリーを実行することもできます。

ステップ 10　結果が出たら、SQL Server Query Analyzer ウィンドウを閉じます。

トラブルシューティングのヒント

次のヒントは、Cisco CallManager のトラブルシューティングに役立ちます。

ヒント　Cisco CallManager のリリース ノートで既知の問題を確認します。

リリース ノートには、既知の問題の説明と対応策が記載されています。

ヒント　デバイスの登録先を確認します。

各 Cisco CallManager ログはファイルをローカルでトレースします。電話機またはゲートウェイが特定の Cisco CallManager に登録されている場合、コールがそこで開始されると、コール処理がその Cisco CallManager で実行されます。問題をデバッグするには、その Cisco CallManager 上のトレースを取り込む必要があります。

デバイスがサブスクライバ サーバに登録されているにも関わらず、パブリッシャ サーバ上のトレースを取り込むという間違いがよくあります。そのトレース ファイルはほとんど空です（そのファイルには目的のコールがまったく含まれていません）。

デバイス 1 を CM1 に登録し、デバイス 2 を CM2 に登録しているために問題が生じることも多くあります。デバイス 1 がデバイス 2 をコールすると CM1 でコール トレースが実行され、デバイス 2 がデバイス 1 をコールすると CM2 でトレースが実行されます。双方向のコール問題のトラブルシューティングを行う場合は、トラブルシューティングに必要なすべての情報を得るために、両方の Cisco CallManager からの両方のトレースが必要となります。

ヒント　問題のおおよその時刻を認識します。

複数のコールが発信された可能性があるため、コールのおおよその時刻を認識していると、TAC が問題を迅速に特定するのに役立ちます。

アクティブなコール中に **i** ボタンを 2 回押すと、Cisco IP Phone 79xx 上で電話統計情報を取得できます。

テストを実行して問題を再現し、情報を生成する場合は、問題を理解するために不可欠な次のデータを確認してください。

- 発信側の番号または着信側の番号
- 特定のシナリオに関係する他の番号
- コールの時刻

（注）　トラブルシューティングには、すべての機器の時刻が同期化されていることが重要であることに注意してください。

問題を再現している場合は、ファイルの変更日付とタイムスタンプを調べて、その時間枠のファイルを選択します。適切なトレースを収集する最良の方法は、問題を再現してからすぐに最新のファイルを見つけ、そのファイルを Cisco CallManager サーバからコピーすることです。

ヒント　ログ ファイルを保存して、上書きされないようにします。

ファイルは、時間が経つと上書きされます。ログが記録されているファイルを調べる唯一の方法は、メニューバーで **View > Refresh** を選択し、ファイルの日付と時刻を確認することです。

ヒント　Cisco CallManager サービスが実行されていることを確認します。

サーバ上で Cisco CallManager サービスがアクティブであることを確認するには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration から、**Application > Cisco CallManager Serviceability** を選択します。

Cisco CallManager Serviceability ウィンドウが表示されます。

ステップ 2　図 2-1 のように、**Tools > Service Activation** を選択します。

図 2-1　　Cisco CallManager Serviceability ウィンドウの Tools メニュー

ステップ 3　Servers カラムから、サーバを選択します。

選択したサーバが Current Server というタイトルの隣に表示され、設定済みのサービスを示すボックスが表示されます。

図 2-2 のように、Cisco CallManager 行の Activated Status カラムに Activated または Deactivated と表示されます。

図 2-2　Service Activation ウィンドウ

Activated というステータスが表示されている場合、選択したサーバ上で Cisco CallManager がアクティブです。

Deactivated というステータスが表示されている場合は、引き続き次のステップを実行します。

ステップ **4**　Cisco CallManager のチェックボックスをオンにします。

ステップ **5**　**Update** ボタンをクリックします。

Cisco CallManager 行の Activation Status カラムに **Activated** と表示されます。

これで、選択したサーバの Cisco CallManager がアクティブになりました。

Cisco CallManager が使用されているかどうか、および現在アクティブであるかどうかを確認するには、次の手順を実行します。

手順

ステップ 1　Cisco CallManager Administration から、**Application > Cisco CallManager Serviceability** を選択します。

Cisco CallManager Serviceability ウィンドウが表示されます。

ステップ 2　**Tools > Control Center** を選択します。

ステップ 3　Servers カラムから、サーバを選択します。

選択したサーバが Current Server というタイトルの隣に表示され、設定済みのサービスを示すボックスが表示されます。

CallManager 行の Activation Status カラムに **Activated** と表示されます。

選択したサーバの Cisco CallManager はアクティブです。

ヒント　Internet Information Server を開始および停止します。

Internet Information Server（IIS）を開始または停止するには、次の任意の手順を実行します。

手順

ステップ 1　Start メニューから、**Start > Programs > Administration Tools > Services** を選択します。

サービスを一覧表示したウィンドウが表示されます。

サービスを停止するには

ステップ 2　**IIS Admin Service** を選択します。

ステップ 3　停止ボタン（ウィンドウの上部にある四角い黒のボックス）をクリックします。

ステップ 4　**Yes** をクリックします。

サービスを開始するには

ステップ 5　**Start** ボタンをクリックします。

ステップ 6　**World Wide Web Publishing** を選択します。

ステップ 7　開始ボタン（ウィンドウの上部にある、右矢印を含む四角い黒のボックス）をクリックします。

IIS が開始されます。

手順

ステップ 1　Start メニューから、**Start > Programs > Administration Tools > Services** を選択します。

サービスを一覧表示したウィンドウが表示されます。

サービスを停止するには

ステップ 2　**IIS Admin Service** を右クリックします。

ステップ 3　**Stop** を選択します。

IIS が停止します。

サービスを開始するには

ステップ 4　**Start** ボタンをクリックします。

ステップ 5　**World Wide Web Publishing** を右クリックします。

ステップ 6　**Start** を選択します。

IIS が開始されます。

手順

ステップ 1　Start メニューから、**Start > Programs > Administration Tools > Services** を選択します。

IIS Administration Service を含むウィンドウが表示されます。

ステップ 2　**IIS Admin Service** を右クリックし、**Stop** を選択します。

IIS が停止します。

ステップ 3　IIS サーバを起動するには、**IIS Admin Service** を右クリックし、**Start** を選択します。

IIS が開始されます。

その他の情報

参考資料

- *Cisco CallManager Serviceability アドミニストレーション ガイド*
- *CiscoCallManager Serviceability システム ガイド*
- *Cisco CallManager アドミニストレーション ガイド*
- *Cisco CallManager インストレーション ガイド*
- 次の URL にある CiscoWorks2000 のユーザ マニュアル

http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cw2000/index.htm

CHAPTER 3

インストール、バックアップ、および復元の問題

この章では、Cisco CallManager のインストール、バックアップ、または復元に関連する、次のような一般的な問題の解決方法について説明します。

- 迅速なアップグレード、バックアップ、および復元のためのヒント
- インストールの問題
- アップグレードの問題
- バックアップと復元の問題

次の手順で問題が解決されない場合は、TAC に連絡して詳細な調査を依頼してください。

『*Cisco IP Telephony Operating System, SQL Server, Security Updates*』に関する最新情報については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/osbios.htm

『*Cisco CallManager Compatibility Matrix*』については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/ccmcomp.htm

警告　**何らかの理由で Cisco CallManager サーバの IP アドレスを変更する必要がある場合は、そのアドレスを参照するすべてのアプリケーションで IP アドレスを変更する必要があります。IP アドレスが変更されていないインスタンスがある場合、Cisco IP Phone が Cisco CallManager に登録されないことがあります。**

迅速なアップグレード、バックアップ、および復元のためのヒント

システムに対してアップグレード、バックアップ、および復元を行う場合は、問題を避けるために、次のヒントを参考にしてください。

- 2 つの異なるバージョンの Cisco CallManager がある場合の復元場所
- データ高速転送用の BAT
- アップグレード、バックアップ、および復元
- パブリッシャのバックアップ
- サードパーティ製バックアップ ユーティリティ

2 つの異なるバージョンの Cisco CallManager がある場合の復元場所

ヒント　同じバージョンの Cisco CallManager 上でシステムを復元します。異なるバージョンから復元しようとすると、リリース間の変更点が原因で問題が生じます。

データ高速転送用の BAT

ヒント　クリーン システムを構築してから、Bulk Administration Tool（BAT）を使用して、電話機およびユーザをインポートします。

アップグレード、バックアップ、および復元

ヒント　アップグレードを実行し、Cisco IP telephony Applications Backup Utility を実行して、新しいシステムを最初から構築し直し、バックアップ テープを復元します。

パブリッシャのバックアップ

ヒント　Cisco CallManager クラスタ内のパブリッシャ サーバだけをバックアップします。他のすべてのサーバ（サブスクライバ）は、インストール時に情報をコピーします。

サードパーティ製バックアップ ユーティリティ

Unity のバックアップでは、サードパーティ製アプリケーションが必要です。

（注）　シスコは、Cisco CallManager データベースをバックアップするためのサードパーティ製ユーティリティをサポートしていません。サードパーティ製ユーティリティを使用して Cisco CallManager データベースをバックアップすると、TAC サポートが無効になります。

ヒント　付属の Cisco IP telephony Applications Backup Utility を使用して、Cisco CallManager データベースを別のマシンにバックアップします。その後、そのマシンを使用して、サードパーティ製バックアップ ソフトウェアを実行します。

インストールの問題

インストール、およびインストールのトラブルシューティングに関する詳細なマニュアルについては、次の URL で『*Cisco CallManager インストレーション ガイド*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/

続いて、**Installation Instructions** をクリックして、使用しているシステム ソフトウェア バージョンのリリース番号のドキュメントを見つけます。

また、現在のソフトウェア バージョンのインストール問題については、『*Release Notes for Cisco CallManager*』を参照してください。

本書では、次のインストール問題について説明します。

Cisco CallManager のサーバ名を変更できない

症状

Cisco CallManager サーバの名前を変更しようとすると、サービスが失敗します。CTI Manager、Extended Functions、Voice Media Streaming など、他のサービスも失敗します。

考えられる原因

シスコは、Cisco CallManager サーバの名前の変更をサポートしていません。

推奨処置

Cisco CallManager サーバの名前ではなく、IP アドレスを変更してください。IP アドレスの変更については、第 4 章「Cisco CallManager システムの問題」を参照してください。

警告　**Cisco CallManager サーバの IP アドレスを変更する必要がある場合は、そのアドレスを参照するすべてのアプリケーションで IP アドレスを変更する必要があります。IP アドレスが変更されていないインスタンスがある場合、Cisco IP Phone が Cisco CallManager に登録されないことがあります。**

ブートの失敗からの回復

次の URL では、ブートの失敗からの詳細な回復手順を参照できます。

http://www.cisco.com/warp/public/130/recovery_index.shtml

1 つのパブリッシャと 2 つのサブスクライバ：1 つのサブスクライバへのインストール後、3 つすべてのデータベースが異なる情報を持つ

エラー メッセージ

Looking for ccmxxxx databases in (local).master.dbo.sysdatabases table

考えられる原因

サブスクライバの構築に失敗しました。

推奨処置

次の手順を実行します。

1. すべてのサーバ間で NetBIOS 名前解決が機能していることを確認します。
2. 各サーバが他のサーバのホスト名および NetBIOS 名を解決できるように、パブリッシャ サーバおよびサブスクライバ サーバ上の hosts と LMHOSTS にデータが入力されていることを確認します（必要に応じて、これらのファイルを編集します）。

   hosts は DNS 解決に使用されます。LMHOSTS は、名前解決に NetBIOS を使用します。SQL も名前解決に NetBIOS を使用します。
3. Web から、Cisco CallManager をパブリッシャ上のソフトウェア バージョンにアップグレードします。

   サブスクライバに SQL データベースがダウンロードされます。

アップグレードの問題

この項では、Cisco CallManager のアップグレードに関する次の問題について説明します。

サブスクライバのアップグレードの失敗：更新されたデータベースが見つからない

症状

Cisco CallManager 3.x において、パブリッシャと複数のサブスクライバをアップグレードしているときに、エラー メッセージが表示されない場合があります。エラー メッセージが表示されなかったにも関わらず、クラスタ内のサーバをリブートしても、電話機もデバイスも正しいサブスクライバに登録されません。

多くの場合、クラスタ内の Cisco CallManager ノード間のフェールオーバーも失敗します。さらに、Application Event Viewer を確認すると、Cisco CallManager サービスの多くのインスタンスが何度も停止したり開始したりしていることがわかります。

考えられる原因

SQL Enterprise Manager にアクセスし、パブリッシャ データベースとサブスクライバ データベースの両方を開きます。パブリッシャおよび各サブスクライバで、最新の Cisco CallManager データベース バージョン（CCM030X）を確認します。SQL Enterprise Manager でパブリッシャ データベースとサブスクライバ データベースを表示しているときに、サブスクライバのデータベースが最新でないことに気づいた場合は、ネットワーク内で名前解決の問題が発生している可能性があります。

この問題を確認するもう 1 つの方法は、**C:\Program Files\Common Files\Cisco\Logs** にある最新のデータベース アップグレード ログを参照することです。下方向にスクロールし、次の出力を探します。

4-28-2002 10:54:00 _DBPullSubscription: CALLMAN01 CCM0302 sa ******** CALLMAN02

CCM0302 sa ******** C:\Program Files\Cisco\Bin\ 0

4-28-2002 11:11:32 Pulling subscription from CALLMAN01 to subscribe to the CCM0302 Database.

Return Code = 8 DB_SCRIPT_ERROR

この出力は、サブスクライバがパブリッシャと通信して正しいデータベース バージョンを確認できたが、そのデータベース バージョンをコピーまたは複製することを妨げる問題が発生したことを示します。

推奨処置

Microsoft SQL Server は、いくつかのタイプの remote-procedure call（RPC; リモート プロシージャ コール）タスクに NetBIOS 名前解決を使用します。そのため、パブリッシャとすべてのサブスクライバは、NetBIOS 名前解決に LMHOSTS ファイルを使用する必要があります。クラスタ内のすべてのサーバは、サーバ間の正しい名前解決のために HOSTS ファイルを使用する必要もあります。

Windows 2000 では、**C:\winnt\system32\drivers\etc** ディレクトリにサンプルの HOSTS ファイルと LMHOSTS ファイル（HOSTS.SAM と LMHOSTS.SAM）が用意されています。次の手順を実行し、カスタム インストール用にサンプル ファイルを変更します。

1. Notepad などのテキスト エディタを使用して、Cisco CallManager パブリッシャからファイル **C:\winnt\system32\drivers\etc\hosts.sam** を開きます。
2. **#** 記号で始まるコメント行を読みます。次に、ファイルからすべての行を削除します。Windows は、名前解決を試行するたびにファイル内のすべての行を解析する必要があります。
3. パブリッシャの IP アドレス、スペース、パブリッシャのホスト名の順に入力します。ホスト名は、**ipconfig /all** コマンドを使用して検出できます。

   この操作を繰り返し、クラスタ内のサーバごとに 1 行ずつファイルに入力していきます。次に、hosts ファイルの例を示します。

```
127.0.0.1           localhost
172.18.110.90       ICSCM1
172.18.110.94       ICSCM2
```

4. 拡張子を付けずに **C:\winnt\system32\drivers\etc\hosts** としてファイルを保存します。

（注） Notepad では、デフォルトで、.txt 拡張子が付加されます。したがって、Windows エクスプローラまたはコマンド プロンプトを使用して、.txt 拡張子を削除してください。

（注） Windows エクスプローラでは、デフォルトで、ファイル拡張子が表示されません。したがって、ファイル拡張子を表示するか、**rename** コマンドを使用してください。

5. Notepad などのテキスト エディタを使用して、ファイル **C:\winnt\system32\drivers\etc\lmhosts.sam** を開きます。
6. すべてのコメント行を読んで削除します。サーバごとに 1 行を追加しますが、サーバ名の後に **#PRE** というテキストを付けます。次に、lmhosts ファイルの例を示します。

```
172.18.110.90      ICSCM1      #PRE
172.18.110.94      ICSCM2      #PRE
```

7. 拡張子を付けずに **C:\winnt\system32\drivers\etc\lmhosts** としてファイルを保存します。

（注） Notepad では、デフォルトで、.txt 拡張子が付加されます。したがって、Windows エクスプローラまたはコマンド プロンプトを使用して、.txt 拡張子を削除してください。

（注） Windows エクスプローラでは、デフォルトで、ファイル拡張子が表示されません。したがって、ファイル拡張子を表示するか、**rename** コマンドを使用してください。

8. コマンド プロンプトを開き、**nbtstat -R** コマンドを入力して、LMHOSTS ファイルの内容を NetBIOS 名キャッシュにロードします。**nbtstat Dc** コマンドを使用して、LMHOSTS ファイルが正常に解析およびロードされたことを確認します。情報が表示されない場合は、Microsoft Knowledge Base 記事 Q180099 を参照してください。

（注）　NetBIOS リモート キャッシュには、リモート ノード用のネーム対アドレスの解決しか含まれていません。

9. **Start > Run** を選択し、**services.msc** と入力します。
10. **OK** をクリックします。
11. **DNS Client Service** をクリックし、サービス名を右クリックして、**Restart** をクリックします。
12. クラスタ内の Cisco CallManager サーバごとにステップ 1 ～ 11 を繰り返します。
13. サブスクライバで Cisco CallManager のアップグレードを再度実行します。

この手順が完了すると、サブスクライバは最新の Cisco CallManager データベースを持つようになり、パブリッシャから正常にサブスクリプションをプルします。

アップグレード後のブランクの Enterprise Parameters ページ

症状

Enterprise Parameters ページにフィールドも変数情報も表示されません。他のすべてのページは正常に表示されます。

考えられる原因

CSCdv65210「Issues occur where an upgrade was not moving all the information to the database.」を参照してください。

推奨処置

次のファイルを実行してページを再初期化します。

C:\Program Files\Cisco\bin\Xmltemp\installxml.vbs

Enterprise Parameters ページが正しく表示されることを確認します。

関連情報

Cisco CallManager をアップグレードする方法の詳細については、次の URL で『*Upgrading Cisco CallManager*』を参照し、使用しているリリース番号を見つけます。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/

特定のソフトウェア リリースのドキュメントを見つけるには、**Installation Instructions** をクリックします。

次の URL では、TAC サイトにある情報が提供されています。

http://www.cisco.com/warp/public/130/upgrade_index.shtml

バックアップと復元の問題

この項では、バックアップに関する次の問題について説明します。

- ローカル テープ ドライブへのバックアップが機能せず、エラー コード 1165 で終了する
- Cisco CallManager のインストール時に、バックアップ先のプロンプトが表示されない
- Cisco CallManager の Sti Backup Utility が「Cancelling Backup」で止まって進まない
- 復元後、データベースが破損している

Cisco IP telephony Applications Backup Utility は、次のアイテムを自動的にバックアップします。

- SQL Server 2000 上の Cisco CallManager データベース（Call Detail Records（CDR）データベースを含む）
- Administrative Reporting Tool（ART）データベース
- DC Directory、LDAP ディレクトリ
- パブリッシャとサブスクライバの設定情報を含む Distribution .ini
- Database.dat（ある場合）
- HKLM\Software\Cisco Systems, Inc.
- Cisco Customer Response Solutions (CRS)

Cisco CallManager をバックアップする方法の詳細については、次の URL で『*Backing Up and Restoring Cisco CallManager*』を参照し、使用しているリリース番号を見つけます。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/

特定のソフトウェア リリースのドキュメントを見つけるには、**Installation Instructions** をクリックします。

ローカル テープ ドライブへのバックアップが機能せず、エラー コード 1165 で終了する

エラー メッセージ `1165 The device has indicated that cleaning is required before further operations are attempted. ERROR_DEVICE_REQUIRED_CLEANING`

考えられる原因

テープ ドライブまたはテープに問題があります。

推奨処置

ハードウェアのマニュアルでテープ ドライブのクリーニングに関する詳細を参照するか、別のきれいなテープを使用してみます。

エラーが発生することなく、バックアップ プロセスが正常に完了することを確認します。

Cisco CallManager のインストール時に、バックアップ先のプロンプトが表示されない

症状

バックアップ フォルダまたは Cisco IP telephony Applications Backup Utility が見つかりません。

考えられる原因

Cisco CallManager を初めてインストールしている場合は、バックアップ画面で **Cancel** をクリックした可能性があります。その場合は、バックアップ先が作成されていません。

推奨処置

バックアップ ユーティリティを正しいフォルダにインストールする方法は、次の 2 つです。

- Cisco IP telephony Applications Backup Utility がインストールされている他の任意のブレードから「backup」フォルダをコピーして、**_stBackSetup.exe** ファイルを実行します。
- Cisco CallManager CD のルート ディレクトリの「Backup」フォルダから **setup.exe** を実行します。

Cisco CallManager の Sti Backup Utility が「Cancelling Backup」で止まって進まない

症状

Sti BackupUtility の実行中に、次のメッセージが表示されます。

```
"Cancelling backup process. Please wait.."
```

バックアップが実行されなかったことを（ステータス モニタを介して）確認した後、バックアップ プロセスをキャンセルしようとしても、このメッセージが消えません。

（注）　サーバをリブートしても、問題が解決されません。

推奨処置

次の手順を実行します。

1. Registry Editor ウィンドウの Config レジストリ キーの値に注意します。
2. Windows の Start ボタンから、**Run** を選択し、**regedit** と入力します。
3. Registry Editor から、**HKEY_LOCAL_MACHINE > SOFTWARE > Cisco Systems > Backup > Config** を選択します。
4. Config レジストリ キーの値を手動で **0** に変更します。
5. Cisco CallManager の StiView.exe プロセスを手動で停止するために、**Ctrl+Alt+Del** キーを押して **Task Manager** を選択します。

   Windows Task Manager が表示されます。
6. Processes タブをクリックし、**stiView.exe** を選択して、**End Process** ボタンをクリックします。

代わりの解決方法として、システム ディレクトリから、**C: > WINNT > SYSTEM32** を選択し、**StiBack.exe** ファイルを実行することもできます。

復元後、データベースが破損している

症状

パブリッシャ サーバおよびサブスクライバ サーバ上でバックアップと復元が正常に完了したようですが、1 つのデータベースで情報が欠落しています。各データベースが、異なるバージョンのソフトウェアを示します。

考えられる原因

あるバージョンでバックアップが作成され、それより新しいバージョンのソフトウェアで復元されました。

推奨処置

同じバージョンの Cisco CallManager 上でシステムを復元する必要があります。異なるバージョンから復元しようとすると、リリース間の変更点が原因で問題が生じます。

次の手順を実行し、データベースを復元します。

（注）　この手順は、必ずパブリッシャ サーバから実行してください。Cisco NT サービスと IIS Admin サービスが停止していることを確認してください。

SQL データベースのバックアップ

手順

ステップ **1**　Cisco CallManager バージョン 4.0 で **Start-Programs > Microsoft SQL Server 2000** を選択します。

ステップ **2**　**Enterprise Manager** をクリックします。

ステップ **3**　**Microsoft SQL Servers** をダブルクリックします。

ステップ **4**　**SQL Server Group** をダブルクリックします。

ステップ 5　マシン名（マシンの DNS 名）をダブルクリックします。

ステップ 6　**Databases** をダブルクリックします。

ステップ 7　**CCM** で始まる最上位レベルのデータベースをクリックします。

ステップ 8　**Tools > Backup Database** を選択します。

ステップ 9　**Database N complete** および **Overwrite existing media** を選択します。

ステップ 10　**Add** をクリックします。

ステップ 11　デフォルト パスにファイル名を入力します。

ステップ 12　**OK** をクリックします。

情報を表示するための SQL データベースの復元

手順

ステップ 1　データベースをバックアップしたことを確認します（「SQL データベースのバックアップ」の手順を参照してください）。

現在のデータベースのアンパブリッシュ

ステップ 2　すべての Cisco NT サービスおよび IIS Admin サービスが停止していることを確認します。

ステップ 3　**Start > Programs > Microsoft SQL Server 2000** を選択します。

ステップ 4　**Enterprise Manager** をクリックします。

ステップ 5　**Microsoft SQL Servers > SQL Server Group** を選択します。

ステップ 6　*サーバ名*をクリックします。

ステップ 7　**Server Name > Replication** を右クリックします。

ステップ 8　**Configure Publishing > Subscribers > Distribution** を選択します。

ステップ 9　ポップアップ ウィンドウで **Publication Database** タブをクリックします。

ステップ 10 現在パブリッシュされているデータベース名のチェックボックスをオフにします。

ステップ 11 **OK** をクリックします。

カスタマー データベースの復元

ステップ 12 すべての Cisco NT サービスおよび IIS Admin サービスが停止していることを確認します。

ステップ 13 カスタマー バックアップ ファイルを **C:MSSQL2000\BACKUP** に置きます。

ステップ 14 **Start > Programs > Microsoft SQL Server 2000** を選択します。

ステップ 15 **Enterprise Manager** をクリックします。

ステップ 16 **Microsoft SQL Servers > SQL Server Group** を選択します。

ステップ 17 **Databases** をダブルクリックします。

ステップ 18 **CCM** で始まる、最も大きい番号のデータベースをクリックします。

ステップ 19 **Restore Database** をクリックします。

事前にデータベースをバックアップし、そのデータベースを復元する場合

ステップ 20　**first backup to restore** を選択します。

ステップ 21　**Database N complete** を選択します。

ステップ 22　**OK** をクリックします。

ステップ 23　このマシンに別のデータベースを復元する場合は、**Restore N from device** を選択します。

ステップ 24　**Select Devices** をクリックします。

ステップ 25　**Add** をクリックし、復元元のファイル名を入力します。

ステップ 26　**Database N complete** を選択します。

ステップ 27　**OK** をクリックします。

ステップ 28　次のメッセージが表示されます。

```
Restore of database CCMxxxx completed successfully.
```

これで、メイン ウィンドウでデータベースをクリックしてデータベースのテーブル、ユーザ、および他の情報を表示し、データベースの内容を調べることができます。

元のデータベースを復元する準備ができたら、**Server Name > Replication** を選択し、**Configure Publishing > Subscribers > Distribution** を右クリックして、元のデータベースのチェックボックスをオンにすることにより、そのデータベースを再度パブリッシュします。

マシン上で Cisco CallManager と連携させるためのカスタマー データベースの復元

手順

ステップ 1　データベースをアンパブリッシュしてカスタマー　データベースを復元するための前述の手順を繰り返します。

ステップ 2　3 つのデフォルト ユーザ CiscoCCMUser、CiscoCCMCDR、および CiscoCCMReader を削除するために、Enterprise Manager から **Tools > SQL Server Query Analyzer** を選択します。

Start > Programs > Microsoft SQL Server > Query Analyzer から Query Analyzer にアクセスすることもできます。

ステップ 3　画面の右上隅にあるプルダウン メニューからデータベースを選択します。

（注）　正しいデータベース名を選択することが重要です。正しいデータベース名を選択しないと、関係ないデータベースからユーザを削除する恐れがあります。

ステップ 4　**Sp_dropuser CiscoCCMUser** と入力し、**Go** をクリックします。

ステップ 5　**Play** ボタンをクリックします。

ステップ 6　次のメッセージが表示されます。

```
User CiscoCCMUser successfully removed from database.
```

ステップ 7　**Sp_dropuser CiscoCCMCDR** と入力し、**Go** をクリックします。

ステップ 8　**Play** ボタンをクリックします。

ステップ 9　次のメッセージが表示されます。

```
User CiscoCCMCDR successfully removed from database.
```

ステップ 10　**Sp_dropuser CiscoCCMReader** と入力し、**Go** をクリックします。

ステップ 11　**Play** ボタンをクリックします。

ステップ 12　次のメッセージが表示されます。

```
User Cisco CCMReader successfully removed from database.
```

マシンの 3 つのデフォルト ユーザの追加

ステップ 13　メイン画面で、データベース名の下にある **Users** を右クリックします。

ステップ 14　**CiscoCCMUser** を選択し、このユーザの「db_owner」ボックスをオンにします。

ステップ 15　**OK** をクリックします。

ステップ 16　**CiscoCCMCDR** を選択し、「db_owner」ボックスをオンにします。

ステップ 17　**OK** をクリックします。

ステップ 18　**CiscoCCMReader** を選択し、「db_datareader」ボックスをオンにします。

ステップ 19　**OK** をクリックします。

データベース テーブルの設定

ProcessConfig テーブル

ステップ 20　**Tables > ProcessConfig** を選択します。

ステップ 21　**ProcessConfig** を右クリックします。

ステップ 22　**open > return all rows** を選択します。

ステップ 23　**SQL** ボタンをクリックし、次の SQL クエリーを実行します。

```
SELECT  *
FROM ProcessConfig
where
tkservice = 9

ORDER by paramname
choose the exclamation point to run
```

ステップ 24　GlassHouseNodeID の paramValue を書き留めます。
このテーブルの GlassHouseNodeId の ParamValue は、Cisco CallManager の fkProcessNode 文字列および ProcessNode の pkid 文字列と一致します。

（注）　最初の番号のセットが最下位になります。

ステップ 25　すべての DBConnection レコードで、パブリッシャ マシン名と一致するようにサーバ名を変更します。

ステップ 26　DBConnection レコードで、現在のデータベース名と一致するようにデータベース名を変更します。

ProcessNode テーブル

ステップ 27　**Tables > ProcessNode** を選択します。

ステップ 28　**ProcessNode** を右クリックし、**open > return all rows** を選択します。

ステップ 29　マシンの *ip アドレス*または *マシン名*になるように、パブリッシャ（pkid= 以前に書き留めた glassHouseNodeID）の「name」カラムを変更します。

CallManager テーブル

ステップ 30　**Tables > CallManager** を選択します。

ステップ 31　**CallManager** を右クリックし、**open > return all rows** を選択します。

ステップ 32　ProcessNode テーブルで変更した正しいマシン名または IP アドレスになるように、CallManager レコード（fkprocessnode=glassHouseNodeID）の「processNodeName」カラムを変更します。

レジストリ設定の確認

ステップ 33　レジストリを開き、HKEY_LOCAL_MACHINE > SOFTWARE に移動します。

ステップ 34　**Cisco Systems, Inc** をクリックします。

ステップ 35　**DBL** をクリックします。

ステップ 36　DBConnection0 キーの値に注意します。
値で、SERVER の値がパブリッシャの DNS 名であり、データベース バージョン名が正しいことを確認します。

データベースのパブリッシュ

ステップ 37　Enterprise Manager で、メイン ツリーに戻ります。

ステップ 38　***サーバ名***をクリックします。

ステップ 39　**New > Publication** を選択します。

ステップ 40　**Next** をクリックします。

ステップ 41　データベース名を選択します。

ステップ 42　**Next** をクリックします。

ステップ 43　**Transactional** を選択します。

ステップ 44　**Next** をクリックします。

ステップ 45　**Next** をクリックします。

ステップ 46　**publish all tables** を選択します。

ステップ 47　**Next** をクリックします。

ステップ 48　**Next** をクリックします。

ステップ 49　**Next** をクリックします。

ステップ 50　**Finish** をクリックします。

関連情報

次の Microsoft ユーティリティは、Cisco CallManager に適用されている OS パッチを調べる場合に役立ちます。

- Hfnetck.exe：インストールされているプログラムおよびサービス　パックをボックスに表示し、新しいパッチを入手できるかどうかを示します。
- Serverinfo.exe：システムに関する基本情報および統計情報を表示します。
- Qfecheck.exe：インストールされているホットフィックスを表示します。このユーティリティは、SQL および Internet Explorer のホットフィックスに対して機能しません。また、Qfecheck は、実行中、プロセッサの使用率を急上昇させます。このユーティリティは、メンテナンス期間内にだけ実行することをお勧めします。

  Internet Explorer に適用されているホットフィックスを表示するには、次の手順を実行します。

手順

ステップ 1　Internet Explorer を開き、**Help > About Internet Explorer** をクリックします。

ステップ 2　Update Versions 行を調べます。

この行には、インストールされている各ホットフィックスの Knowledge Base 番号が一覧表示されます。

CHAPTER 4

Cisco CallManager システムの問題

この章では、Cisco CallManager システムに関連する、次のような一般的な問題の解決方法について説明します。

応答しない Cisco CallManager システム

この項では、応答しない Cisco CallManager システムに関する次の問題について説明します。

Cisco CallManager システムが応答を停止する

症状

Cisco CallManager システムが応答しません。

考えられる原因

Cisco CallManager サービス（ccm.exe）がクラッシュすると、システム イベント ログに次のメッセージが表示されます。

```
The Cisco CallManager service terminated unexpectedly.
It has done this 1 time. The following corrective action
will be taken in 60000 ms. Restart the service.
```

クラッシュの場合、次のようなメッセージが表示されることもあります。

```
Timeout 3000 milliseconds waiting for
Cisco CallManager service to connect.
```

Cisco CallManager は、次のエラーのために起動できませんでした。

```
The service did not respond to the start or control request in a
timely fashion.
```

この時点で、Cisco IP Phone やゲートウェイなどのデバイスが Cisco CallManager から登録解除されると、ユーザに発信音の遅延が発生したり、CPU の使用率が高いために Cisco CallManager サーバがフリーズしたりします。ここに記載されていないイベント ログ メッセージについては、『*Cisco CallManager Event Logs*』を参照してください。

Cisco CallManager サービスは、次のいずれかの原因でクラッシュすることがあります。

- Cisco CallManager サービスに、予期しないイベントが発生する。このクラッシュでは、既存の Dr.Watson ログにエントリが追加され、C:\Documents and Settings\All Users\Documents\DrWatson フォルダに user.dmp が生成されます。P.4-3 の「予期しないイベント」を参照してください。
- Cisco CallManager サービスが機能するための十分なリソース（CPU やメモリ）がない。通常、サーバの CPU 使用率はその時点で 100 % です。P.4-6 の「リソース不足」を参照してください。

発生するクラッシュのタイプに応じて、クラッシュの根本原因を特定するために役立つデータを収集する必要があります。

関連項目

- P.4-7 の「CPU の使用率が高くなることを防ぐためのバックアップ ユーティリティの設定確認」
- P.4-7 の「パフォーマンス モニタのカウンタ ログの設定」

予期しないイベント

Cisco CallManager がクラッシュした場合に必要な情報を収集して TAC に提供するには、次の手順を参考にしてください。

手順

ステップ 1　クラッシュの前後 15 分の Cisco CallManager トレースを収集します。このトレースは、**C:\Program Files\cisco\trace\ccm** にあります。

ステップ 2　クラッシュの前後 15 分の SDL トレースを収集します。このトレースは、C:\Program Files\cisco\trace\sdl\ccm にあります。

ステップ 3　**Start > Programs > Administrative Tools > Event Viewer** を選択し、**System Log** をクリックして、イベント ビューアでシステム イベント ログ ファイルを見つけ、**Action > Save Log as** を選択してログを保存します。アプリケーション ログに対してもこの操作を行います。

ステップ 4　各 Cisco CallManager で SdlMaxUnhandledExceptions パラメータが 0（ゼロ）に設定されていることを確認します。

ステップ 5　次の場所にある Dr. Watson ログ ファイルを見つけます。

C:\Documents and Settings\All Users\Documents\DrWatson

ファイル名は Drwtsn32.log です。

ステップ 6　C:\Documents and Settings\All Users\Documents\DrWatson で、user.dmp ファイルを見つけます。

（注）　これらのファイルは非常に大きい場合があります。TAC に送信する前にこれらのファイルを圧縮してください。これらのファイルには、TAC エンジニアおよび開発者がクラッシュの原因を特定するために必要な情報が含まれていることに注意してください。

ステップ 7　Notepad で Dr. Watson ログ ファイルを開き、最新のエントリを調べて、ccm.exe のエントリが追加されているかどうかを確認します。ファイルの一番下から始めて、**Application exception occurred** を検索します。これを検索することにより、最新のクラッシュを検出できます。

次に、Drwtsn32.log ファイルにあるクラッシュ エントリのヘッダーの例を示します。

```
Application exception occurred:
            App:  (pid=680)
            When: 3/8/2003 @ 14:01:06.978
            Exception number: e06d7363
```

クラッシュの日付と共に、PID が記載されています。その PID がタスク リスト内の ccm.exe の PID と一致する場合は、その Cisco CallManager がクラッシュしたことがわかります。

（注）　この例では、PID = 680 です。次のリストから、この PID が ccm.exe と一致することがわかります。

次に、Drwtsn32.log のタスク リストの例を示します。

例

```
PID  PROCESS
   8 System.exe
 212 SMSS.exe
 240 CSRSS.exe
 264 WINLOGON.exe
 292 SERVICES.exe
 304 LSASS.exe
 424 termsrv.exe
 520 svchost.exe
 560 msdtc.exe
 696 DLLHOST.exe
 736 Ipvmsapp.exe
 752 DLLHOST.exe
 824 AudioTranslator.exe
 848 RisDC.exe
 860 LogoutService.E.exe
 884 DCX500.exe
 936 svchost.exe
 980 LLSSRV.exe
1028 sqlservr.exe
1112 ntpd.exe
1140 rcmdsvc.exe
1172 regsvc.exe
1176 mstask.exe
1204 SNMP.exe
1244 WinMgmt.exe
1260 cpqnimgt.exe
1284 cqmgserv.exe
1296 cqmgstor.exe
1308 sysdown.exe
1372 cqmghost.exe
1524 aupair.exe
```

```
1552 sqlagent.exe
 276 svchost.exe
2400 inetinfo.exe
2412 explorer.exe
2752 sqlmangr.exe
2700 taskmgr.exe
2704 mmc.exe
 680 ccm.exe
 868 DRWTSN32.exe
```

PID のリストがない場合は、Drwtsn32.log の最新のエントリのタイムスタンプと、イベント ログ内のエラーのタイムスタンプを調べます（Cisco CallManager サービスのクラッシュに関する説明を参照してください）。これらのタイムスタンプが完全に同じ時刻である場合は、予期しないイベント Cisco CallManager クラッシュが発生した可能性があります。

クラッシュを一意にするのはスタック トレースです。このため、「予期しないイベント」の項で要求された完全な Drwtsn32.log ファイルを参照します。

クラッシュの日の PID が ccm.exe ではないか、タイムスタンプが一致しなかった場合は、リソース不足によるクラッシュまたは別のプロセスのクラッシュが発生している可能性が高くなります。

リソース不足

リソース不足によるクラッシュが発生している場合は、次の手順を実行します。

手順

ステップ **1**　クラッシュの前後 15 分の Cisco CallManager トレースを収集します。このトレースは、**C:\Program Files\cisco\trace\ccm** にあります。

ステップ **2**　クラッシュの前後 15 分の SDL トレースを収集します。このトレースは、**C:\Program Files\cisco\trace\sdl\ccm** にあります。

ステップ **3**　使用可能になっている場合は、perfmon トレースを収集します。

ステップ 4　このトレースが使用可能になっていない場合は、perfmon トレースの収集を開始して、サーバ上で動作しているプロセスごとにメモリと CPU の使用状況を追跡します。perfmon トレースを設定するには、「パフォーマンス モニタのカウンタ ログの設定」の項を参照してください。このトレースは、次にリソース不足によるクラッシュが発生した場合に役立ちます。

CPU の使用率が高くなることを防ぐためのバックアップ ユーティリティの設定確認

Cisco IP Telephony Applications Backup が高い CPU 使用率で長時間動作していたことが原因でシステムがクラッシュするのを避けるには、最新の Cisco IP Telephony Applications Backup を実行していることを確認します。

Cisco CallManager 3.1(3a)spC 以降または Cisco CallManager 3.2(1)spA 以降を実行している場合は、シスコ バグ ID CSCdt91655（登録済みのお客様専用）により、デフォルトで、新しいバックアップ ユーティリティが低いプライオリティで実行されます。

登録済みのお客様は、Voice Software ダウンロード ページの Cisco CallManager のセクションから最新バージョンの Cisco IP Telephony Application Backup をダウンロードできます。

この変更以前のバージョンでは、**Performance** という名前のタブを使用して、Cisco IP Telephony Applications Backup アプリケーションを実行するプロセスの Base Priority を変更していました。パフォーマンスを below normal または low に変更することにより、このプロセスが他のプロセス（normal の Base Priority で動作しているもの、たとえば ccm.exe）と、CPU について競合しないことが保証されます。

パフォーマンス モニタのカウンタ ログの設定

実行されているプロセス、および消費されている CPU とメモリの量を確認するには、次の手順を実行してクラッシュに関連するカウンタを収集します。

手順

ステップ 1　**Start > Programs > Administrative Tools > Performance** を選択します。

ステップ 2　パフォーマンス モニタから **Performance Logs > Alerts > Counter Logs** を選択します。

ステップ 3　**Action > New log settings** を選択し、カウンタ ログの名前を入力します。

ステップ 4　counters ページで **Add** をクリックします。

ローカル コンピュータのカウンタを使用し、クラッシュが発生している Cisco CallManager で直接この設定を行っていることを確認します。

ステップ 5　Performance Object で **Process** を選択します。

ステップ 6　Select Counters で **List > Select Instances** を選択し、次のカウンタおよび関連付けられているインスタンスをクリックします。

```
% Processor Time / All Instances
ID Process / All Instance
Virtual Bytes / All Instances
Private Bytes / All Instances
```

ステップ 7　Sample Data Every で、間隔を **2** に、単位を **seconds** に設定します。

Log Files タブで、ログ ファイルのタイプが **Text File - CSV** であることを確認します。また、ログ ファイルの場所に注意します。デフォルトは **C:\PerfLogs** です。**20,000 Kb** のログ ファイル制限を選択します。

ステップ 8　**Schedule** タブをクリックします。

ステップ 9　ログの開始用に **Start Log Manually** を選択します。

ステップ 10　ログの停止用に **When the 20,000 Kb Log File is Full** を選択します。

ステップ 11　ログが閉じたときのために Start a new log file を選択し、OK をクリックします。

ステップ 12　ロギングを開始するために、作成したカウンタ ログを選択します。

ステップ 13　**Action > Start** を選択します。

（注）　このようなパフォーマンス モニタ ログを有効にすると、時間が経つにつれて多数のファイルが生成され、大量のディスク スペースが使用されます。したがって、このアクティビティを監視し、多数のファイルが生成されている場合は、古いログを圧縮したりローカル ドライブから移動したりしてください。

ステップ 14　イベント ログ データは、必ずしも必要ではありません。ただし、先を見越してシステム イベントとアプリケーション イベントの両方をダンプし、クラッシュ直前の 30 分間のイベントだけを抽出する必要があります。TAC に送信する前にこれらのイベントを調べます。注意すべき点が見つかることがあります。

（注）　使用率の高いシステムでは、イベント ビューア（Microsoft の組み込みユーティリティ）を使用してこれらのイベントをテキスト ファイルにダンプすると、電話機登録の管理に使用される Cisco CallManager KeepAlive プロセスなど、他のすべてのプロセスが CPU 不足となることが多くあります。イベント ログ ファイルは .csv ファイル形式で保存してください。

ステップ 15　ファイルを電子メールで送信したりコピーしたりする前に、WinZip バージョン 8 を使用して、次の順序ですべてのファイルを圧縮します。通常は、速く評価するために、ファイルをローカル マシンにコピーします。ファイルを圧縮すると使用スペースが削減されるため、元のファイル形式よりも速くファイルを移動できます。

a. USER.DMP と DRWTSN32.LOG をまとめて圧縮します。この Zip ファイルと、症状についての説明を、すぐに送信およびコピーします。正確な Cisco CallManager バージョン、該当するデバイス負荷、および Cisco IOS バージョンも記載します。特別なパッチを使用している場合は、その点も明確にします。

b. Cisco CallManager トレース ファイルと SDL トレース ファイルをまとめて圧縮し、送信します。

c. パフォーマンス モニタのログをまとめて圧縮し、送信します。

d. イベント ログのエントリをまとめて圧縮し、送信します。

Cisco CallManager Administration ページが表示されない

症状

Administration Web ページが表示されません。

考えられる原因

Cisco CallManager サービスが停止しています。

推奨処置

次の手順を実行し、ローカル サーバまたはリモート サーバ上で Cisco CallManager サービスがアクティブであることを確認します。

1. Cisco CallManager Administration から、**Application > Cisco CallManager Serviceability** を選択します。

   Cisco CallManager Serviceability ウィンドウが表示されます。

2. **Tools > Service Activation** を選択します。

3. Servers カラムから、サーバを選択します。

   選択したサーバが Current Server というタイトルの隣に表示され、設定済みのサービスを示すボックスが表示されます。

   Cisco CallManager 行の Activation Status カラムに **Activated** または **Deactivated** と表示されます。

   Activated と表示された場合は、選択したサーバ上で Cisco CallManager がアクティブであるため、TAC に問い合せる必要があります。

   Deactivated と表示された場合は、引き続き次のステップを実行します。

4. **Cisco CallManager** チェックボックスをオンにします。

5. **Update** ボタンをクリックします。

   Cisco CallManager 行の Activation Status カラムに **Activated** と表示されます。

これで、選択したサーバの Cisco CallManager がアクティブになりました。

Cisco CallManager が使用されているかどうか、および現在アクティブであるかどうかを確認するには、次の手順を実行します。

1. Cisco CallManager Administration から、**Application > Cisco CallManager Serviceability** を選択します。

   Cisco CallManager Serviceability ウィンドウが表示されます。

2. **Tools > Control Center** を選択します。
3. Servers カラムから、サーバを選択します。

   選択したサーバが Current Server というタイトルの隣に表示され、設定済みのサービスを示すボックスが表示されます。

   Cisco CallManager 行の Activation Status カラムに **Activated** と表示されます。

   選択したサーバの Cisco CallManager はアクティブです。TAC に問い合せてください。

   Deactivated と表示された場合は、引き続き次のステップを実行します。
4. **Cisco CallManager** チェックボックスをオンにします。
5. **Update** ボタンをクリックします。

   Cisco CallManager 行の Activation Status カラムに **Activated** と表示されます。

   これで、選択したサーバの Cisco CallManager がアクティブになりました。

   上記の手順を繰り返し、Cisco CallManager サービスがアクティブになっていることを確認します。

ブラウザから Cisco CallManager Administration ページにアクセスしようとすると、エラーが発生する

症状

Cisco CallManager が常駐するサーバから administration ページにアクセスしようとすると、次のいずれかのエラー メッセージが表示されます。

- Internet Explorer：The page cannot be displayed.
- Netscape（警告ボックスが表示されます）：There was no response.The server could be down or is not responding.

考えられる原因

IIS Admin サービスまたは WWW パブリッシング サービスが、自動的に開始されません。ローカルでページが表示されない原因で最も多いのは、これらのサービスのいずれかが停止していることです。

推奨処置

次の手順を実行し、IIS を開始します。

（注）　IIS が停止している場合は、WWW パブリッシング サービスも停止している可能性があります。WWW パブリッシング サービスを開始すると、IIS が自動的に開始されます。

1. Start メニューから、**Start > Programs > Administration Tools > Services** を選択します。

   IIS Administration を含むウィンドウが表示されます。
2. **IIS Admin Service** を右クリックします。
3. **Start** を選択します。
4. **Yes** をクリックします。

   IIS が開始されます。

次の手順を実行し、その他のサービスを開始します。

1. Start メニューから、**Start > Programs > Administration Tools > Services** を選択します。
2. サービスを右クリックします。
3. **Start** を選択します。
4. **Yes** をクリックします。

   サービスが開始されます。

確認

次の手順を実行し、IIS が開始されていることを確認します。

1. Start メニューから、**Start > Programs > Administration Tools > Services** を選択します。
2. サービスを右クリックします。
3. ステータスを確認します。ステータスは、Started と表示される必要があります。
4. サービスが停止している場合は、次の手順を実行して、サービスを開始します。

次の手順を実行し、IIS を開始します。

（注）　IIS が停止している場合は、WWW パブリッシング サービスも停止している可能性があります。WWW パブリッシング サービスを開始すると、IIS が自動的に開始されます。

1. Start メニューから、**Start > Programs > Administration Tools > Services** を選択します。

   IIS Admin Service を含むウィンドウが表示されます。
2. **IIS Admin Service** を右クリックします。
3. **Start** を選択します。

4. **Yes** をクリックします。
5. IIS が開始されます。

次の手順を実行し、その他のサービスを開始します。

1. Start メニューから、**Start > Programs > Administration Tools > Services** を選択します。
2. サービスを右クリックします。
3. **Start** を選択します。
4. **Yes** をクリックします。
5. サービスが開始されます。

   ウィルスが原因で IIS サービスが停止し、administration ページにアクセスしようとすると、不審なメッセージが表示されることもあります。詳細については、「ウィルス保護」を参照してください。

ページを表示する権限がない

症状

administration ページにアクセスすると、次のエラー メッセージが表示されます。

エラー メッセージ　ページを表示する権限がない

また、次のようなエラー メッセージが表示されることもあります。

- You do not have permission to view this directory or page using the credentials you supplied.
- HTTP 401.3 Access denied by ACL on resource Internet Information Services.
- Server Application Error.The server has encountered an error while loading an application during the processing of your request.Please refer to the event log for more detailed information.Please contact the server administrator for assistance.
- Error: Access is Denied.

考えられる原因

Cisco CallManager サーバ上で、子ディレクトリに継承されるように C ドライブのルート ディレクトリに設定されていた NTFS 権限が変更されました。

NTFS 権限がサーバ上でデフォルト設定から変更されており、その権限では IIS を正常に実行できなくなっています。

推奨処置

Microsoft のサイト（次の URL）にアクセスし、問題 Q271071「Minimum NTFS Permissions Required for IIS 5.0 to Work」で詳細を参照します。

http://support.microsoft.com/default.aspx?ln=EN-GB&pr=kbinfo&

確認

次の手順を実行し、IIS が開始されていることを確認します。

1. Start メニューから、**Start > Programs > Administration Tools > Services** を選択します。
2. サービスを右クリックします。
3. ステータスを確認します。ステータスは、Started と表示される必要があります。
4. サービスが停止している場合は、次の手順を実行して、サービスを開始します。

次の手順を実行し、IIS を開始します。

（注）　IIS が停止している場合は、WWW パブリッシング サービスも停止している可能性があります。WWW パブリッシング サービスを開始すると、IIS が自動的に開始されます。

1. Start メニューから、**Start > Programs > Administration Tools > Services** を選択します。

   IIS Admin Service を含むウィンドウが表示されます。
2. **IIS Admin Service** を右クリックします。

3. **Start** を選択します。
4. **Yes** をクリックします。
   IIS が開始されます。

次の手順を実行し、その他のサービスを開始します。

1. Start メニューから、**Start > Programs > Administration Tools > Services** を選択します。
2. サービスを右クリックします。
3. **Start** を選択します。
4. **Yes** をクリックします。
   サービスが開始されます。

リモート サーバ上のブラウザから Cisco CallManager Administration ページにアクセスしようとすると、エラーが発生する

Cisco CallManager サーバ上で Administration Web ページにローカルではアクセスできても、リモート サーバからはこのページを参照できない場合は、次のいずれかの状況が該当するかどうかを確認してください。最も可能性の高い原因から順に記載しています。

Cisco CallManager でのユーザの表示または追加に関する問題

症状

Cisco CallManager Administration ユーザ ページでユーザを追加することも、検索することもできません。

考えられる原因

ホスト名に特殊文字（アンダースコアなど）が含まれるサーバにインストールされた Cisco CallManager 3.x で作業している場合、または SP2 および Q313675 パッチ以降が適用された MS Internet Explorer 5.5 で作業している場合、次の問題が発生することがあります。

- 基本的な検索を行うときに submit をクリックすると、同じページに戻る。
- 新しいユーザを追加しようとすると、次のエラー メッセージが表示される。

```
The following error occurred while trying to execute the
command.
Sorry, your session object has timed out.
Click here to Begin a New Search
```

推奨処置

Cisco CallManager のホスト名にアンダースコアやピリオドなどの特殊文字が含まれている場合（たとえば、Call_Manager）、Cisco CallManager Admin ユーザ ページでユーザを追加することも、検索することもできません。Domain Name System（DNS; ドメイン ネーム システム）でサポートされている文字は、すべての英字（A ～ Z、a ～ z）、数字（0 ～ 9）、およびハイフン（-）であり、特殊文字は使用できません。ブラウザに Q313675 パッチがインストールされている場合は、URL に DNS でサポートされていない文字が含まれていないことを確認してください。

Q313675 パッチの詳細については、「MS01-058: File Vulnerability Patch for Internet Explorer 5.5 and Internet Explorer 6.」を参照してください。

この問題を解決するには、次の方法があります。

- サーバの IP アドレスを使用して Cisco CallManager Admin ページにアクセスする。
- サーバ名に DNS でサポートされていない文字を使用しない。
- URL に localhost または IP アドレスを使用する。

SQLSvc ユーザがログインできない

症状

SQLSvc ユーザがログインできず、従属サービスが開始されません。

考えられる原因

Cisco CallManager、SQLServerAgent、MSSQLServer、および COM+ Event System サービスを開始して、サービス固有の機能を実行するには、SQLSvc ユーザがローカル システムにログインする必要があります。SQLSvc パスワードがローカルとクラスタ内の両方で正しく設定されていないと、SQLSvc ユーザはログインできず、従属サービスは開始されません。Cisco CallManager とその基本機能が影響を受ける可能性があります。

（注）　SQLSvc パスワードは、クラスタ全体で同じである必要があります。

この問題は、次のものに影響を及ぼします。

- Cisco CallManager
- Cisco CallManager 用の Microsoft SQL サーバ
- Cisco Music on Hold（MOH）Audio Translator
- Cisco Trivial File Transfer Protocol（TFTP）

推奨処置

次の手順を実行し、SQLSvc アカウント パスワードを回復します。

1. **Start > Programs > Administrative Tools > Computer Management** を選択します。
2. 左カラムの Local Users and Groups の隣にある +（プラス記号）をクリックします。
3. **Users** をクリックします。
4. 右カラムで **SQLSvc** を右クリックし、**Set Password** を選択します。
5. 新しいパスワードを入力し、パスワードを確認します。
6. **OK** をクリックして確定し、Change Password ダイアログボックスを閉じます。

7. 左カラムの Services and Applications の隣にある +（プラス記号）をクリックします。
8. **Services** をクリックします。
9. 右カラムで、**MSSQLServer 2000** をクリックして強調表示します。
10. **MSSQLServer 2000** を右クリックし、**Properties** を選択します。
11. **Log On** タブをクリックします。
12. パスワードを変更し、そのパスワードがステップ 5. で設定した SQLSvc ユーザ パスワードと一致することを確認します。
13. **OK** をクリックし、Services List に戻ります。
14. **SQLServerAgent** をクリックして強調表示します。
15. **SQLServerAgent** を右クリックし、**Properties** を選択します。
16. **Log On** タブをクリックします。
17. ステップ 5. で設定した SQLSvc ユーザ パスワードと一致するようにパスワードを変更します。
18. **OK** をクリックし、Services List に戻ります。
19. Computer Management ウィンドウを閉じます。
20. **Start > Programs > Administrative Tools > Component Services** を選択します。
21. Component Services の隣にある +（プラス記号）をクリックします。
22. Computers の隣にある +（プラス記号）をクリックします。
23. My Computer の隣にある +（プラス記号）をクリックします。
24. COM+ Applications の隣にある +（プラス記号）をクリックします。
25. **DBL** を右クリックし、**Properties** を選択します。
26. **Identity** タブをクリックします。
27. パスワードを変更し、そのパスワードがステップ 5. で設定した SQLSvc ユーザ パスワードと一致することを確認します。
28. **OK** をクリックし、Component Manager に戻ります。
29. **DBL** を右クリックし、**Shut Down** をクリックします。
30. **DBL** を右クリックし、**Start** をクリックします。
31. Component Manager ウィンドウを閉じます。

名前からアドレスへの解決の失敗

症状

次の URL にアクセスしようとすると、次のいずれかのエラー メッセージが表示されます。

http://your-cm-server-name/ccmadmin

Internet Explorer：`This page cannot be displayed`

Netscape：`Not Found.The requested URL / ccmadmin was not found on this server.`

名前ではなく Cisco CallManager の IP アドレス（http://10.48.23.2/ccmadmin）を使用して同じ URL にアクセスすると、ページが表示されます。

考えられる原因

「your-cm-server-name」に入力した名前が、DNS または hosts ファイルで間違った IP アドレスにマッピングされています。

推奨処置

1. DNS を使用するように設定した場合は、DNS を調べて、*your-cm-server-name* のエントリに Cisco CallManager サーバの正しい IP アドレスが関連付けられているかどうかを確認します。IP アドレスが正しくない場合は、変更します。
2. DNS を使用していない場合は、ローカル マシンで「hosts」ファイルを調べて、*your-cm-server-name* のエントリおよびそれに関連付けられている IP アドレスがあるかどうかを確認します。このファイルを開き、Cisco CallManager のサーバ名と IP アドレスを追加します。

   hosts ファイルは、Windows ステーションの **C:\WINNT\system32\drivers\etc\hosts** にあります。

Cisco CallManager のサーバ名を変更できない

症状

Cisco CallManager サーバの名前を変更しようとすると、サービスが失敗します。CTI Manager、Extended Functions、Voice Media Streaming など、他のサービスも失敗します。

考えられる原因

シスコは、Cisco CallManager サーバの名前の変更をサポートしていません。

推奨処置

次の手順を実行し、Cisco CallManager サーバの名前ではなく IP アドレスを変更します。

（注）　すべてのアプリケーションで IP アドレスを変更する必要があります。

1. Customer Response Applications Administration から、**System > Engine** を選択し、Engine Web ページにアクセスします。

（注）　この手順は、IP アドレスを変更するマシンに対して、お客様が Extended Services をインストールした場合、または CRS を共存インストールした場合に必要となります（Extended Services は、エクステンション モビリティのバージョン 3.2 以下で必要であり、また、IP-Auto Attendant または TAPS（これらは無料アプリケーション）のすべてのバージョンで必要です）。

図 4-1　Engine ウィンドウ：Engine Status 領域

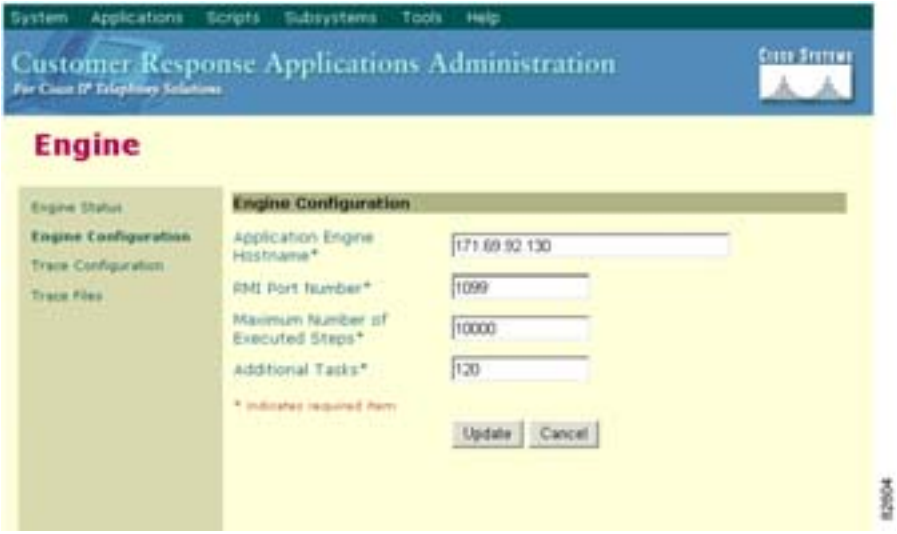
Engine Status 領域に、CRS システムとそのサブシステムに関する情報が表示されます。

2. **Stop Engine** ボタンをクリックし、CRS Engine を停止します。

（注）　Windows の Service ウィンドウから CRS Engine を制御することもできます。このウィンドウを表示するには、**Start > Programs > Administrative Tools > Services** を選択します。

3. Engine Web ページのナビゲーション バーで **Engine Configuration** ハイパーリンクをクリックして Engine Configuration 領域にアクセスします。この領域には、ユーザ プロファイル作成中に指定した情報が表示されます。

図 4-2　Engine ウィンドウ：Engine Configuration 領域



4. Application Engine Hostname フィールドに、サーバの新しい IP アドレスを入力します。
5. Customer Response Applications Administration から、**Subsystems > JTAPI** を選択します。

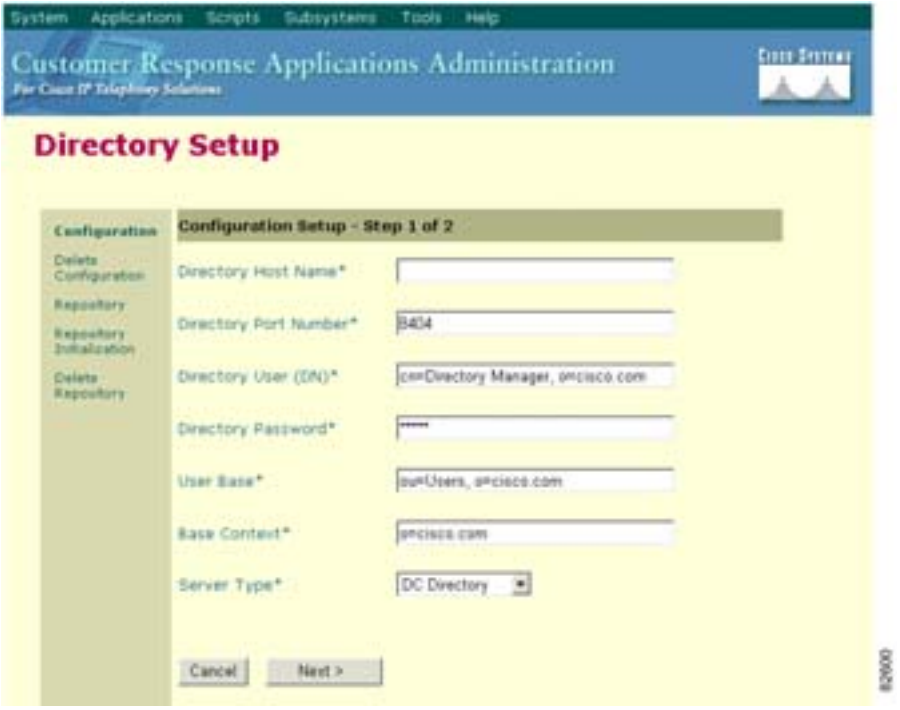
   JTAPI Configuration Web ページが表示されます。

図 4-3　JTAPI Configuration ウィンドウ

6. JTAPI Provider(s) フィールドに、Cisco CallManager CTI Manager を実行する Cisco Media Convergence サーバ（Cisco MCS）の新しい IP アドレスを入力します。
7. Customer Response Applications Administration から、**System > Configuration and Repository** を選択します。

   Directory Setup ウィンドウが表示されます。

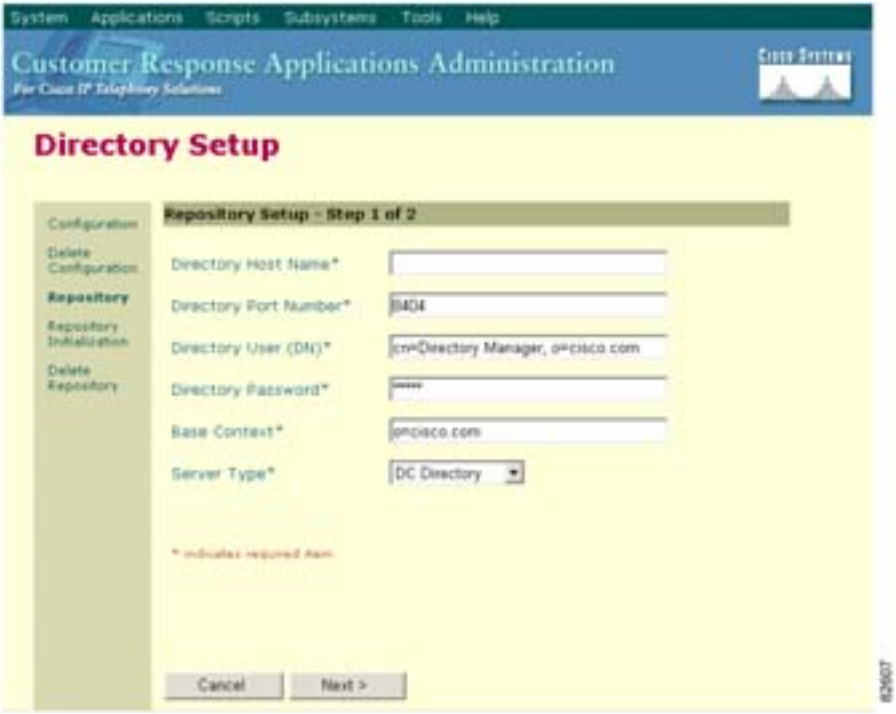
図 4-4　Directory Setup ウィンドウ：Configuration Setup 領域



8. **Directory Host Name** フィールドに、新しい IP アドレスを入力します。
9. Directory Setup ウィンドウのナビゲーション バーで **Repository** ハイパーリンクをクリックします。

   Repository Setup 領域が表示されます。

図 4-5　Directory Setup ウィンドウ：Repository Setup 領域



10. **Directory Host Name** フィールドに、新しい IP アドレスを入力します。
11. **Control Panel > Administrative Tools > Services** を選択し、サーバ上の DC Directory サービスを停止します。
12. **Start > Programs > DC Directory Administrator Directory Manager** を選択します。
13. インストール中に入力した*ディレクトリ マネージャ パスワード*を入力します。
14. **Directory > cisco.com > CCN > systemProfile** を選択します。
15. **Hoteling Profile** をダブルクリックします。
16. **Modify** をクリックし、新しい IP アドレスを入力します。

17. Cisco CallManager Administration で、**System > Server** を選択し、新しい IP アドレスを入力します。
18. Cisco CallManager Administration で、**System > Enterprise Parameters** を選択し、URL Directories に新しい IP アドレスを入力します。複数の URL エントリを変更する必要がある場合があります。
Help、Authentication、Directories、Information、および Services はすべて、Enterprise Parameters の下に URL があります。
19. Cisco CallManager Administration で、**Features > Phone Services** を選択し、すべての URL に新しい IP アドレスを入力します。これは、変更しているサーバを指す URL すべてに適用されます。サービスは、他のサーバの www サイトを指すことができます（多くの場合、他のサーバの www サイトを指す必要があります）。
20. Network Properties で、Server IP address を新しい IP アドレスに変更します。
21. クラスタ内のすべてのサーバで、LMHOSTS ファイルと HOSTS ファイルを新しい IP アドレスに変更します。
22. DHCP Option 150 を新しい IP アドレスに変更します。
23. **Start > Programs Microsoft SQL Server 2000 > Enterprise Manager** を選択して SQL Enterprise Manager を開き、Plugin テーブル内の URL で IP アドレスを変更します。
24. **ツリー サーバ名 > Databases >** ***最新の CCM03xx データベース*** を選択します。
25. **Tables > PlugIn** を選択します。
26. **PlugIn** を右クリックしてテーブルを開き、**Return All Rows** を選択します。

（注）　変更はただちに実行されます。変更を取り消すことはできません。

27. **Start > Programs Administrative Tools > Services Console > stiBack for Cisco IP Telephony Applications** を選択して stiBackup 設定を開き、該当するすべてのタブに新しい IP アドレスを入力します。
28. **C:\TAPS\TAPSCCM.txt** で、新しい IP アドレスを入力します。

IIS のデフォルト Web サイトの設定が正しくない

症状

次の URL にアクセスしようとすると、次のいずれかのエラー メッセージが表示されます。

http://your-cm-server-name/ccmadmin

- Internet Explorer：`This page cannot be displayed`
- Netscape：`Not Found.The requested URL /ccmadmin was not found on this server.`

名前ではなく Cisco CallManager の IP アドレス（http://10.48.23.2/ccmadmin）を使用して同じページにアクセスすると、ページが表示されます。

考えられる原因

サーバ上で、IIS の **Default Web Site** タブの設定が正しくありません。

推奨処置

1. Cisco CallManager マシンの Internet Service Manager で、**Default Web Site** を確認します。**Web Site** タブで、マシンの IP アドレスではなく **All Unassigned** を選択します。

   この設定を確認するには、次のように選択します。
   Start > Programs > Administrative tools/Internet Service Manager
   サーバ名を示すアイコンを展開します。
2. **Default Web Site** を右クリックします。選択する必要のあるオプションのプロパティが用意されています。**Web Site** タブを探し、**All Unassigned** 設定を確認します。

（注）　何らかの理由で特定の IP アドレスを保持する必要がある場合は、リモート Web ブラウザから IP アドレスの代わりに名前を使用できません。

ローカル ブラウザと Cisco CallManager サーバの間にある 1 つまたは複数のルータでポート 80 がブロックされる

症状

ファイアウォールが Web サーバまたは http トラフィックによって使用されるポートをブロックすると、次のいずれかのエラー メッセージが表示されます。

- Internet Explorer：`This page cannot be displayed`
- Netscape：`There was no response.The server could be down or is not responding`

考えられる原因

セキュリティ上の理由から、システムが、ローカル ネットワークからサーバ ネットワークへの http アクセスをブロックしました。

推奨処置

1. Cisco CallManager　サーバへの他のタイプのトラフィック（ping　や Telnet など）が許可されるかどうかを確認します。許可されるトラフィックがある場合は、リモート ネットワークから Cisco CallManager Web サーバへの http アクセスがブロックされていると考えられます。
2. ネットワーク管理者に連絡して、セキュリティ ポリシーを確認します。
3. サーバが配置されているそのネットワークから、再試行します。

アクセスが明示的に拒否されているマシンにアクセスしようとする

症状

次のいずれかのエラー メッセージが表示されます。

- Internet Explorer：`This page cannot be displayed`
- Netscape：`Not Found.The requested URL / ccmadmin was not found on this server.`
- **show friendly http error messages** 詳細設定が行われていない両方のブラウザから：`Access to this server is forbidden.`

考えられる原因

ネットワーク管理者によって適用されているセキュリティ ポリシーが原因と考えられます。

推奨処置

1. ネットワーク管理者に連絡して、セキュリティ ポリシーを確認します。別のマシンから再試行します。
2. 自分がネットワーク管理者である場合は、Cisco CallManager サーバの Internet Service Manager で、**Default Web Site** の **Directory Security** タブを確認します。
3. この設定を確認するには、次のように選択します。

   Start > Programs > Administrative tools/Internet Service Manager
4. サーバ名を示すアイコンを展開します。
5. **Default Web Site** を右クリックします。選択する必要のあるオプションのプロパティが用意されています。
6. **Directory Security** タブを探し、設定を確認します。

ブラウズに使用しているリモート マシンのネットワーク設定が正しくない

症状

接続性がありません。または、Cisco CallManager と同じネットワーク内の他のデバイスへの接続性がありません。

他のリモート マシンから同じアクションを試行すると、Cisco CallManager Administration ページが表示されます。

考えられる原因

ステーションまたはデフォルト ゲートウェイのネットワーク設定が正しくないと、そのネットワークへの接続性が一部または完全になくなるため、Web ページが表示されないことがあります。

推奨処置

1. Cisco CallManager サーバおよび他のデバイスの IP アドレスに ping を試行し、接続できないことを確認します。

2. ローカル ネットワークから他のどのデバイスへの接続も失敗する場合は、自分のステーションでネットワーク設定を確認します。また、ケーブルとコネクタの整合性を確認します。
3. ローカル ネットワークから他のどのデバイスへの接続も失敗する場合は、自分のステーションでネットワーク設定を確認します。また、ケーブルとコネクタの整合性を確認します。詳細については、該当するハードウェアのマニュアルを参照してください。

   LAN で TCP-IP を使用して接続している場合は、引き続き次のステップを実行して、リモート ステーションのネットワーク設定を確認します。
4. **Start > Setting > Network and Dial-up connections** を選択します。
5. **Local Area Connection** を選択し、**Properties** を選択します。

   チェックボックスがオンになった状態で、通信プロトコルのリストが表示されます。
6. **Internet Protocol (TCP-IP)** を選択し、**Properties** を再度クリックします。
7. ネットワークに応じて、**Obtain an ip address automatically** または **set manually your address, mask and default Gateway** のどちらかを選択します。

   ブラウザ固有の設定が正しくない可能性もあります。
8. Internet Explorer ブラウザで、**Tools > Internet Options** を選択します。
9. **Connections** タブを選択し、LAN 設定またはダイヤルアップ設定を確認します。

   デフォルトでは、LAN 設定およびダイヤルアップ設定は行われていません。Windows からの一般的なネットワーク設定が使用されます。
10. Cisco CallManager ネットワークへの接続だけが失敗する場合は、ネットワークにルーティングの問題が存在する可能性があります。ネットワーク管理者に連絡して、デフォルト ゲートウェイに設定されているルーティングを確認します。

（注）　この手順を実行してもリモート サーバからブラウズできない場合は、TAC に連絡し、問題の詳しい調査を依頼してください。

設定の詳細については、次の URL を参照してください。

http://www.cisco.com/warp/public/63/initial_config.shtml

パブリッシャとサブスクライバの間で複製が失敗する

SQL データベースの複製は、Cisco CallManager クラスタの中核機能です。データベースのマスター コピーを持つサーバはパブリッシャと呼ばれ、そのデータベースを複製するサーバはサブスクライバと呼ばれます。

パブリッシャが使用できないため、データを更新できない

症状

次のエラー メッセージが表示されます。

エラー メッセージ `Cannot update data because the publisher is not available. Please try again later. (58)`

考えられる原因

サブスクライバの構築に失敗しました。

推奨処置

1. すべてのサーバ間で NetBIOS 名前解決が機能していることを確認します。
2. 各サーバが他のサーバのホスト名および NetBIOS 名を解決できるように、パブリッシャ サーバおよびサブスクライバ サーバ上の hosts と LMHOSTS にデータが入力されていることを確認します（必要に応じて、これらのファイルを編集します）。

   hosts は DNS 解決に使用されます。LMHOSTS は、名前解決に NetBIOS を使用します。SQL も名前解決に NetBIOS を使用します。

   Cisco CallManager が更新に失敗する場合は、サブスクライバのデータベース層がパブリッシャを検出できません。
3. パブリッシャの SQL「ディストリビューション エージェント」で、履歴とエラーを確認します。
4. **Start > Programs > Administrative Tools > Local Security Policy** を選択します。
5. **Audit Policy** を選択します。

6. **Failure auditing for all events** を有効にします。
   SQL に対して、**Authentication** を有効にします。

（注）　ユーザは、SQL ではなく DC Directory で複製されます。

7. Web から、Cisco CallManager をパブリッシャ上のソフトウェア バージョンにアップグレードします。
   サブスクライバに SQL データベースがダウンロードされます。

サブスクライバがパブリッシャからのデータ複製を停止する

症状

パブリッシャ上で行われた変更が、サブスクライバに登録されている電話機に反映されません。

考えられる原因

パブリッシャとサブスクライバの間で複製が失敗しています。

推奨処置

次の手順を実行し、2 つのシステム間の関係を再確立します。まず、パブリッシャ上でサブスクライバのサブスクリプションを再作成する必要があります。次に、サブスクリプションを削除し、サブスクライバ システム上で再作成します。

パブリッシャ上のサブスクリプションの再作成

1. パブリッシャから **Programs > Microsoft SQL Server 2000 > Enterprise Manager** を選択し、SQL Enterprise Manager を起動します。
2. サブスクリプションは、パブリッシャから再作成できます。Microsoft SQL Server で、**New SQL Server Registration...** を選択します。
   Register SQL Server Wizard が表示されます。**From now on I want to perform the task without using a wizard** チェックボックスがオフであることを確認します。

3. **Next** をクリックします。

   Cisco CallManager 上に存在するその他の SQL サーバが Additional Servers ボックスに表示されます。

4. すべてのサーバを選択し、Added servers ボックスに **Add**（追加）します。
5. **Next** をクリックします。

   The SQL Server login information that was assigned to me by the system administrator をクリックします。

6. **Next** をクリックします。
7. 次の画面で、サブスクライバ システムの「sa」アカウントとパスワードを使用します。

（注）　これは、「サブスクライバ」システムの sa アカウントとパスワードです。パスワードは、サブスクライバ システムのインストール時に選択されたものです。

8. Select SQL Server Group ウィンドウで、オプション **Add the SQL server(s) to the existing SQL Server group** を選択します。
9. **Finish** をクリックします。

   Finish を選択すると、追加したサーバの追加のステータスがウィザードに表示されます。

   「Registered successfully」と表示されます。

10. **Close** をクリックします。

    画面の 2 つのサーバのリストは、これらのサーバがパブリッシャによって認識されていることを意味します。したがって、これらのサーバとデータを共有できます。

パブリッシャ上のサブスクリプションの削除

次の手順を実行し、パブリッシャ上のサブスクリプションを削除します。

1. Enterprise Manager から **Microsoft SQL Servers > SQL Server Group > Machine_name > Databases > CCM0301 > Publications** を選択し、CCM0301 データベースのパブリケーションを見つけます。

2. 障害の発生している Cisco CallManager サブスクリプションを選択し、そのエントリを削除します。

（注）　右側のエリアを選択します。左側の本のアイコンは削除しないでください。

パブリッシャでサブスクリプションが削除されたが、サブスクライバでは削除されていないことを示す警告が表示され、サブスクライバに接続してサブスクリプションを削除するかどうかの確認を求められます。

3. **Yes** をクリックします。

次に、サブスクリプションは削除されたが、データは削除されていないことを示すメッセージが表示されます。

4. **OK** をクリックします。

サブスクライバ上のサブスクリプションの再作成

次に、サブスクライバ SQL サーバにサブスクリプションを再び追加する必要があります。次の手順を実行し、サブスクライバ上にサブスクリプションを再作成します。

1. パブリッシャから削除したサブスクライバの SQL サーバ名を選択します。
2. 右クリックして、メニューを表示します。
3. メニューから **New > Pull Subscription** を選択します。

（注）　必ず、以前のバージョンではなく最新バージョンのデータベースを選択してください。

Pull Subscription Wizard が表示されます。

4. **Next** をクリックします。
5. Choose Publication 画面で、パブリッシャ（表示されています）を展開し、データベースを選択します。
6. **Next** をクリックします。

7. Specify Synchronization Agent Login 画面で、**Using SQL Server Authentication of this account** を選択します。

   ログイン名は sa で、パスワードはパブリッシャの **sa** アカウントと同じパスワードになります。

8. Specify Immediate-Updating Subscription(s) ポップアップで、**Yes, make this an immediate-updating subscription(s)** をクリックします。
9. **Next** をクリックします。
10. Initialize Subscription 画面で、**Yes, initialize the schema and data at the Subscriber** をクリックします。
11. **Next** をクリックします。
12. Set Distribution Agent Schedule ポップアップで、**Continuously** を選択します。
13. **Next** をクリックします。
14. 次のステップで、SQL サーバ エージェントと Microsoft DTC サービスの両方が動作していることを確認します。
15. **Next** をクリックします。
16. Completing the Pull Subscription Wizard 画面で、**Finish** をクリックします。

    サブスクリプションが設定され、完了時に、成功したと表示されます。

    プロセスが完了すると、成功を示す画面が表示されます。
17. これでサブスクリプションが作成されました。次に、スナップショット エージェントを実行し、データをサブスクライバに渡して同期化する必要があります。
18. パブリッシャ SQL サーバを選択し、**Replication Monitor > Publishers > Machine_name >CCM0301 subscription** を選択します。
19. **Snapshot** エントリを選択し、**Start** を選択します。

    この時点でスナップショット エージェントが実行されます。タスクが完了するまでに約 3 ～ 5 分かかります。スナップショット エージェントが完了すると、プル エージェントが起動してスナップショットをサブスクライバに適用します。これにはさらに 3 ～ 5 分かかります。
20. パブリッシャでプル サブスクリプションが完了したら、サブスクライバ SQL サーバを選択し、CCM0301 データベースのプル サブスクリプションを開きます。

    サブスクリプションは実行状態で、更新を待っています。

（注）　最後のアクションが「Waiting for snapshot agent to become available」のままである場合は、F5 キーを押して画面を更新してください。

この時点で、サブスクライバはパブリッシャと再び同期化され、ローカル サブスクライバ SQL データベースに更新が記録されています。

確認

次の手順を実行し、SQL サブスクリプションが機能していることを確認します。

1. データの伝播をテストするには、容易に認識できるデバイスをパブリッシャ サーバ上に作成します。

（注）　デバイスが認識しやすいほど、検出が容易になります。

2. **Insert** をクリックします。

   デバイスが機能している必要はありません。

3. **Update** and **Close** をクリックします。
4. SQL Enterprise Manager で、該当する SQL サブスクライバを展開し、データベース テーブルを調べて新しいデバイスが存在するかどうかを確認します。

サーバの応答が遅い

この項では、サーバからの応答が遅いことに関連する問題である「デュプレックス ポート設定の不一致」について説明します。

デュプレックス ポート設定の不一致

症状

サーバからの応答が遅くなっています。

考えられる原因

スイッチのデュプレックスが Cisco CallManager サーバ上のデュプレックス ポート設定と一致しない場合、応答が遅くなることがあります。

推奨処置

1. 最適なパフォーマンスを得るには、スイッチとサーバの両方を **100/Full** に設定します。

   スイッチでもサーバでも Auto 設定を使用することはお勧めしません。
2. Cisco CallManager サーバを再起動して、この変更を有効にする必要があります。

JTAPI サブシステムの起動に関する問題

Java Telephony API（JTAPI）サブシステムは、Cisco Customer Response Solutions（CRS）プラットフォームの非常に重要なコンポーネントです。JTAPI は、Cisco CallManager と通信するコンポーネントで、テレフォニー コール制御を担当します。CRS プラットフォームは、Cisco AutoAttendant、Cisco IP ICD、Cisco IP-IVR などのテレフォニー アプリケーションをホストします。この項は、これらのうち特定のアプリケーションを対象としているわけではありません。JTAPI サブシステムは、これらすべてのアプリケーションによって使用される基本コンポーネントです。

トラブルシューティング プロセスを開始する前に、使用しているソフトウェア バージョンの互換性を確認してください。互換性を確認するには、使用している Cisco CallManager のバージョンの Cisco CallManager Release Notes を読んでください。

CRS のバージョンを確認するには、http://servername/appadmin（*servername* は、CRS がインストールされているサーバの名前）と入力して AppAdmin ページにログインします。メイン メニューの右下隅に、現在のバージョンが表示されます。

JTAPI サブシステムが OUT_OF_SERVICE である

症状

JTAPI サブシステムが起動しません。

考えられる原因

トレース ファイルに次のいずれかの例外が表示されます。

- MIVR-SS_TEL-4-ModuleRunTimeFailure
- MIVR-SS_TEL-1-ModuleRunTimeFailure

MIVR-SS_TEL-4-ModuleRunTimeFailure

トレース ファイルで **MIVR-SS_TEL-1-ModuleRunTimeFailure** という文字列を検索します。その行の末尾に、例外の原因が記載されています。

一般的なエラーは、次のとおりです。

- Unable to create provider ー bad login or password
- Unable to create provider -- Connection refused
- Unable to create provider -- login=
- Unable to create provider -- hostname
- Unable to create provider -- Operation timed out
- Unable to create provider -- null

Unable to create provider ー bad login or password

考えられる原因

JTAPI 設定に入力されているユーザ名またはパスワードが正しくありません。

エラー メッセージの全テキスト

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI
Subsystem,Failure Cause=7,Failure
Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create providerÅ|bad login or password
%MIVR-SS_TEL-7-
EXCEPTION:com.cisco.jtapi.PlatformExceptionImpl:
Unable to create providerÅ|bad login or password
```

推奨処置

ユーザ名とパスワードが正しいことを確認します。Cisco CallManager で CCMuser ページ（http://servername/ccmuser）にログインし、Cisco CallManager が正しく認証できることを確認します。

Unable to create provider -- Connection refused

考えられる原因

Cisco CallManager への JTAPI 接続が、Cisco CallManager によって拒否されました。

エラー メッセージの全テキスト

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl: Unable
Unable to create provider -- Connection refused
%MIVR-SS_TEL-7-EXCEPTION:com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- Connection refused
```

推奨処置

Cisco CallManager Control Center で、CTI Manager サービスが実行されていることを確認します。

Unable to create provider -- login=

考えられる原因

JTAPI configuration ページで、設定が行われていません。

エラー メッセージの全テキスト

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- login=
%MIVR-SS_TEL-7-EXCEPTION:com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- login=
```

推奨処置

CRS サーバの JTAPI configuration ページで、JTAPI プロバイダーを設定します。

Unable to create provider -- hostname

考えられる原因

CRS エンジンが Cisco CallManager のホスト名を解決できません。

エラー メッセージの全テキスト

```
%M%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- dgrant-mcs7835.cisco.com
%MIVR-SS_TEL-7-EXCEPTION:com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- dgrant-mcs7835.cisco.com
```

推奨処置

CRS エンジンから、DNS 解決が正しく機能していることを確認します。DNS 名ではなく、IP アドレスを使用してみます。

Unable to create provider -- Operation timed out

考えられる原因

CRS エンジンに、Cisco CallManager との IP 接続性がありません。

エラー メッセージの全テキスト

```
101: Mar 24 11:37:42.153 PST
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- Operation timed out
102: Mar 24 11:37:42.168 PST %MIVR-SS_TEL-7-EXCEPTION:
com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- Operation timed out
```

推奨処置

CRS サーバで、JTAPI プロバイダーに設定されている IP アドレスを確認します。CRS サーバと Cisco CallManager で、デフォルト ゲートウェイの設定を確認します。IP ルーティングの問題が存在しないことを確認します。CRS サーバから Cisco CallManager に ping を実行して、接続性をテストします。

Unable to create provider -- null

考えられる原因

JTAPI プロバイダーの IP アドレスまたはホスト名が設定されていません。または、JTAPI クライアントが正しいバージョンを使用していません。

エラー メッセージの全テキスト

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-time
failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl:
Unable to create provider -- null
```

推奨処置

JTAPI 設定で、ホスト名または IP アドレスが設定されていることを確認します。JTAPI のバージョンが正しくない場合は、Cisco CallManager Plugins ページから JTAPI クライアントをダウンロードし、CRS サーバにインストールします。

MIVR-SS_TEL-1-ModuleRunTimeFailure

症状

この例外は、通常、JTAPI サブシステムがポートを初期化できない場合に発生します。

考えられる原因

CRS サーバは Cisco CallManager と通信できますが、JTAPI を介して CTI ポートまたは CTI ルート ポイントを初期化できません。このエラーは、CTI ポートおよび CTI ルート ポイントが JTAPI ユーザに関連付けられていない場合に発生します。

エラー メッセージの全テキスト

```
255: Mar 23 10:05:35.271 PST %MIVR-SS_TEL-1-ModuleRunTimeFailure:
Real-time failure in JTAPI subsystem: Module=JTAPI Subsystem,
Failure Cause=7,Failure Module=JTAPI_SS,Exception=null
```

推奨処置

Cisco CallManager で JTAPI ユーザをチェックし、CRS サーバに設定されている CTI ポートおよび CTI ルート ポイントがユーザに関連付けられていることを確認します。

JTAPI サブシステムが PARTIAL_SERVICE である

症状

トレース ファイルに次の例外が表示されます。

MIVR-SS_TEL-3-UNABLE_REGISTER_CTIPORT

考えられる原因

JTAPI サブシステムが、1 つまたは複数の CTI ポートまたはルート ポイントを初期化できません。

エラー メッセージの全テキスト

```
1683: Mar 24 11:27:51.716 PST
MIVR-SS_TEL-3-UNABLE_REGISTER_CTIPORT
Unable to register CTI Port: CTI Port=4503,
Exception=com.cisco.jtapi.InvalidArgumentExceptionImpl:
Address 4503 is not in provider's domain.
1684: Mar 24 11:27:51.716 PST %MIVR-SS_TEL-7-EXCEPTION:
com.cisco.jtapi.InvalidArgumentExceptionImpl:
Address 4503 is not in provider's domain.
```

推奨処置

トレース内のエラー メッセージには、どの CTI ポートまたはルート ポイントを初期化できなかったかが記載されています。このデバイスが Cisco CallManager 設定に存在すること、および Cisco CallManager でこのデバイスが JTAPI ユーザに関連付けられていることを確認します。

セキュリティ

この項では、次のセキュリティ問題について説明し、セキュリティ プロセスに関する詳細なマニュアルを参照できる場所を示します。

セキュリティのための IIS パラメータの変更

症状

IIS サーバをロックダウンして Cisco CallManager をハッカー、攻撃、または脅威から保護するための設定が失われています。

考えられる原因

Cisco CallManager をアップグレードまたは再インストールすると必ず、すべての IIS 設定が Cisco CallManager のデフォルトに戻ります。

推奨処置

実稼働サーバで設定を変更する前に、非実稼働 Cisco CallManager ですべての設定をテストします。

アップグレードまたは再インストールのたびに設定が変更されるため、設定を書き留めて、再設定する必要があります。

（注）　Cisco web ディレクトリ内の設定を変更しないでください。変更すると、ファイルが欠落または移動するため、Cisco CallManager サービスが失われる恐れがあります。

短期的なセキュリティ ソリューション

次のドキュメントを参照して、ネットワーク全体で quality of service（QoS; サービス品質）が正しく設定されていることを確認し、残りのクリーンアップ操作中に音声品質への影響ができるだけ小さくなるようにします。

- *Cisco IP Telephony QoS Design Guide*
- *Cisco IP Telephony Network Design Guide*
- *IP Telephony Solutions Guide*

これらのガイドは、次の URL で提供されています。

http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/index.htm

個別の Voice/Data VLAN を確立する方法については、『*Cisco IP Telephony Network Design Guide*』を参照してください。

（注）　関連するネットワークのサイズや複雑さによっては、短期的なソリューションが長期的なソリューションになることもあります。

長期的なセキュリティ ソリューション

次の URL にあるマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/index.htm

関連情報

次の URL では、『*Cisco CallManager Security Patch Process*』が提供されています。

http://www.cisco.com/warp/public/cc/pd/nemnsw/callmn/prodlit/cmspp_qa.pdf

Microsoft からパッチをインストールしないことを強くお勧めします。CCO から、ラップ バージョンをダウンロードしてください。

次の URL で Microsoft のセキュリティ パッチ アラートにサインアップできます。

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp

アラートには、関連する格付けが記載されているため、ホットフィックスが CCO に提供される推定時刻がわかります。

IP テレフォニー ネットワークのセキュリティの考慮事項については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/ip_tele/index.htm

ウィルス保護

アクティブなセキュリティ攻撃を停止させるための手順、または差し迫ったセキュリティ リスクを防ぐための手順については、次の URL を参照してください。

http://www.cisco.com/en/US/partner/products/sw/voicesw/ps556/prod_security_advisories_list.html

サーバに最新のパッチが適用されていることを確認するには、次のドキュメントを参照してください。

- *Cisco CallManager インストレーション ガイド*
- *Cisco CallManager アップグレード手順*
- *Cisco CallManager Upgrade Assistant Utility の使用方法*

CHAPTER 5

ディレクトリの問題

この章では、Lightweight Directory Access Protocol（LDAP）ディレクトリを使用する Cisco CallManager DC Directory（DCD）、および Microsoft Active Directory（AD）に関連する一般的な問題の解決方法について説明します。

この章では、次のディレクトリ問題について説明します。

- DC Directory の安定性
- DC Directory でユーザ設定用のアプリケーション プロファイルが表示されない
- 新しいユーザの追加が機能せず、DC Directory Administrator にアクセスできない
- 子ドメインがダウンしていると、Active Directory でスキーマ更新が失敗する
- ユーザ ページへのアクセスに失敗した後、SSL を介した Netscape Directory プラグインが失敗する
- SSL を介した LDAP での Netscape Directory 統合では、データベースに CA 証明書が必要である

次の手順でディレクトリの問題が解決されない場合は、TAC に連絡して詳細な調査を依頼してください。

注意 DC Directory、Netscape Directory、または Active Directory でカタカナやキリルなどのダブルバイト文字セットを使用すると、ディレクトリ データベース エラーが発生することがあります。このリリースの Cisco CallManager では、どのディレクトリでもダブルバイト文字セットの使用をサポートしていません。

IP Phone のディレクトリ問題の詳細については、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_ipphon/index.htm

複製の問題

複製の問題については、第 4 章「Cisco CallManager システムの問題」および P.4-32 の「パブリッシャとサブスクライバの間で複製が失敗する」を参照してください。

DC Directory の安定性

「DCD の不安定性」の手順は、バージョン 4.0(1) 以降を実行している Cisco CallManager サーバで有効です。

DCD の不安定性

症状

次の問題は、DCD の不安定性に関連しています。

- Cisco CallManager パブリッシャ サーバには正しいユーザ データがあるが、1 つまたは複数の Cisco CallManager サブスクライバ サーバにユーザ データがないか、ユーザ データがパブリッシャのデータベースよりも古い。
- Cisco CallManager パブリッシャ サーバ上の DC Directory サービスの開始に時間がかかる（開始時にストールまたはハングしているように思える）。
- Cisco CallManager パブリッシャ サーバまたはサブスクライバ サーバ（あるいはその両方）の Application Event Viewer に、DC Directory Replication エラーが記録される。

  考えられる原因

  C:\dcdsrvr\run\dcx500\dcx500.out を調べると、重複する複製許諾契約または無効な複製許諾契約（あるいはその両方）があります。

  無効な複製許諾契約があると、DC Directory データベース（C:\dcdsrvr\run\dcx500\database 内のファイル）が大きくなりすぎて（100 MB を超える）、DC Directory の終了および起動に非常に時間がかかります。

  このような重複する許諾契約や無効な許諾契約は、次のいずれかの原因によって発生します。

  - お客様が Cisco Customer Response Solutions（CRS）サーバ（または Cisco CallManager サブスクライバ）を 1 回以上再インストールした（CRS サーバまたは Cisco CallManager サーバを再インストールするたびに、サブスクライバに対する新しい複製許諾契約がパブリッシャに作成される）。
  - Cisco CallManager クラスタ内で、DC Directory の再設定手順を実行せずに、既存の CRS サーバ（または Cisco CallManager サブスクライバ）を破棄した。

（注）　Cisco CallManager クラスタからディレクトリ ノードを削除しても、削除したサブスクライバに対する DC Directory 複製許諾契約は自動的にクリーンアップされません。

－ サブスクライバ上で **avvid_scfg** コマンドを複数回手動で実行した（たとえば、DC Directory 再設定手順の一部を試行した）。

（注）　DC Directory 再設定手順の一部を実行しないでください（たとえば、パブリッシャと CRS サーバや Cisco CallManager サブスクライバ上で **cleandsa** を実行せずに **avvid_scfg** を実行するなど）。

データベースがこのように大きくなる根本的な原因は、DC Directory が、複製に失敗するたびに各複製処理の状態を保存しようとするためです。時間が経つにつれて、無効な複製許諾契約に関する状態情報が保存されて、データベースが数百 MB にもなります。

DcDirectory 複製を SQLServer 複製と混同しないでください。これらは、完全に独立した 2 つのプロセスです。

Cisco CallManager サブスクライバを再インストールする場合は、DC Directory パブリッシャから始めて、クラスタ内のすべてのノード（スタンドアロン CRS サーバを含む）で DC Directory の再設定手順を実行する必要があります。

推奨処置

これらのタスクの実行中は、Keyboard/Video/Mouse（KVM）スイッチを介して接続された Media Convergence Server（MCS）サーバのコンソールの前にいるか、または Telnet を介して MCS サーバに接続している必要があります。Terminal Services Client 接続で接続してこれらのタスクを実行することは十分にテストされていないため、予期せぬ結果が生じることがあります。

（注）　ダウンタイムにこの手順を実行するようにスケジュールすることをお勧めします。

再設定

インストール後に DC Directory を再設定する場合は、次の 2 つのシナリオが考えられます。

- DC Directory データベースが 100 MB より大きい。
- DCD データベースが 100 MB より小さい。

両方の手順を次に示します。

Cisco CallManager パブリッシャでの DC Directory の再設定（データベースが 100 MB より大きい場合）

この手順では、DC Directory データベース（C:\dcdsrvr\run\dcx500\database）が 100 MB より大きい場合、この手順の実行中に障害などが発生したときに備えて、パブリッシャ Cisco CallManager サーバ上の DC Direcory 内にあるユーザ データを確実にバックアップします。

1. MCS バックアップ ユーティリティを使用するか、DOS コマンド プロンプトから **dcbckdib /y backup C:\dcdsrvr\backup** コマンドを実行して、現在のディレクトリ情報をバックアップします。

   （注）　前述のコマンドを実行するには、C:\dcdsrvr\backup フォルダが存在する必要があります。

2. パブリッシャ サーバで、Administrator としてログインし、**Start > Run** を選択して **cmd** と入力し、コマンド プロンプトを開きます。
3. **avvid_migrate_save.cmd <*servername*><*password*>** コマンドを入力し、プロンプトが表示されたら任意のキーを押します。

このコマンドでは、次のような出力が表示されます。

```
C:\>avvid_migrate_save jayas-w2k ciscocisco
A subdirectory or file C:\dcdsrvr\log already exists.

**************************************
*                                    *
* -- CISCO User Preferences Support -- *
*                                    *
**************************************

A subdirectory or file C:\dcdsrvr\suspense already exists.

Run the perl script avvid_migrate_save.pl
A subdirectory or file C:\dcdsrvr\log already exists.
A subdirectory or file
C:\dcdsrvr\run\DCX500\config\Migration-Backup already
exi
sts.
Saving User Information...
Saving Profile Information...
Saving Apps20 Information...
Saving Admin Information...
Saving PA node Information...
Saving E911 node Information...
Saving systemProfile...
Saving MITRA data...
Saving Groups data...


C:\>
```

4. コマンド プロンプトから **net stop dcdirectory** と入力し、DC Directory サービスを停止します。
5. **cleandsa.cmd** を実行します。cleandsa.cmd がサポートされていないことが cleandsa.cmd によって報告される場合は、**deletedib.cmd** を実行します。
6. **avvid_migrate_cfg "*<password>*"** を実行します。
7. **avvid_migrate_restore *<Server Name>* *<Directory Manager Password>*** を実行します。
8. **reconfig_cluster *<Directory Manager Password>*** を実行します。

このコマンドにより、すべての Cisco CallManager サブスクライバに対する複製許諾契約が確立されます。Cisco CallManager サブスクライバでタスクを実行する必要はありません。

Cisco CallManager パブリッシャでの DC Directory の再設定（データベースが 100 MB より小さい場合）

DCD データベース（C:\dcdsrvr\run\dcx500\database）が 100 MB より小さい場合は、次の手順を実行し、Cisco CallManager パブリッシャの DC Directory を再設定します。

1. **reconfig_cluster.cmd** を実行します。
2. このコマンドにより、すべての Cisco CallManager サブスクライバ サーバに対する複製許諾契約が確立されます。Cisco CallManager サブスクライバで追加の手順を実行する必要はありません。

（注）　ネットワークに 1 つの Cisco CallManager サーバがある場合は、そのサーバに CRS が共存しているかどうかに関わらず、**reconfig_cluster.cmd** コマンドを実行してください。この場合は、Cisco CRS サーバ用の手順は実行しないでください。

DC Directory でユーザ設定用のアプリケーション プロファイルが表示されない

症状

ユーザをディレクトリに追加しているときに、アプリケーション プロファイル（AutoAttendant、Softphone、エクステンション モビリティなど）が表示されず、ユーザをアプリケーション プロファイルにリンクできません。

考えられる原因

アプリケーション プロファイルが正しく設定されていません。

推奨処置

次の手順を実行してアプリケーション プロファイルを設定し、DC Directory にユーザを追加または表示できるようにします。

1. **DC Directory Administrator** に接続します。
2. **Directory > cisco.com > CCN** を選択します。
3. **systemProfile** をクリックします。
4. **systemProfile** を右クリックし、**Properties** を選択します。
5. **Application Install Status** タブをクリックします。
6. アプリケーションの値を確認します。「AA Installed」、「Softphone Installed」、「ASR Installed」、および「Hotelling Installed」の値がブランクである場合は、7. に進みます。

   それ以外の場合は、11. に進みます。
7. **Modify** を選択します。
8. 値を true から **false** に変更し、false の値は **true** に変更します。
9. **Apply** をクリックします。
10. **OK** をクリックします。
11. 4. と 5. を繰り返します。
12. **Modify** をクリックします。
13. すべての値が表示されます。
14. インストールされているアプリケーションの値を **true** に変更します。
15. **Apply** をクリックします。
16. **OK** をクリックします。
17. **Services** をクリックします。
18. 右のパネルで、**World Wide Web Publishing Service** を選択します。
19. **Restart Service** アイコンをクリックします。
20. 問題が発生したクラスタ内のすべてのサーバに対してすべてのステップを繰り返します。

確認

DC Directory にアプリケーション プロファイルが表示されます。

新しいユーザの追加が機能せず、DC Directory Administrator にアクセスできない

症状

Cisco CallManager Administration からユーザを追加できません。また、DC Directory Administrator にログインすることもできません。

新しいユーザを追加すると、次のエラーが表示されます。

エラー メッセージ `Sorry your session object has timed out. Click here to Begin a New search.`

新しいユーザを検索すると、ページが更新され、入力待機状態になります。

考えられる原因

ディレクトリ マネージャのユーザ パスワードに、「^」などの特殊文字が含まれています。

推奨処置

次の手順を実行し、DC Directory パスワードを、特殊文字を含まないパスワードに変更します。

（注）　DC ディレクトリ マネージャのパスワードを変更するには、スーパーユーザ アカウント特権を持っている必要があります。

（注）　クラスタ内にパブリッシャ サーバと 1 つまたは複数のサブスクライバ サーバがある場合は、クラスタ内のすべての Cisco CallManager で次の手順を実行する必要があります。

1. Cisco CallManager Administration から、**Start > Programs > DC Directory Administrator** を選択します。
2. **Next** をクリックします。

3. Password フィールドに、デフォルト パスワード **cisco** を入力し、**Finish** をクリックします。

   DC Directory Administrator ウィンドウが表示されます。

4. Tools メニューから、**Change Password** を選択します。

   Change User Password ウィンドウが表示されます。

5. Old Value フィールドに、**cisco** と入力します。

6. New Value フィールドに、特殊文字を含まない新しい *ÉpÉXÉèÅ[Éh* を入力します。

7. Confirm New Value フィールドに、新しい *ÉpÉXÉèÅ[Éh* を再入力します。

8. **OK** をクリックします。

   DC Directory パスワードが変更されます。

9. 「Windows レジストリの設定」に進みます。

Cisco CallManager Administration は、DC Directory LDAP サーバ上での追加、削除、または更新の各操作にもディレクトリ マネージャ アカウントを使用します。

Windows レジストリの設定

次の手順を実行し、レジストリに格納されている情報を更新して、レジストリが正しいディレクトリを指すようにします。

1. コマンドラインを開き、**c:\dcdsrvr\bin** と入力します。

2. passwordutils.exe とパスワードを入力します。

   passwordutils.exe *password*

3. **Enter** キーを押します。

   レジストリに、この暗号化パスワード値情報が必要です。

4. **Start > Run** を選択します。

5. Open フィールドに、**regedit** と入力します。

   Registry Editor ウィンドウが表示されます。

6. My Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\Directory Configuration に移動します。

LDAPURL が正しいディレクトリを指す必要があります。

`ldap://`*host:port*

7. **DCDMGRPW** をダブルクリックします。

   Edit String ウィンドウが表示されます。

8. Value Data フィールドに、ステップ 3. で取得した暗号化パスワード値を入力します。
9. **OK** をクリックします。
10. Registry Editor ウィンドウから、**MGRPW** をダブルクリックします。

    Edit String ウィンドウが表示されます。

11. Value Data フィールドに、ステップ 3. で取得した暗号化パスワード値を入力します。
12. **OK** をクリックします。

    レジストリでパスワードを正常に変更しました。

（注）　レジストリ エントリの変更後は、Cisco CallManager ノード上の WWW サービスと IIS サービスを再起動して、レジストリから最新の設定を取得する必要があります。

13. **Control Panel > Administrative Tools** を選択します。
14. **Services** をダブルクリックします。

    Services ウィンドウが表示されます。

15. **Worldwide Web Publishing Service** を選択します。
16. **Stop** をクリックします。
17. **Start** をクリックします。
18. **DC Directory Server** を選択します。
19. **Stop** をクリックします。
20. **Start** をクリックします。

    Cisco Customer Response Solutions（CRS）、Cisco IPCC Express 3.5（x）、または Cisco CallManager Extended Services 3.5（x）を使用している場合は、次の「CRS および Extended Services のディレクトリ マネージャ パスワードの再設定」の手順に進みます。

CRS および Extended Services のディレクトリ マネージャ パスワードの再設定

次の手順を実行し、ディレクトリ マネージャ パスワードを更新します。

1. 前述の「Windows レジストリの設定」の手順で使用した暗号化パスワードのコピーを作成します。
2. CRS サーバで CMD プロンプトを開き、ディレクトリを c:\winnt\system32\ccn サブディレクトリに変更します。
3. 'dir'<Enter> を入力し、ディレクトリの内容を表示します。'ccndir.ini' という名前のファイルを見つける必要があります。'copy ccndir.ini ccndir.ini.oldpass'<Enter> を入力し、そのファイルのバックアップを作成します。
4. 'notepad ccndir.ini'<Enter> を入力し、ccndir.ini ファイルを開いて編集します。'MGRPW' と書いてある行を見つけます。この行を見て、引用符の内側の暗号化文字列を、ステップ 1 で記録した暗号化パスワードに置き換えます。
5. ccndir.ini ファイルを閉じて保存します。
6. CRS サーバで Application Administration ページを開き、ログインします。メニューから、System、Engine を選択します。エンジンを停止および開始して、すべてのサブシステムが IN_SERVICE であることを確認します。

確認

Cisco CallManager の DC ディレクトリ マネージャのパスワードを正常に変更したことを確認するには、次の手順を実行します。

1. Cisco CallManager Administration から、**User > Global Directory** を選択します。

   User Information ウィンドウが表示されます。
2. **Search** をクリックします。
3. システムに設定されているユーザが表示される場合は、設定が成功しています。

システムに設定されているユーザが表示されない場合は、次の情報を確認します。

- 新しいパスワードが有効である（新しいパスワードで DC Directory にログインします）。
- 暗号化パスワードがレジストリに正しく入力されている。
- ディレクトリが、別のディレクトリ（AD や、空の可能性のある古いディレクトリ）ではなく、正しいディレクトリを指している。
- Worldwide Web Publishing サービスと DC Directory サービスが再起動され、再起動後に実行されている。

子ドメインがダウンしていると、Active Directory でスキーマ更新が失敗する

症状　1 つの子ドメインがダウンしていると、2 ドメインの Active Directory Forest 構成でスキーマ更新が失敗します。

考えられる原因　子ドメインがネットワークから接続解除されている可能性があります。

推奨処置　Cisco CallManager を Active Directory Forest と統合する場合、すべてのドメインがネットワークに接続されている必要があります。スキーマ更新をフォレスト全体に複製するために、スキーマ マスター サーバは、すべてのドメインにアクセスできる必要があります。

ユーザ ページへのアクセスに失敗した後、SSL を介した Netscape Directory プラグインが失敗する

症状　Netscape Directory を統合するプラグインが、無効な SSL 証明書で実行されている場合、ユーザ ページを表示できません。

考えられる原因　Netscape Directory を統合するプラグインが、無効な SSL 証明書で実行されています。たとえば、ND サーバが、WebServer 証明書を持っている必要がある場合に、Subordinate Certification Authority 証明書を持っています。

推奨処置　Netscape Directory マシンで、Netscape Directory Service を再起動します。次に、有効な証明書を使用して、Cisco CallManager を Netscape Directory と統合するプラグインを再び実行します。

SSL を介した LDAP での Netscape Directory 統合では、データベースに CA 証明書が必要である

症状　SSL を介した Netscape Directory 統合で、ユーザ ページにアクセスできません。

考えられる原因　証明書データベースに CA 証明書が存在しません。

推奨処置　証明書データベースに CA 証明書をコピーしてから、プラグインを実行します。Cisco CallManager（LDAP クライアント）が、Netscape Directory Server（LDAP Server）証明書に署名した者を特定できない場合、LDAP クライアントは証明書が本物であると確信できないため、Netscape Directory Server への接続が失敗します。

関連情報

ディレクトリのインストールと設定については、次の URL にアクセスしてください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/install

CHAPTER 6

デバイスの問題

この章では、Cisco 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のある、次のような一般的な問題について説明します。

音声品質

通話中に、音声信号の損失や歪みなど、音声品質の問題が発生することがあります。

一般的な問題としては、音声が途切れる（言葉が聞き取れないなど）、異常なノイズが入る、音声が歪む（エコーが聞こえるなど）、音声がこもったり合成音のようになったりする、といった問題があります。単方向音声（二者間でどちらか一方だけに音声が聞こえる会話）は、本来は音声品質の問題ではありませんが、この問題についてもこの章で取り上げます。

音声問題は、次のアイテムのいずれか 1 つまたは複数で発生する可能性があります。

- ゲートウェイ
- 電話機
- ネットワーク

この項では、次の一般的な音声品質問題について説明します。

音声の損失または歪み

症状

発生する可能性のある最も一般的な問題の 1 つに、音声信号の途切れがあります（これは、「音声が聞き取りにくい」、「単語や文の中の音節が脱落する」などとよく言われる問題です）。この問題の一般的な原因は、パケット損失とジッタの 2 つです。どちらか 1 つまたは両方が原因になる場合があります。パケット損失とは、音声パケットがドロップされたため、または到達が遅すぎて無効になったために、音声パケットが宛先に到達しないことを意味します。ジッタは、パケットの到達時間のばらつきを示します。最適的な状況では、すべての Voice over IP

（VoIP）パケットが正確に 20 ミリ秒（ms）に 1 個の割合で到達します。ジッタは、パケットがポイント A からポイント B に到達する所要時間ではなく、単に、パケット到達時間のばらつき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、遅延のばらつきの原因が数多く存在します。それらの原因の中は、制御できるものとできないものがあります。パケット音声ネットワークにおける遅延のばらつきを完全になくすことはできません。電話機などの音声対応デバイス上の Digital Signal Processors（DSP; デジタル信号プロセッサ）は、遅延のばらつきを想定して音声の一部を計画的にバッファリングします。このデジッタリングは、音声パケットが宛先に到達し、通常の音声ストリームに使用される準備が整った場合に限り実行されます。

Cisco IP Phone 7960 は、1 秒間の音声サンプルをバッファリングできます。ジッタ バッファは状況に応じて使用されます。つまり、一度に大量のパケットが受信された場合、Cisco IP Phone 7960 はジッタを制御するためにそれらのパケットを再生することができます。ネットワーク管理者は、quality of service（QoS; サービス品質）などの手段をあらかじめ適用することで、パケット到達時間のばらつきを最小化する必要があります（この作業は、コールが WAN を経由する場合は特に重要です）。

ビデオ エンドポイントの中には、G.728 をサポートしていないものもあります。そのため、G.728 を使用するとノイズが発生することがあります。そのような場合には、G.729 など、別のコーデックを使用してください。

推奨処置

1. 音声の損失または歪みの問題が発生した場合は、最初に、その音声のパスを割り出す必要があります。そのコールの音声ストリームのパスにある各ネットワーク デバイス（スイッチおよびルータ）を特定します。音声は、2 台の電話機間、電話機とゲートウェイ間、または複数の区間（電話機からトランスコーディング デバイスまでの区間、およびそのトランスコーディング デバイスから別の電話機までの区間）に存在する場合があることに留意してください。問題が発生しているのは、2 つのサイト間だけか、特定のゲートウェイを介した場合だけか、特定のサブネット上か、などを特定します。このような作業によって、さらに詳しく調べる必要があるデバイスの範囲を絞り込むことができます。
2. 次に、無音抑止（Voice Activation Detection または VAD とも呼ばれます）を無効にします。このメカニズムは、無音がある場合に音声を送信しないようにすることで帯域幅を節約しますが、単語の最初の部分で顕著な（容認できない）音飛びが発生する原因となる場合があります。

Cisco CallManager Administration でこのサービスを無効にし、**Service > Service Parameters** を選択します。表示されたメニューで、サーバと Cisco CallManager サービスを選択します（図 6-1 を参照）。

図 6-1　Cisco CallManager Administration の Service メニュー

3. Cisco CallManager　クラスタ内のすべてのデバイスに対して無音抑止を無効にするには、SilenceSuppression を **False** に設定します。または、SilenceSuppressionForGateways を **False** に設定する方法もあります。判断に迷う場合は、それぞれ **False** を選択して、両方ともオフにします。
4. ネットワーク アナライザが使用可能な場合には、ネットワーク アナライザを使用して、無音抑止が無効の状態で 2 台の電話機間の監視対象コールに 1 秒あたり 50 パケット（20 ミリ秒あたり 1 パケット）が存在するかどうかを確認します。適切なフィルタリングを行うことで、極端に多くのパケットが失われていないか、または遅延していないかを確認できます。

   音飛びの原因となるのは遅延そのものではなく、遅延のばらつきだけです。下記の表に注目してください。この表は、20 ミリ秒の音声パケット（RTP ヘッダーを含む）間の到達時間に関する完全なトレースを表しています。低品質のコール（多くのジッタが含まれるコールなど）の場合、到達時間は大きく変動します。

   次の表は、完全なトレースを示しています。

パケット番号	時間 - 絶対値（秒）	時間 - 増分値（ミリ秒）
1	0	
2	0.02	20
3	0.04	20
4	0.06	20
5	0.08	20

パケット アナライザをネットワーク内のさまざまなポイントに配置すると、遅延が発生する場所の数を絞り込むのに役立ちます。使用可能なアナライザがない場合は、他の方法を使用する必要があります。音声のパス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。

診断に使用する Call Detail Record（CDR）には、低音質のコールの追跡に役立つ別のツールが指定されています。CDR の詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。

Cisco IP Phone による音声問題の解決

症状

音声問題はコールの進行中に発生します。

考えられる原因

デバイスでは高速インターフェイスが低速インターフェイスに送り込まれるため、デバイスが遅延とパケット損失の最も一般的な原因になります。たとえば、ルータによっては、LAN に接続された 100 メガバイト（MB）のファースト イーサネット インターフェイスと WAN に接続された低速フレームリレー インターフェイスを持っている場合があります。リモート サイトに通信しているときにだけ音声品質が低下する場合は、その問題の最も可能性の高い原因としては、次のようなことが挙げられます。

- データ　トラフィックより音声トラフィックが優先されるようにルータが正しく設定されていない。
- アクティブ コールの数が多すぎて WAN がサポートできない（つまり、発信可能なコール数を制限するコール アドミッション制御がない）。

－ 物理ポートのエラーが発生している。

－ WAN 自体で輻輳が発生している。

LAN 上の最も一般的な問題は、物理レベルのエラー（CRC エラーなど）です。これらのエラーは、ケーブルやインターフェイスの障害、またはデバイスの誤った設定（ポートの速度やデュプレックスの不一致など）が原因で発生します。トラフィックがハブなどのシェアドメディア デバイスを通過していないことを確認してください。

推奨処置

Cisco IP Phone 7960 には、発生する可能性のある音声問題を診断するためのツールが別途用意されています。

1. アクティブ コールに対して、*i* ボタンをすばやく 2 回押すと、電話機の情報画面に、パケットの送受信に関する統計情報、平均ジッタ カウンタ、および最大ジッタ カウンタが表示されます。

（注） この画面で、ジッタは最後に到達した 5 パケットの平均値を表し、最大ジッタは平均ジッタの最大値を表します。

2. トラフィックが予想よりも遅いパスでネットワークを通過す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のであれば、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。アドミッション制御を実行するには、トポロジに応じて、Cisco CallManager Administration 設定の **Locations** 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します。いずれの場合も、WAN 全体でサポートされ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 ノイズの診断

3. クラックル ノイズ（パチパチという音）も音声品質の低下を示す症状の 1 つです。これは、電源装置の欠陥や電話機周辺の何らかの強い電気的干渉が原因になる場合があります。電源装置を交換し、電話機を移動してください。

ロードの確認

4. ゲートウェイと電話機のロードを確認します。www.cisco.com の Cisco Connection Online（CCO）で、最新のソフトウェアのロード、新しいパッチ、または問題に関連するリリース ノートがあるかどうかを確認します。

確認

1. 「音声の損失または歪み」の説明に従って無音抑止を無効にしてテストを行います。次に、2 つのサイト間で通話します。パケットが送信されなくなるので、コールを保留または消音にしないでください。
2. WAN を経由するコールの最大数が設定されていれば、すべてのコールは許容できる品質になります。
3. コールをもう 1 件発信しようとしたときに、速いビジー音が返ってくることを確認するテストを行います。

エコー

症状

エコーが発生するのは、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、遠端の受信パスに連結されたときです。このとき、送話者には、エコーパスの合計遅延時間の分だけ遅れて自分の声が聞こえます。

音声は反響することがあります。従来の音声ネットワークでは、反響しても遅延が小さいので認識されません。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、パケット化と圧縮により遅延が大きくなるため、常にエコーは明確に認識されます。

考えられる原因

エコーの原因は必ずアナログ コンポーネントと配線にあります。たとえば、IP パケットは、低い音声レベルのソースまたはデジタル T1/E1 回線上のソースに方向を変えて戻ることができません。例外となる可能性があるのは、一方がスピーカフォンを使用して音量を極端に高く設定している場合など、音声ループが生成されるような状況が発生している場合だけです。

推奨処置

1. 問題の電話機でスピーカフォンが使用されていないこと、およびヘッドセットの音量が適切なレベル（最大音声レベルの 50 パーセントから開始する）に設定されていることを確認します。ほとんどの場合、この問題は、デジタル ゲートウェイまたはアナログ ゲートウェイを経由して PSTN に接続しているときに発生します。

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判別します。デジタル ゲートウェイが使用されている場合、送信方向に（PSTN に向かって）パディングを追加できます。信号の強度を低下させると反響するエネルギーが減少するので、この方法で問題を解決できます。

   これに加えて、受信レベルを調整することで、反響音をさらに小さくすることもできます。1 回の調整は微量にすることが重要です。信号の減衰量が大きすぎると、コールの両側で音声が聞こえなくなります。

3. 通信事業者に連絡して、回線の確認を依頼する方法もあります。北米で一般的な T1/PRI 回線の場合、入力信号は -15 dB である必要があります。信号レベルがそれよりも大幅に高い（たとえば -5 dB）場合は、エコーが発生する可能性があります。

エコー ログの記録

4. エコーが発生したすべてのコールのログを記録する必要があります。

   問題が発生した時刻、発信側の電話番号、および着信側の電話番号を記録します。ゲートウェイのエコー キャンセレーションは固定で 16 ミリ秒に設定されています。

   反響音の遅延がこれよりも大きい場合、エコー キャンセラは正常に動作できません。正常に動作できなくても、市内電話については問題ありませんが、長距離電話の場合は、セントラル オフィスでネットワークに組み込まれた外部エコー キャンセラを使用する必要があります。この事実は、エコーが発生するコールの外部電話番号を記録することが重要である理由の 1 つです。

ロードの確認

5. ゲートウェイと電話機のロードを確認します。www.cisco.com の Cisco Connection Online で、最新のソフトウェアのロード、新しいパッチ、または問題に関連するリリース ノートがあるかどうかを確認します。

単方向音声または無音声

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を介してコールを確立すると、一方の側しか音声を受信しません（単方向通信）。

2 つの Cisco ゲートウェイ間でトールバイパス コールを確立すると、一方の側しか音声を受信しません（単方向通信）。

考えられる原因

この問題が発生する可能性があるのは、特に、Cisco IOS Gateway、ファイアウォール、またはルーティングの設定が正しくない場合、またはデフォルト ゲートウェイに問題がある場合です。

推奨処置

Cisco IOS ゲートウェイまたはルータで IP ルーティングが有効になっていることを確認する

VG200 など、Cisco IOS ゲートウェイの中には、IP ルーティングがデフォルトで無効になっているものがあります。これが原因で単方向音声の問題が発生します。

（注）　作業を進める前に、ルータの IP ルーティングが有効になっている（つまり、ルータにグローバル設定コマンド **no ip routing** が設定されていない）ことを確認してください。

IP ルーティングを有効にするには、Cisco IOS ゲートウェイで次のグローバル設定コマンドを入力するだけです。

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

基本 IP ルーティングの確認

基本 IP の到達可能性は、必ず最初に確認する必要があります。RTP ストリームは UDP で転送されるコネクションレス型なので、トラフィックは一方向には正常に進みますが、反対方向には正常に進みません。

次の点を確認してください。

- エンド ステーションにデフォルト ゲートウェイが設定されている。
- そのデフォルト ゲートウェイの IP ルートが宛先ネットワークに通じている。

（注）　各種 Cisco IP Phone のデフォルト ルータまたはゲートウェイの設定を検証する方法を次に示します。

- Cisco IP Phone 7910：**Settings** を押し、オプション 6 を選択してから、Default Router フィールドが表示されるまで下向きの音量キーを押します。
- Cisco IP Phone 7960/40：**Settings** を押し、オプション 3 を選択してから、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 IP Phone 2sp+/30vip：**# を押してから、gtwy= が表示されるまで # を押します。

（注）　Cisco IP SoftPhone アプリケーションを使用していて、複数の Network Interface Card（NIC; ネットワーク インターフェイス カード）がボックスにインストールされている場合は、ボックスに正しい NIC が設定されていることを確認してください。この問題は、Cisco IP SoftPhone ソフトウェア バージョン 1.1.x に共通する問題です（バージョン 1.2 では解決します）。

（注）　Cisco DT24+ Gateway の場合は、DHCP Scope を確認し、スコープ内に Default Gateway (003 router) オプションがあることを確認してください。003 router パラメータは、デバイスと PC の Default Gateway フィールドに読み込まれるものです。スコープ オプション 3 には、ゲートウェイ用のルーティングを実行するルータ インターフェイスの IP アドレスが指定されている必要があります。

H.323 シグナリングを Cisco IOS ゲートウェイまたはルータ上の特定の IP アドレスにバインドする

Cisco IOS ゲートウェイにアクティブな IP インターフェイスが複数ある場合、H.323 シグナリングの一部は 1 つの IP アドレスから調達され、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。この結果、さまざまな問題が発生します。その 1 つが単方向音声です。

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属すことができます（ループバック）。インターフェイス設定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 CallManager 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 Release 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) にはバグが存在するため、このソリューションでは単方向音声の問題が発生する可能性があります。詳細については、Cisco Software Bug Toolkit（登録済みのお客様専用）でバグ ID CSCdw69681（登録済みのお客様専用）を参照してください。

Telco または交換機から応答監視が正しく送受信されていることを確認する

Telco または交換機に接続された Cisco IOS ゲートウェイが含まれる実装では、Telco または交換機の内側にある着信側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てい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）できず、単方向音声となります。回避方法は、**voice rtp send-recv on** を設定することです。

Cisco IOS ゲートウェイまたはルータで voice rtp send-recv を使用し、双方向音声を早期にカットスルーする

RTP ストリームが開始されるとすぐに、逆方向の音声パスが確立されます。順方向の音声パスは、Cisco IOS ゲートウェイが Connect メッセージをリモート エンドから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 チャネルが開いたらすぐに（Connect メッセージが受信される前に）双方向の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** グローバル設定コマンドを使用します。

Cisco IOS ゲートウェイまたはルータのリンクバイリンク ベースの cRTP 設定を確認する

この問題は、複数の Cisco IOS ルータまたはゲートウェイが音声パスに関与していて、Compressed RTP（cRTP; 圧縮 RTP）が使用されている、トールバイパスなどのシナリオに該当します。cRTP、つまり RTP ヘッダー圧縮機能は、VoIP パケットのヘッダーを小さくして帯域幅を取り戻すための方法です。cRTP では、VoIP パケット上に 40 バイトの IP/UDP/RTP ヘッダーを設定し、それを 1 パケットにつき 2 ～ 4 バイトに圧縮するので、G.729 で符号化されたコールの場合、cRTP 使用時に約 12 KB 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、すべてのホップで圧縮解除と再圧縮が行われます。ルーティングするには各パケット ヘッダーを検査する必要があるので、IP リンクの両端で cRTP を有効にする必要があります。

リンクの両端で cRTP が期待どおりに機能していることを確認することも重要です。各 Cisco IOS レベルは、スイッチング パスと同時 cRTP サポートによって異なります。

履歴の要約を次に示します。

- Cisco IOS Software Release 12.0.5T まで、cRTP はプロセス交換されます。
- Cisco IOS Software Release 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; Cisco エクスプレス転送）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 Software Release 12.1.2T では、アルゴリズムのパフォーマンスが向上しています。

Cisco IOS プラットフォーム（IOS Release 12.1）上で cRTP を実行している場合は、バグ CSCds08210（登録済みのお客様専用）（VoIP and FAX not working with RTP header compression ON）がご使用の IOS バージョンに影響しないことを確認します。

Cisco IOS ゲートウェイまたはルータ上の NAT に必要な最低限のソフトウェア レベルを確認する

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、最低限のソフトウェア レベルを満たす必要があります。以前のバージョンの NAT は Skinny プロトコル変換をサポートしないので、単方向音声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低限のソフトウェア レベルは、Cisco IOS® Software 12.1(5)T です。IOS ゲートウェイが NAT を使用して Skinny と H.323v2 をサポートするには、このレベルのソフトウェアが必要です。

（注）　Cisco CallManager が Skinny シグナリング用にデフォルトの 2000 と異なる TCP ポートを使用している場合は、**ip nat service skinny tcp port<number>** グローバル設定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 ファイアウォール上で NAT と Skinny を同時に使用するために必要な最低限のソフトウェア レベルは 6.0 です。

（注）　これらのレベルのソフトウェアが、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するわけではありません。ゲートキーパーのサポートについては、この文書では取り上げません。

AS5350 および AS5400 の voice-fastpath を無効にする

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設定コマンドを取得します。これは、デフォルトで有効になっています。これを無効にするには、**no voice-fastpath enable** グローバル設定コマンドを使用します。

有効になっていると、このコマンドは特定のコール用に開いている論理チャネルの IP アドレスと UDP ポート番号の情報をキャッシュします。それによって RTP ストリームはアプリケーション層に到達できなくなり、それより下位の層にパケットが転送されます。そのため、大量のコールがあるシナリオでは CPU 使用率がわずかに抑えられます。

保留や転送などの補助的なサービスを使用している場合、voice-fastpath コマンドを使用すると、ルータは保留されたコールの再開後または転送の完了後に収集された新しい論理チャネルの情報を無視して、キャッシュされている IP アドレスと UDP ポートに音声を送信します。この問題を回避するには、論理チャネルの再定義を考慮して、音声が新しい IP アドレスと UDP ポート

のペアに送信されるように、トラフィックを常にアプリケーション層に到達させる必要があります。そのため、補助的なサービスをサポートするには voice-fastpath を無効にする必要があります。

VPN IP アドレスを SoftPhone に設定する

Cisco IP SoftPhone を使用すると、PC を Cisco IP Phone 7900 シリーズの電話機のように使用できます。リモート ユーザが VPN を経由して自社のネットワークに接続し直す場合は、単方向音声の問題を回避するために、いくつかの追加設定を行う必要があります。

解決策は、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ことです。

確認

パケット フローを確認するには、コマンド **debug cch323 rtp** が便利です。このコマンドは、ルータが送信したパケット（X）と受信したパケット（R）を表示します。大文字は正常な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 *****
XXXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXrXrXrXrXr
XrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXrXrXrXrXr
XrXrXXrrrrrrrrrrrrrrr
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 *****
XXXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXrXrXrXrXrXr
XrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXrXrXrXrXrXr
XXrrrrrXrXrXrXrXrXrXrXrXrXrXrXrXrrXXrrXrXrXrXrXrXXXXXXXXXXXXXXXXrXXX
XXXXXrXrXrXXrrXr
XrXrXrXrXrXrXrXrXXrrrrrrrrrrrrrrrrrrrrrrrrrrrrr

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

*Mar 3 23:53:30.378: ****** cut through in BOTH direction *****
XRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRXRXRXRXRXR
XXRRXRXRXXRRXRXRXRXRXXRXRXRXRXRXRXRRXRXXRXRXRXRXRXRXRXRXRXRXRXRXRXRX
RXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXRXRX
RXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXR
XRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRR
RRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRXRXRXRXRXR
RXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXR
XXRRRRRRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRX
RXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXXRRRRXR

!-- End of conversation.
```

コーデックとリージョンの不一致

オフフックしたときにリオーダー音（話し中の音）が聞こえる場合は、リージョン間でコーデックが一致していないことが原因である可能性があります。コールの両端で少なくとも 1 つの共通のコーデック（たとえば、G.711）がサポートされていることを確認してください。共通のコーデックがサポートされていない場合は、トランスコーダーを使用する必要があります。

リージョンには、他の各リージョンとともに使用できる、サポートされているコーデックの種類が特定されています。すべてのデバイスは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 またはその他のサポートされている任意のコーデック（G.711、G.729、G.723 など、G.711 と同じかそれより小さい帯域幅を必要とするコーデック）を使用できることを意味しています。

（注）　各デバイス用にサポートされているコーデックを次に示します。
Cisco IP Phone 7960：G.711A-law/μ-law、G.729、G729A、G.729Annex-B
Cisco 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

ロケーションと帯域幅

番号をダイヤルした後にリオーダー音が聞こえる場合は、いずれかのコール終端デバイスのロケーションに対する Cisco CallManager の帯域割り当てが超過していることが原因である可能性があります。Cisco CallManager は、コールを発信する前に、各デバイスで使用できる帯域幅があるかどうかを確認します。使用可能な帯域幅がない場合、Cisco CallManager はコールを発信しないので、ユーザにはリオーダー音が聞こえます。

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

コールが確立されると、Cisco CallManager 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 が使用されている場合、Cisco CallManager は 80k を差し引きます。
- コールで G.723 が使用されている場合、Cisco CallManager は 24k を差し引きます。
- コールで G0.729 が使用されている場合、Cisco CallManager は 24k を差し引きます。

電話機の問題

この項では、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

症状

電話機がリセットされます。

考えられる原因

電話機の電源が切れて再投入されたり、電話機がリセットされたりする理由には、次の 2 つがあります。

- Cisco CallManager に接続する際に TCP エラーが発生した。
- 電話機の KeepAlive メッセージに対する確認応答を受信する際にエラーが発生した。

推奨処置

1. 電話機と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. www.cisco.com の Cisco Connection Online で、最新のソフトウェアのロード、新しいパッチ、または問題に関連するリリース ノートがあるかどうかを確認します。
3. 電話機のリセットに関するインスタンスがあるかどうかを Event Viewer で確認します。電話機のリセットは Information イベントに相当します。
4. 電話機がリセットされた時刻の前後に発生した可能性のあるエラーを探します。
5. SDI トレースを開始し、リセットが発生している電話機に共通する特徴を見極めて、問題を特定します。たとえば、それらの電話機がすべて同じサブネットに配置されているかどうか、あるいは、同じ VLAN に配置されているかどうかなどを確認します。トレースを調べて次の点を確認します。
   - リセットは通話中に発生するか、それとも断続的に発生するか。

- 電話機モデル（Cisco IP Phone 7960 または Cisco IP Phone 30VIP など）に類似性があるかどうか。

6. 頻繁にリセットが発生する電話機上で Sniffer トレースを開始します。電話機がリセットされた後にトレースを調べて、TCP リトライが行われているかどうかを確認します。行われている場合は、ネットワークに問題があることを示しています。トレースを実行すると、たとえば、電話機のリセットが 7 日に 1 回発生しているなど、リセットの規則性が見いだされる場合があります。このことから、DHCP リースの有効期限が 7 日に 1 回の周期に設定されている可能性があります（この値はユーザが設定できます。たとえば、2 分に 1 回にすることもできます）。

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異常終了します。

考えられる原因

ドロップされたコールが早期異常終了する場合は、電話機またはゲートウェイのリセットが原因である可能性があります（「電話機のリセット」を参照）。または、PRI 設定の誤りなど、回線の問題が原因である可能性もあります。

推奨処置

1. この問題を 1 台の電話機または 1 つの電話機グループに特定できるかどうかを確認します。影響を受けている電話機はすべて特定のサブネットまたはロケーションに配置されていることもあります。
2. 電話機またはゲートウェイのリセットを Event Viewer で確認します。

   リセットが発生する電話機ごとに、Warning メッセージと Error メッセージが 1 つずつ表示されます。これは、その電話機が Cisco CallManager への TCP 接続を維持できないために、Cisco CallManager が接続をリセットすることを示しています。このリセットは、電話機の電源をオフにしたため、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。この問題が断続的に発生しているときは、Microsoft Performance を使用して電話機登録を記録すると役立つ場合があります。

3. 特定のゲートウェイ（Cisco Access DT-24+ など）を経由した場合にだけ問題が発生していると考えられる場合は、トレースを有効にするか、Call Detail Record（CDR）を確認するか、あるいはその両方を行います。CDR ファイルには、問題の原因を判別するのに役立つ Cause of Termination（CoT）が含まれています。CDR の詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。
4. 接続解除の理由種別（コールを接続解除した側に応じて origCause_value および destCause_value）を見つけます。接続解除の理由種別は、次の場所にある Q.931 接続解除理由コード（10 進表記）に対応しています。

   http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/dbook/disdn.htm
5. コールがゲートウェイから出て PSTN に向かう場合は、CDR を使用して、どちらの側がコールを切断したかを判別できます。Cisco CallManager でトレースを有効にすることにより、ほぼ同じ情報を入手できます。トレース ツールは Cisco CallManager のパフォーマンスに影響を与える可能性があるので、最後の手段として使用するか、またはネットワークが稼働していないときに使用してください。

ゲートウェイの問題

この項では、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音

症状

リオーダー音が発生します。

考えられる原因

ゲートウェイを経由するコールを発信する場合、制限されているコールを発信したり、ブロックされている番号にダイヤルしたりすると、リオーダー音が聞こえることがあります。リオーダー音は、ダイヤルした番号が使用不可になっている場合、または PSTN の機器やサービスに問題がある場合に発生することがあります。

リオーダー音を発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、コールが正常にルーティングされることも確認してください。

推奨処置

ゲートウェイを経由する場合のリオーダー音のトラブルシューティングを行う手順を次に示します。

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. www.cisco.com の Cisco Connection Online で、最新のソフトウェアのロード、新しいパッチ、または問題に関連するリリース ノートがあるかどうかを確認します。
3. SDI トレースを開始し、問題を再現します。リオーダー音は、Cisco CallManager が許容可能なコール数を制限する、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する設定の問題が原因である可能性があります。SDI トレースでコールを特定して、ルート パターンやコール検索スペース（コーリング サーチ スペース）などの構成設定によってそのコールが意図的にブロックされたかどうかを判別します。

4. PSTN　を経由する場合もリオーダー音が発生することがあります。SDI トレースで Q.931 メッセージがないかどうか確認します。特に接続解除メッセージに注意します。Q.931 の接続解除メッセージがある場合、接続解除の原因は相手側にあり、こちら側でそれを解決することはできません。

ゲートウェイの登録障害

この項では、ゲートウェイの 2 つのカテゴリについて説明します。これらのカテゴリは類似していますが、同一ではありません。Cisco Access AS-X、AT-X、Cisco Access DT-24+、および DE-30+ は同じ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）に直接接続されていないスタンドアロン ユニットです。もう 1 つのカテゴリには、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 のシャーシに取り付けられたブレードとして、制御と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 CallManager に設定された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

登録が失敗するのは、さまざまな理由が考えられます。

推奨処置

1. まず、ゲートウェイが稼働していることを確認します。すべてのゲートウェイにはハートビート LED が付属しており、ゲートウェイ ソフトウェアが正常に稼働している場合は 1 秒間隔で点滅します。

   この LED がまったく点滅しない場合、または非常に速く点滅する場合、ゲートウェイ ソフトウェアは稼働していません。その結果、通常、ゲートウェイは自動的にリセットされます。また、約 2 ～ 3 分経過して登録プロセスを完了できない場合にも、通常、ゲートウェイは自動的にリセットされます。したがって、確認したときデバイスがたまたまリセット中である場合もありますが、10 ～ 15 秒後に通常の点滅パターンが示されない場合は、ゲートウェイに重大な障害があります。

Cisco Access Analog ゲートウェイでは、前面パネルの右端に緑色ハートビート LED があります。Cisco Access Digital ゲートウェイでは、カード上部の左端に赤色 LED があります。Cisco Analog Access WS-X6624 では、前面に近いカード右端にあるブレードの内部に緑色 LED があります（前面パネルからは見えません）。Digital Access WS-X6608 では、ブレード上の 8 スパンそれぞれに別個のハートビート LED があります。8 個の赤色 LED はカード上に並んでいます（前面パネルからは見えません）。これらの LED は、背面に向かって約 3 分の 2 進んだ位置にあります。

2. ゲートウェイが自分の IP アドレスを受信したことを確認します。スタンドアロン ゲートウェイは、自分の IP アドレスを DHCP または BOOTP を介して受信する必要があります。Catalyst ゲートウェイは、DHCP または BOOTP によって、あるいは NMP を介した手動設定によって自分の IP アドレスを受信できます。
3. DHCP　サーバに対するアクセス権を持っている場合、スタンドアロン ゲートウェイを調べる最善の方法は、デバイスに未解決の IP アドレス リースがある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、そのことは良い目安になりますが、決定的ではありません。DHCP サーバで、その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. 数分以内にゲートウェイがリースとともにサーバ上に再び表示される場合、この領域の動作はすべて正常です。表示されない場合は、ゲートウェイが DHCP サーバに接続できない（ルータの設定が誤っていないか、そのために DHCP ブロードキャストが転送されていないか、また、サーバが稼働しているかを確認してください）か、または、肯定応答を取得できない（IP アドレス プールがいっぱいになっていないかを確認してください）かのいずれかです。
6. これらのことを確認しても答えが得られない場合は、Sniffer トレースを使用して問題点を特定します。
7. Catalyst 6000 ゲートウェイの場合、NMP がゲートウェイと通信できることを確認する必要があります。これは、NMP からゲートウェイの内部 IP アドレスに対して ping を実行することで確認できます。

   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 が正常に実行された場合、**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 アドレス情報と TFTP IP アドレスが正しいことも確認してください。
9. ゲートウェイが有効な DHCP 情報の取得に失敗する場合は、Cisco TAC によって提供される tracy ユーティリティを使用して問題を特定します。
10. このユーティリティを TAC から入手したら、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、1 個の 860 プロセッサしか持っていないのでポート 1 です。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を次に示します。ただし、tracy コマンドの出力は、860 コンソール ポートの単なるリモート 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 メッセージがスクロールし続ける場合は、DHCP サーバへの接続に問題があります。

11. まず、Catalyst 6000 ゲートウェイ ポートが正しい VLAN 上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 上にない場合は、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。VLAN 番号が変わった後に、ゲートウェイは、リセットされるまで INIT 状態のままになっていることがあります。

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 をリセットするたびに tracy セッションは失われるので、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度確立する必要があります。

    tracy_close *mod port*

    tracy_start *mod port*

14. それでも **DHCPState = INIT** メッセージが表示される場合は、DHCP サーバが正常に機能しているかどうかを確認します。

15. 正常に機能している場合は、Sniffer 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 が正常に機能している場合、tracy デバッグ ユーティリティの使用を可能にする IP アドレスがゲートウェイに設定されています。このユーティリティには、Catalyst ゲートウェイ用の NMP コマンド セットの組み込み機能が含まれており、Windows 98/NT/2000 上でスタンドアロン ゲートウェイ用のヘルパー アプリケーションとして使用可能です。

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上で動作し、ゲートウェイごとに別個のトレース ウィンドウを表示します（一度にトレースできるのは最大 8 個）。トレースは指定したファイルに直接記録できます。

17. TFTP サーバの IP アドレスがゲートウェイに正しく指定されたことを確認します。DHCP は通常、Option 66（名前または IP アドレス）、Option 150（IP アドレスのみ）、または si_addr（IP アドレスのみ）で DHCP を提供します。サーバに複数の Option が設定されている場合、si_addr が Option 150 より優先され、Option 150 は Option 66 より優先されます。

    Option 66 が TFTP サーバの DNS_NAME を提供する場合、DNS サーバの IP アドレスは DHCP によって指定されている必要があります。また、Option 66 に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 を使用して DHCP が無効になるように 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、TFTP サーバのアドレスを含むすべての設定パラメータをコンソールから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 を介して名前 CiscoCM1 の解決を試行します。解決に成功すると、CiscoCM1 の IP アドレスは、DHCP サーバまたは NMP が TFTP サーバのアドレスとして示すどの情報よりも優先されます。これは、NMP が DHCP を無効にしている場合も同じです。

18. ゲートウェイにある現在の TFTP サーバの IP アドレスは、tracy ユーティリティを使用して確認できます。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 が含まれる行を探し、対応する番号を次の行（Cisco Access Digital gateway など）の taskID として使用します。この後の例では、説明対象のメッセージを判別しやすいように太字のテキスト行で示しています。実際の画面出力では、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. このコマンドによって、TFTP サーバの IP アドレスが表示されます。その IP アドレスが正しくない場合は、DHCP オプションと表示されたその他の情報が正しいことを確認します。

20. TFTP アドレスが正しい場合は、ゲートウェイが自分の設定ファイルを TFTP サーバから取得していることを確認します。tracy 出力で次の情報が表示される場合は、TFTP サービスが正常に機能していないか、ゲートウェイが Cisco CallManager に設定されていない可能性があります。

```
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ない場合、TFTP サーバと同じ IP アドレスに対する接続を試行します。クラスタ化された環境でなければ、これで接続できます。クラスタ化された環境では、ゲートウェイは冗長 Cisco CallManager のリストを受信する必要があります。

21. カードが自分の TFTP 情報を正常に取得していない場合は、Cisco CallManager の TFTP サービスを調べて、サービスが動作していることを確認してください。

22. Cisco CallManager の TFTP トレースを確認します。

ゲートウェイが Cisco CallManager に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。典型的なエラーは、ゲートウェイ用に誤った MAC アドレスを入力したことで発生します。その場合、Catalyst 6000 ゲートウェイでは、次のメッセージが 2 分間隔で NMP コンソールに表示されることがあります。

```
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 CCM 10.123.9.2
00:00:05.610 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState =
BackupCCM
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 CCM 10.123.9.2
00:00:20.600 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState =
BackupCCM
```

登録に関する別の問題としては、ロード情報が正しくないこと、またはロード ファイルが破損していることが考えられます。この問題は、TFTP サーバが稼働していない場合にも発生する可能性があります。この場合、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、正しいアプリケーション ロード名が A0020300 であるにもかかわらず、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 ロードがそれに対応する DSP ロードも取得する必要がある場合、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、類似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 CCM 10.123.9.2
00:00:05.730 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState =
BackupCCM
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 = BadCCM
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 CCM 10.123.9.2
00:01:51.300 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState =
BackupCCM
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: CCM#0 CPEvent = LOADID --> CPState =
LoadResponse
```

ここでの相違点は、ゲートウェイが LoadResponse の段階に留まっているために、最終的にはタイム アウトすることです。この問題は、Cisco CallManager Administration の Device Defaults エリアでロード ファイル名を修正することで解決できます。

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てください。IP 接続が存在する場合は、この項にある次の情報を参照してゲートキーパー コールのトラブルシューティングを行ってください。

- クラスタ間トランクまたは H.225 トランク
- アドミッション拒否
- 登録拒否

クラスタ間トランクまたは H.225 トランク

次の場所で、『*Cisco CallManager アドミニストレーション ガイド*』および『*Cisco CallManager システム ガイド*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/4_1/index.htm

アドミッション拒否

症状

Admission Reject（ARJ; アドミッション拒否）が発行されるのは、Cisco CallManager がゲートキーパーに登録されていてもコールを送信できない場合です。

考えられる原因

ゲートキーパーが ARJ を発行している場合は、特に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 CallManager からゲートキーパーへの IP 接続を確認します。
2. ゲートキーパのステータスを表示し、ゲートキーパーが動作していることを確認します。
3. ゲートキーパにゾーン サブネットが定義されていることを確認します。定義されている場合は、許可されたサブネットに Cisco CallManager のサブネットが含まれていることを確認します。

4. Cisco CallManager とゲートキーパー設定との間でテクノロジー プレフィッ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

Registration Reject（RRJ; 登録拒否）が発行されるのは、Cisco CallManager がゲートキーパーに登録できない場合です。

考えられる原因

ゲートキーパーが RRJ を発行している場合は、特に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 CallManager からゲートキーパーへの IP 接続を確認します。
2. ゲートキーパのステータスを表示し、ゲートキーパーが動作していることを確認します。
3. ゲートキーパにゾーン サブネットが定義されていることを確認します。定義されている場合は、許可されたサブネットにゲートウェイのサブネットが含まれていることを確認します。

Cisco CallManager が B チャネルをロックして Restart を送信する

この項では、次のトピックについて取り上げます。

チャネルの再起動

症状

Cisco CallManager が特に理由もなく B チャネルをロックし、そのチャネルに対して再起動を指示します。関連情報については、「Restart_Ack に Channel IE が含まれていない場合に B チャネルがロックされたままになる」を参照してください。

コールを発信すると、DSP がロックします。

（注）　Release 3.1(2c) Engineer Special 21 でこの問題は解決されています。

考えられる原因

ISDN チャネルの選択順序が原因でグレア状態が発生します。これは、大量のコールがある場合に発生することがあります。

また、発信コール用の B チャネルの選択は排他的です（Cisco CallManager は他の B チャネルを受け入れません）。チャネルが使用不可の場合、PABX または CO は Release Complete を送信します。

推奨処置

1. Cisco CallManager Administration から、**Device > Gateway** を選択します（図 6-2 を参照）。

図 6-2　Cisco CallManager Administration の Device メニュー

Find and List Gateways ウィンドウが表示されます。

2. 検索基準を入力して特定のゲートウェイを見つけます（図 6-3 を参照）。

図 6-3　Find and List Gateways ウィンドウ

3. **Find** をクリックします。

   検出されたデバイスのリストが表示されます。

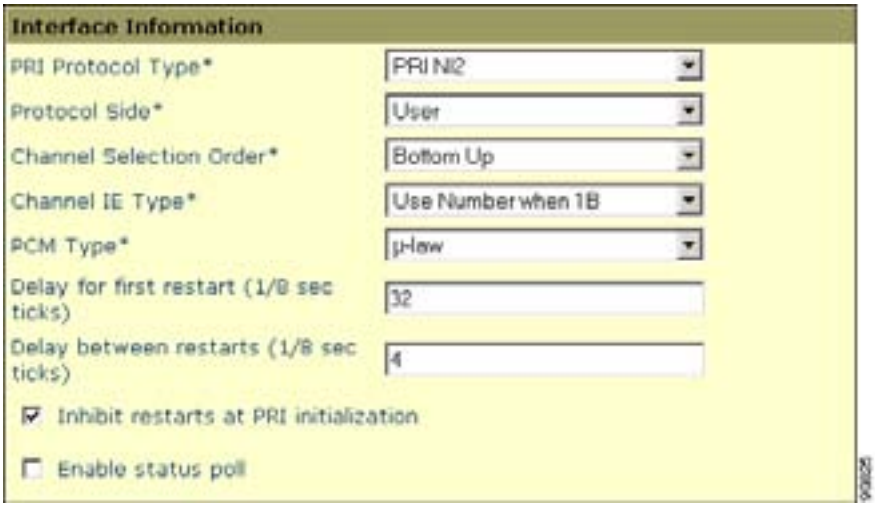
4. アップデートするゲートウェイの ***デバイス名***をクリックします。

   Gateway Configuration ウィンドウが表示されます。

5. ゲートウェイ ポートにアクセスするには、そのゲートウェイ ポートのアイコンクリックするか、または選択したゲートウェイの設定ウィンドウの左側にある MGCP エンドポイント リンクをクリックします。

6. **Inhibit Restarts at PRI initialization** チェックボックスをオンにします（図 6-4 を参照）。

図 6-4　Interface Information ウィンドウ



7. **Update** をクリックします。
8. ゲートウェイを再起動して変更内容を適用します。
9. Cisco CallManager サーバを再起動します。

（注）　再起動の問題を解決するには、**Inhibit Restarts at PRI Initialization** チェックボックスをオンにした後、Cisco CallManager サーバを再起動する必要があります。

E1/T1 PRI 設定の詳細については、『*Cisco CallManager アドミニストレーション ガイド*』を参照してください。

Restart_Ack に Channel IE が含まれていない場合に B チャネルがロックされたままになる

症状

この問題は、前述の問題「Cisco CallManager が B チャネルをロックして Restart を送信する」に関連しています。

Cisco CallManager システムは、ie=channel not available という理由付きの Release Complete を受信すると、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 内で、Channel IE を使用して、再起動する必要のあるチャネルを指定しています。ネットワークが Channel IE を含めずに Restart_Ack で応答した場合、システムはこのチャネルがロックされた状態を維持します。ネットワーク側では、この同じチャネルがアイドル状態に戻ります。

その結果、ネットワークは着信コール用にこのチャネルを要求することになります。

チャネルは Cisco CallManager サーバ上でロックされているので、Cisco CallManager はこのチャネルに対するコール要求をすべて解放します。

この動作は、ゲートウェイが E1 ブレードの場合、イギリスの多数のサイトで発生します（MGCP バックホールを 2600/3600 上で使用している場合も同じ動作が発生する可能性があります）。

グレア状態は、Release Complete が送信される理由であると考えられます。

これは大量のコールがあるサイトで頻繁に発生します。

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

B チャネルの選択が一定時間のラウンドロビンの場合、E1 ブレードのすべての B チャネルがロックされる結果になります。

推奨処置

E1 ポートをリセットします。

確認

B チャネルはアイドル状態に戻ります。

ダイヤル プランとルーティングの問題

この章では、ダイヤル プラン、ルート パーティション、およびコール検索スペース（コーリング サーチ スペース）で発生する可能性のある、次のような一般的な問題について説明します。

ルート パーティションとコール検索スペース

ルート パーティションは、Cisco CallManager ソフトウェアのエラー処理機能を継承します。つまり、情報メッセージとエラー メッセージをログに記録するために、コンソールおよび SDI ファイル トレースが提供されます。これらのメッセージは、トレースの番号分析コンポーネントの一部となります。問題の原因を特定するには、パーティションとコール検索スペースがどのように設定されているか、各パーティションおよびそのパーティションに関連付けられているコール検索スペースにどのようなデバイスがあるかを把握しておく必要があります。コール検索スペースにより、コールの発信にどの番号を使用できるかが決まります。パーティションにより、デバイスまたはルート リストへの許可されるコールが決まります。

詳細については、『*Cisco CallManager アドミニストレーション ガイド*』および『*Cisco CallManager システム ガイド*』のルート プランに関する章を参照してください。

次のトレースは、デバイスのコール検索スペース内にある番号がダイヤルされる例を示しています。SDI トレースの詳細については、本書のケース スタディを参照してください。

```
08:38:54.968 Cisco CallManager|StationInit - InboundStim -
OffHookMessageID tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|StationD - stationOutputDisplayText
tcpHandle=0x6b88028, Display= 5000
08:38:54.968 Cisco CallManager|StationD - stationOutputSetLamp stim:
9=Line instance=1 lampMode=LampOn tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|StationD - stationOutputCallState
tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|StationD -
stationOutputDisplayPromptStatus tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|StationD -
stationOutputActivateCallPlane tcpHandle=0x6b88028
08:38:54.968 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="")
```

上記のトレースの番号分析コンポーネントでは、コールを発信するデバイスの pss（パーティション検索スペース、コール検索スペースとも呼ばれる）が表示されています。

次のトレースにおいて、RTP_NC_Hardwood;RTP_NC_Woodland;Local_RTP は、このデバイスがコールできるパーティションを示しています。

```
08:38:54.968 Cisco CallManager|Digit analysis:
potentialMatches=PotentialMatchesExist
08:38:54.968 Cisco CallManager|StationD - stationOutputStartTone:
33=InsideDialTone tcpHandle=0x6b88028
08:38:55.671 Cisco CallManager|StationInit - InboundStim -
KeypadButtonMessageID kpButton: 5 tcpHandle=0x6b88028
08:38:55.671 Cisco CallManager|StationD - stationOutputStopTone
tcpHandle=0x6b88028
08:38:55.671 Cisco CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:55.671 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="5")
08:38:55.671 Cisco CallManager|Digit analysis:
potentialMatches=PotentialMatchesExist
08:38:56.015 Cisco CallManager|StationInit - InboundStim -
KeypadButtonMessageID kpButton: 0 tcpHandle=0x6b88028
08:38:56.015 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="50")
08:38:56.015 Cisco CallManager|Digit analysis:
potentialMatches=PotentialMatchesExist
08:38:56.187 Cisco CallManager|StationInit - InboundStim -
KeypadButtonMessageID kpButton: 0 tcpHandle=0x6b88028
08:38:56.187 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="500")
08:38:56.187 Cisco CallManager|Digit analysis:
potentialMatches=PotentialMatchesExist
08:38:56.515 Cisco CallManager|StationInit - InboundStim -
KeypadButtonMessageID kpButton: 3 tcpHandle=0x6b88028
08:38:56.515 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="5003")
08:38:56.515 Cisco CallManager|Digit analysis: analysis results
08:38:56.515 Cisco CallManager||PretransformCallingPartyNumber=5000
```

PotentialMatchesExist は、完全な一致が見つかり、それに従ってコールがルーティングされるまでの間にダイヤルされた番号に関する番号分析の結果であることに特に注意してください。

次のトレースは、Cisco CallManager が電話番号 1001 をダイヤルしようとしているときに、その番号がそのデバイスのコール検索スペースにない場合の処理を示しています。この場合も、最初の番号がダイヤルされるまでの間に番号分析ルーチンが一致の候補を処理していることに特に注意してください。番号 1 に関連付

けられているルート パターンは、デバイスのコール検索スペース RTP_NC_Hardwood;RTP_NC_Woodland;Local_RTP 以外のパーティションに存在します。したがって、電話機はリオーダー音（話し中の音）を受信します。

```
08:38:58.734 Cisco CallManager|StationInit - InboundStim -
OffHookMessageID tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD - stationOutputDisplayText
tcpHandle=0x6b88028, Display= 5000
08:38:58.734 Cisco CallManager|StationD - stationOutputSetLamp stim:
9=Line instance=1 lampMode=LampOn tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD - stationOutputCallState
tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD -
stationOutputDisplayPromptStatus tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|StationD -
stationOutputActivateCallPlane tcpHandle=0x6b88028
08:38:58.734 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="")
08:38:58.734 Cisco CallManager|Digit analysis:
potentialMatches=PotentialMatchesExist
08:38:58.734 Cisco CallManager|StationD - stationOutputStartTone:
33=InsideDialTone tcpHandle=0x6b88028
08:38:59.703 Cisco CallManager|StationInit - InboundStim -
KeypadButtonMessageID kpButton: 1 tcpHandle=0x6b88028
08:38:59.703 Cisco CallManager|StationD - stationOutputStopTone
tcpHandle=0x6b88028
08:38:59.703 Cisco CallManager|StationD - stationOutputSelectSoftKeys
tcpHandle=0x6b88028
08:38:59.703 Cisco CallManager|Digit analysis: match(fqcn="5000",
cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="1")
08:38:59.703 Cisco CallManager|Digit analysis:
potentialMatches=NoPotentialMatchesExist
08:38:59.703 Cisco CallManager|StationD - stationOutputStartTone:
37=ReorderTone tcpHandle=0x6b88028
```

ルート パーティションは、パーティション名をシステム内の各電話番号に関連付けることによって機能します。その電話番号をコールできるのは、コールの発信先として許可されているパーティションのリスト（パーティション検索スペース）内のパーティションが発信側のデバイスに含まれている場合だけです。この動作によって、きわめて強力にルーティングを制御できます。

コールが発信されると、番号分析により、パーティション検索スペースで指定されているパーティションだけで、ダイヤルされたアドレスの解決が試行されます。各パーティション名は、ダイヤル可能なグローバル アドレス スペースの個々のサブセットで構成されています。番号分析では、一覧表示されている各パーティションから、ダイヤルされた一連の番号と一致するパターンが取得されます。その後、番号分析では、一致するパターンの中から、一致度の最も高いものが選択されます。2 つのパターンで、ダイヤルされた一連の番号に対する一致度が等しい場合、番号分析では、パーティション検索スペースに最初に記載されているパーティションに関連付けられているパターンが選択されます。

グループ ピックアップ設定

症状

パーティションを設定されているグループで、グループ ピックアップ機能が動作しません。

考えられる原因

グループ内の各 Domain Name（DN; ドメイン名）の Calling Search Space（CSS; コール検索スペース）が、正しく設定されていない可能性があります。

例

次の手順は、パーティショニングがある場合の正しいグループ ピックアップ設定の例を示しています。

a. Marketing/5656 という名前のグループを設定します。ここで *Marketing* はパーティションで、*5656* はピックアップ番号です。

b. DN 6000 および 7000 の設定ページで、これらの DN をそれぞれ *Marketing/5656* という名前のピックアップ グループに追加します。

推奨処置

グループ ピックアップが失敗する場合は、各ドメイン名（この例では DN 6000 および 7000）の CSS を確認します。この例で、*Marketing* という名前のパーティションがそれぞれの CSS に含まれていない場合は、設定が誤っているためにピックアップが失敗した可能性があります。

ダイヤル プランの問題

この項では、次のようなダイヤル プランの問題について説明します。

番号をダイヤルするときの問題

症状

番号をダイヤルするときに問題が発生します。

考えられる原因

ダイヤル プランは、番号および番号グループのリストです。このリストは、特定の番号列が収集されるときに、コールの送信先となるデバイス（電話機やゲートウェイなど）を Cisco CallManager に知らせます。ダイヤル プランは、ルータのスタティック ルーティング テーブルに似ています。

ダイヤル プランに関連すると思われる問題のトラブルシューティングを行う前に、ダイヤル プランの概念、基本的なコール ルーティング、およびプランニングが入念に検討され正しく設定されていることを確認してください。多くの場合、プランニングと設定に問題があります。詳細については、『*Cisco CallManager アドミニストレーション ガイド*』のルート プランの設定に関する章を参照してください。

推奨処置

1. コールを発信している Directory Number（DN; 電話番号）を識別します。
2. その DN のコール検索スペースを識別します。

ヒント　コール検索スペースにより、コールの発信にどの番号を使用できるかが決まります。

3. 該当する場合、どのデバイスでコール検索スペースがこの DN に関連付けられているかを識別します。必ず正しいデバイスを識別してください。複数回線の着信表示がサポートされているため、複数のデバイスに同じ DN が設定されている場合があります。デバイスのコール検索スペースに注意してください。

   コールの発信元が Cisco IP Phone である場合は、特定の回線（DN）およびその回線が関連付けられているデバイスがコール検索スペースを持つことに注意してください。コールの発信時に、コール検索スペースが結合されます。たとえば、回線インスタンス 1000 がコール検索スペース AccessLevelX を持ち、内線番号が 1000 に設定されている Cisco IP Phone がコール検索スペース AccessLevelY を持つ場合、その回線からコールを発信すると、Cisco CallManager はコール検索スペース AccessLevelX と AccessLevelY に含まれるパーティションを検索します。

4. コール検索スペースに関連付けられているパーティションを識別します。

ヒント　パーティションにより、デバイスまたはルート リストへの許可されるコールが決まります。

5. デバイスのどのパーティションにコールが発信されるか（または発信されないか）を識別します。
6. ダイヤルされている番号を識別します。ユーザが 2 つ目の発信音を聞いたかどうか、聞いた場合はいつ聞いたかに注意します。すべての番号を入力した後にユーザには何が聞こえるか（リオーダー、速いビジー音）にも注意します。その前に、ユーザにプログレス トーンが聞こえるかどうかを確認します。発信者は、番号間タイマーが切れるのを待たなければならないことがあるため、最後の番号を入力してから少なくとも 10 秒間待つ必要があります。
7. Cisco CallManager Administration で Route Plan Report を生成し、そのレポートを使用して、問題のコールのコール検索スペース内にあるパーティションのすべてのルート パターンを調べます。
8. 必要に応じて、ルート パターンまたはルート フィルタを追加または変更します。
9. コールの送信先のルート パターンを検出できる場合は、そのパターンが指すルート リストまたはゲートウェイに注意します。

10. それがルート リストである場合、どのルート グループがそのリストに含まれているか、およびどのゲートウェイがそのルート グループに含まれているかを確認します。
11. 適切なデバイスが Cisco CallManager に登録されていることを確認します。
12. ゲートウェイが Cisco CallManager にアクセスできない場合は、show tech コマンドを使用して、その情報を取り込んで確認します。
13. @ 記号に注意します。このマクロは、多くの異なる機能を含むように展開できます。これは、多くの場合、フィルタリング オプションと組み合せて使用されます。
14. デバイスがパーティションに含まれていない場合、そのデバイスはヌル パーティションまたはデフォルト パーティションに含まれていると考えられます。すべてのユーザが、そのデバイスにコールできます。システムは、常に、ヌル パーティションを最後に検索します。
15. 9.@ パターンに一致する外線番号にダイヤルし、コールが通じるまでに 10 秒かかる場合は、フィルタリング オプションを確認します。デフォルトでは、9.@ パターンを使用する場合、7 桁の番号がダイヤルされると、Cisco IP Phone は 10 秒待ってからコールを発信します。LOCAL-AREA-CODE DOES-NOT- EXIST および END-OF-DIALING DOES-NOT-EXIST と表示されるパターンにルート フィルタを適用する必要があります。

安全なダイヤル プラン

ユーザ向けに安全なダイヤル プランを作成するように Cisco CallManager を設定するには、パーティションとコール検索スペースに加え、ルート パターン内の @ マクロ（North American Numbering Plan を意味する）のセクションに基づく一般的なフィルタリングを使用します。パーティションとコール検索スペースはセキュリティに不可欠であり、特に、マルチテナント環境や、個々のユーザ レベルの作成に役立ちます。コール検索スペースおよびパーティションの概念のサブセットであるフィルタリングにより、セキュリティ プランをさらに綿密にすることができます。

通常は、フィルタリングの問題を解決する手段として SDI トレースを実行することはお勧めできません。このトレースでは、十分な情報が得られないでけではなく、問題が悪化する可能性が非常に高くなります。

Cisco CallManager サービスの問題

この章では、Cisco CallManager サービスに関連する、次のような一般的な問題の解決方法について説明します。

使用可能な Conference Bridge がない

エラー メッセージ　No Conference Bridge Available

考えられる原因

これは、ソフトウェアまたはハードウェアのいずれかに問題があることを示している可能性があります。

推奨処置

1. Cisco CallManager に登録されている使用可能なソフトウェアまたはハードウェアの Conference Bridge リソースがあるかどうかを確認します。
2. Microsoft Performance または Admin Serviceability Tool のいずれかを使用して、Unicast AvailableConferences の数を確認します。

（注）　Cisco CallManager Release 3.1 では、カウンタとオブジェクトに対して異なる名前が使用されています。詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。

Cisco IP Voice Media Streaming アプリケーションは、Conference Bridge 機能を実行します。次のトレースに示されているように、Cisco IP Voice Media Streaming の 1 つのソフトウェア インストールは、16 個の Unicast Available Conferences（3 人 / 会議）をサポートします。

（注）　サポートされるデバイスの数は、Cisco CallManager のリリースによって異なる場合があります。http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_1/index.htm で、Release 3.1 のマニュアルを参照してください。

```
10:59:29.951 Cisco CallManager|UnicastBridgeControl -
wait_capabilities_StationCapRes - Device= CFB_kirribilli -
Registered - ConfBridges= 16, Streams= 48, tcpHandle=4f12738
10:59:29.951 Cisco CallManager|UnicastBridgeManager -
UnicastBridgeRegistrationReq - Device Registration Complete for
Name= Xoð ô%ð  - DeviceType= 50, ResourcesAvailable= 16,
deviceTblIndex= 0
```

次のトレースに示されているように、1 個の E1 ポート（WS-X6608-E1 カードには 8 個の E1 ポートがあります）は、5 個の Unicast Available Conferences（最大会議サイズ = 6）を提供します。

```
11:14:05.390 Cisco CallManager|UnicastBridgeControl -
wait_capabilities_StationCapRes - Device= CFB00107B000FB0 -
Registered - ConfBridges= 5, Streams= 16, tcpHandle=4f19d64
11:14:05.480 Cisco CallManager|UnicastBridgeManager -
UnicastBridgeRegistrationReq - Device Registration Complete for
Name= Xoð ô%ð  - DeviceType= 51, ResourcesAvailable= 5,
deviceTblIndex= 0
```

Cisco Catalyst 6000 8 Port Voice T1/E1 および Services Module の次のハードウェア トレースは、カードの E1 ポート 4/1 が Conference Bridge として Cisco CallManager に登録されていることを示しています。

```
greece-sup (enable) sh port 4/1
Port  Name               Status     Vlan       Duplex Speed
Type
----- ------------------ ---------- ---------- ------ -----
----------
 4/1                     enabled    1            full     -Conf
Bridge

Port      DHCP    MAC-Address       IP-Address      Subnet-Mask
--------- ------- ----------------- ---------------
---------------
 4/1      disable 00-10-7b-00-0f-b0 10.200.72.31
255.255.255.0

Port      Call-Manager(s)   DHCP-Server     TFTP-Server
Gateway
--------- ----------------- --------------- ---------------
-----------
 4/1    10.200.72.25     -            10.200.72.25   -

Port      DNS-Server(s)     Domain
--------- -----------------
-------------------------------------------
 4/1      -                 0.0.0.0

Port      CallManagerState DSP-Type
--------- ---------------- --------
4/1      registered       C549

Port  NoiseRegen NonLinearProcessing
----- ---------- -------------------
 4/1  disabled   disabled
```

3. Ad Hoc 会議または Meet-Me 会議に設定されている最大ユーザ数を調べて、この数を超過したために問題が発生したかどうかを確認します。

ハードウェア トランスコーダーが期待どおりに機能しない

症状

Cisco Catalyst 6000 8 Port Voice T1/E1 および Services Module にインストールしたハードウェア トランスコーダーが期待どおりに機能しません（共通のコーデックを持たない 2 人のユーザ間でコールを発信できません）。

考えられる原因

Cisco CallManager に登録された使用可能なトランスコーダー リソース（ハードウェア）がない可能性があります。

推奨処置

Microsoft Performance または Admin Serviceability Tool のいずれかを使用して、使用可能な MediaTermPointsAvailable の数を確認します。

（注）　Cisco CallManager Release 3.1 では、カウンタとオブジェクトに対して異なる名前が使用されています。詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。

次のトレースに示されているように、1 個の E1 ポート（WS-X6608-E1 カードには 8 個の E1 ポートがあります）は、16 件のコールに対応するトランスコーダー /MTP リソースを提供します。

（注）　サポートされるデバイスの数は、Cisco CallManager のリリースによって異なる場合があります。http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_1/index.htm で、Release 3.1 のマニュアルを参照してください。

```
11:51:09.939 Cisco CallManager|MediaTerminationPointControl -
Capabilities Received - Device= MTP00107B000FB1 - Registered -
Supports 16 calls
```

Cisco Catalyst 6000 8 Port Voice T1/E1 および Services Module の次のハードウェア トレースは、カードの E1 ポート 4/2 が MTP/ トランスコーダーとして Cisco CallManager に登録されていることを示しています。

```
greece-sup (enable) sh port 4/2
Port  Name               Status     Vlan       Duplex Speed Type
----- ------------------ ---------- ---------- ------ -----
----------
 4/2                     enabled    1            full     - MTP

Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- --------------- ---------------
 4/2     disable 00-10-7b-00-0f-b1 10.200.72.32    255.255.255.0

Port     Call-Manager(s)   DHCP-Server     TFTP-Server     Gateway
-------- ----------------- --------------- ---------------
-----------
 4/2    10.200.72.25      -             10.200.72.25    -

Port     DNS-Server(s)     Domain
-------- -----------------
-----------------------------------------
 4/2     -                 0.0.0.0

Port     CallManagerState DSP-Type
-------- ---------------- --------
 4/2     registered       C549

Port  NoiseRegen NonLinearProcessing
----- ---------- -------------------
 4/2  disabled   disabled
```

（注）　Conference Bridge と Transcoder/MTP の両方に同一の E1 ポートを設定することはできません。

ビット レートの低いコード（G.729 や G.723 など）を使用していて、同一のコーデックをサポートしていない 2 つのデバイス間でコールを発信するには、トランスコーダー リソースが必要です。

Region1 と Region2 間のコーデックが G.729 になるように Cisco CallManager が設定されていると仮定します。この場合、次のシナリオが該当します。

- Phone A で発信者がコールを開始すると、Cisco CallManager はその電話機が Cisco IP Phone 7960 であり、G.729 をサポートしていると認識します。番号が収集された後に、Cisco CallManager は、コールの宛先が Region2 にいる User D であると判別します。宛先デバイスも G.729 をサポートしているので、コールが確立され、音声が Phone A と Phone D 間を直接流れます。
- Cisco IP Phone 12SP+ の Phone B で発信者が Phone D に対するコールを開始した場合、Cisco CallManager は、発信側の電話機が G.723 または G.711 だけをサポートすると認識します。Phone B とトランスコーダー間は G.711 として、Phone D とトランスコーダー間は G.729 として、それぞれ音声が流れるように、Cisco CallManager はトランスコーディング リソースを割り当てる必要があります。使用可能なトランスコーダーがない場合、Phone D では呼び出し音が鳴りますが、そこで応答すると、そのコールはすぐに接続解除されます。
- Phone B で Cisco IP Phone 12SP+ の Phone F にコールを発信した場合は、そのリージョン間で使用されるコーデックとして G.729 が設定されていても、この 2 台の電話機は G.723 を使用します。G.723 が使用されるのは、両方のエンドポイントで G.723 がサポートされており、G.729 よりも小さい帯域幅を使用するためです。

確立されたコールで補助的なサービスが使用できない

症状

コールは確立されますが、補助的なサービスが使用できません。

考えられる原因

コールが確立されていても、H323v2 をサポートしない H.323 デバイスで補助的なサービスが使用できない場合は、MTP リソースの問題がトランスコーディングの問題の原因になっている可能性があります。

推奨処置

1. Cisco CallManager　に登録されている使用可能なソフトウェアまたはハードウェアの MTP リソースがあるかどうかを確認します。
2. Microsoft Performance または Admin Serviceability Tool のいずれかを使用して、MediaTermPointsAvailable の数を確認します。

（注）　Cisco CallManager Release 3.1 では、カウンタとオブジェクトに対して異なる名前が使用されています。詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。

次のトレースに示されているように、H.323v2 をサポートしない H.323 デバイスで MTP を使用して補助的なサービスをサポートすると、1 つの MTP ソフトウェア アプリケーションが 24 件のコールをサポートできます。

（注）　サポートされるデバイスの数は、Cisco CallManager　のリリースによって異なる場合があります。http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/3_1/index.htm で、Release 3.1 のマニュアルを参照してください。

```
10:12:19.161 Cisco CallManager|MediaTerminationPointControl -
Capabilities Received - Device= MTP_kirribilli. - Registered -
Supports 24 calls
```

次のトレースに示されているように、1 個の E1 ポート（WS-X6608-E1 カードには 8 個の E1 ポートがあります）は、16 件のコールに対応する MTP リソースを提供します。

```
11:51:09.939 Cisco CallManager|MediaTerminationPointControl -
Capabilities Received - Device= MTP00107B000FB1 - Registered -
Supports 16 calls
```

Cisco Catalyst 6000 8 Port Voice T1/E1 および Services Module の次のハードウェア トレースは、カードの E1 ポート 4/2 が MTP/ トランスコーダーとして Cisco CallManager に登録されていることを示しています。

```
greece-sup (enable) sh port 4/2
Port  Name               Status     Vlan       Duplex Speed
Type
----- ------------------ ---------- ---------- ------ -----
----------
 4/2                     enabled    1            full     - MTP

Port     DHCP    MAC-Address       IP-Address      Subnet-Mask
-------- ------- ----------------- ---------------
---------------
 4/2     disable 00-10-7b-00-0f-b1 10.200.72.32
255.255.255.0

Port     Call-Manager(s)   DHCP-Server     TFTP-Server
Gateway
-------- ----------------- --------------- ---------------
-----------
 4/2    10.200.72.25     -           10.200.72.25   -

Port     DNS-Server(s)     Domain
-------- ----------------
-----------------------------------------
 4/2     -                 0.0.0.0

Port     CallManagerState DSP-Type
-------- ---------------- --------
 4/2     registered       C549

Port  NoiseRegen NonLinearProcessing
----- ---------- -------------------
 4/2  disabled   disabled
```

3. Cisco CallManager Administration の Gateway Configuration 画面で、**Media Termination Point Required** チェックボックスがオンになっているかどうかを確認します。

4. Cisco CallManager が必要な数の MTP デバイスを割り当てていることを確認します。

■ 確立されたコールで補助的なサービスが使用できない

ボイス メッセージの問題

この章では、ボイス メッセージに関連する、次のような一般的な問題の解決方法について説明します。

- ボイス メッセージ
- Unity の問題

ボイス メッセージ

Cisco Unity ボイス メッセージに関する広範なトラブルユーティング情報については、次の URL で『*Cisco Unity トラブルシューティング ガイド*』を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity31/tsg/index.htm

Cisco Unity に関連するすべてのマニュアルについては、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/index.htm

Cisco Unity の日本語版マニュアルについては、次の URL を参照してください。

http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/index_uc_cu.shtml

30 秒経過するとボイス メッセージが停止する

症状

Cisco CallManager と連動して Cisco Unity 3.x を実行している場合に、ボイスメール メッセージを残すための時間が発信者に 30 秒しか与えられていません。

考えられる原因

この問題は、発信者がボイス メッセージを残そうとしているときに発生し、メッセージ開始から 30 秒でコールが強制終了されます。有効な内線番号または電話番号をダイヤルし、30 秒より長いボイス メッセージを残そうとすることで、これは簡単に再現できます。

推奨処置

1. この問題を解決するには、Media Gateway Control Protocol（MGCP; メディア ゲートウェイ コントロール プロトコル）が音声ゲートウェイで使用されていることを確認します。
2. MGCP が使用されている場合は、**no mgcp timer receive-rtcp** コマンドを追加します。
3. MGCP が音声ゲートウェイで使用されていない場合は、Cisco Unity サーバに対する Skinny トレースと Cisco CallManager トレースを有効にします。

Cisco Unity 3.x 以降で Skinny トレースを設定する方法の詳細については、次の URL で『Configuring Unity Traces with MaestroTools.exe』を参照してください。
http://www.cisco.com/warp/public/788/AVVID/unity_trace_maestrotools.html

Cisco Unity 3.1 以降は、MaestroTools に代わって Cisco Unity Diagnostic Tool が採用されています。このツールの使用方法の詳細については、次の URL で「Cisco Unity Diagnostic Tool」を参照してください。
http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity31/tsg/tsg31/tsg_0900.htm#xtocid13

Unity の問題

この項では、次のトピックについて取り上げます。

Unity がロール オーバーせずにビジー音が聞こえる

症状

Unity が最初の回線を通過せず、2 番目のポートにロール オーバーしません。

例

```
Call 5000 from 1001
Get Unity
Place the call on Hold
Press New Call
Dial 5000
Get Busy tone
Press End Call
Press Resume Call
Press End Call
```

考えられる原因

Messaging Interface が Unity と同じ番号（5000）で設定されており、代行受信を登録中であるため、コールが CMI にヒットしています。

推奨処置

CMI サービスのパラメータを調べて、voicemaildn が設定されていないことを確認します。

ボイス メッセージに転送されたコールが Unity に対する直接コールとして処理される

症状

Unity のバージョンは 2.4.5.135、TSP は 6.0(1)、Cisco CallManager は 3.1(31)spD です。

ある IP Phone から別の IP Phone へのコールがボイス メッセージに転送されると、そのコールは発信側の電話機から Unity への直接コールとして処理されます。ただし、これは番号がダイヤルされた場合に発生しますが、Redial ソフトキーが押された場合には正しく機能します（着信側電話機のグリーティングを受信します）。

考えられる原因

TSP のロジックでは、転送されたコールの場合、originalCalledPartyName が「Voicemail」のときは、そのコールは直接コールと見なされます。これは、Cisco CallManager を使用するフェールオーバー Unity システムのための動作です。

推奨処置

1. Cisco CallManager サーバで、Cisco Voice Mail ポートの Display フィールドの名前を「VoiceMail」以外のものに変更します。
2. Unity サーバで、HKLM\Software\ActiveVoice\AvSkinny\voiceMail display Name= *anything other than VoiceMail* という新しい Registry 文字列値を追加します。

管理者アカウントが Cisco Unity サブスクライバに関連付けられていない

症状

System Administrator（SA）ページにアクセスしようとしているとき、管理者アカウントが Unity サブスクライバに関連付けられていないというエラーが表示されます。

考えられる原因

ユーザにアクセス権が設定されていません。

推奨処置

1. SA ページに対する適切なアクセス権を取得するには、GrantUnityAccess ユーティリティを実行する必要があります。このツールは **C:\commserver\grantunityaccess.exe** にあります。

   （注） GrantUnityAccess ユーティリティの詳細については、次の URL で、「*Granting Administrative Rights to Other Cisco Unity Servers*」を参照してください。
   http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/unity31/sag/sag312/sag_0255.htm#xtocid8

2. オプションを選択せずにこのユーティリティを実行すると、使用説明が表示されます。このツールを通常の使用方法で実行すると、SA に対するアクセス権が付与されるアカウントのドメインまたはエイリアスが表示され、次に、それらのアクセス権のコピー元となるアカウントに関する情報が表示されます。

   たとえば、管理者アクセス権を付与する対象のユーザのエイリアスが TempAdministrator で、自分のドメイン名が MyDOMAIN の場合、DOS プロンプトで次のコマンドを使用します。
   GrantUnityAccess -u MyDOMAIN\TempAdministrator -s Installer -f.

   インストール担当者のアカウントには、常に管理者アクセス権を持つ特別なアカウントが指定されます。ただし、そのアカウントはディレクトリ自体には作成されず、SQL データベース専用のローカルなアカウントになります。

Cisco Unity 3.1.2 または 3.1.3 の録音メッセージにノイズがある

症状

この問題が発生するのは、Automatic Gain Control（AGC）のレジストリ設定値が誤っている場合だけです。一般に、誤った値には次のものがあります。

- AGCsamplesize が 16 進数 4e20（10 進数 20000）になっている。16 進数 1f40（10 進数 8000）にする必要があります。
- AGCgainthreshold が 16 進数 28（10 進数 40）になっている。16 進数 5（10 進数 5）にする必要があります。

考えられる原因

Cisco Unity 3.1.2 サーバの場合、AGC レジストリ設定が誤った値に設定されていることがあります。また、Cisco Unity 3.1.3 にアップグレードされたサーバの場合も、その可能性があります。これらの誤った設定が原因で、大きなホワイト ノイズが次の位置で発生する可能性があります。

- メッセージの冒頭
- メッセージの途中（メッセージの録音中にユーザが話すのを中断したとき）
- メッセージの末尾

推奨処置

レジストリ設定を正しい値に変更することで問題は解消します。詳細については、次の URL で Cisco Unity 製品のマニュアルを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_unity/index.htm

TAC への問い合せ

Cisco TAC へのお問い合せに際しては、問題点を識別して限定しやすくするために、予備情報をご提供いただく必要があります。問題の性質によっては、追加情報をご提供いただく場合もあります。お問い合せをした後に、エンジニアが求める次の情報を収集した場合には、必然的に解決が遅れます。

- 必要な予備情報
  - ネットワーク レイアウト
  - 問題の説明
  - 一般的な情報
- TAC Web
- CCO の利用
- 添付ファイル
- Cisco Live!
- リモート アクセス

必要な予備情報

すべての問題について、次の情報は必ず TAC に提供してください。TAC に問い合せを行う際に使用できるように、これらの情報を収集および保存しておき、変更については定期的に更新してください。

ネットワーク レイアウト

物理的な構成と論理な構成に関する詳細な説明、および音声ネットワークに関与する次のネットワーク要素（該当する場合）に関する詳細な説明です。

- Cisco CallManager
  - バージョン（Cisco CallManager Administration で **Details** を選択して確認します）
  - Cisco CallManager の数
  - 構成（スタンドアロン、クラスタ）
- Unity
  - バージョン（Cisco CallManager Administration で確認します）
  - 統合タイプ
- アプリケーション
  - インストールされているアプリケーションのリスト
  - 各アプリケーションのバージョン番号
- IP/ 音声ゲートウェイ
  - OS バージョン
  - Show tech（IOS ゲートウェイ）
  - Cisco CallManager ロード（Skinny ゲートウェイ）
- スイッチ
  - OS バージョン
  - VLAN 設定
- ダイヤル プラン：番号付け方式、コール ルーティング

可能な場合は、Visio またはその他の詳細な図（JPG など）を提出してください。Cisco Live! セッションで、ホワイトボードを使用して図を用意することもできます。

問題の説明

問題発生時にユーザが実行した操作を順序どおりに説明した詳細な情報を用意してください。その中には次の項目を含めてください。

- 予想した動作
- 実際の動作の詳細

一般的な情報

次の情報をすぐに提示できるようにしておいてください。

- 新しいバージョンをインストレールしているか。
- 古いバージョンの Cisco CallManager をインストールしている場合、この問題は当初から発生していたか（当初は発生していなかった場合、システムに対して最近どのような変更を行ったか）。
- この問題は再現可能か。
  - 再現可能な場合、それは通常の状況か、それとも特殊な状況か。
  - 再現不能な場合、問題が実際に発生した状況に関して何か特別な情報はあるか。
  - 問題が発生する頻度はどのくらいか。
- 影響を受けるデバイスは何か。
  - 特定の複数デバイスが影響を受ける場合（影響を受けるデバイスがいつも決まっている場合）、それらのデバイスに共通することは何か。
  - 問題に関与するすべてのデバイスの DN または IP アドレス（ゲートウェイの場合）。
- Call-Path 上にあるデバイスは何か（該当する場合）。

TAC Web

TAC Web（各種ツールや TAC エンジニアが作成した技術文書を豊富に収集したサイト）は、一般的な問題を分析し、解決方法を見いだすために使用します。TAC Web ツールとその使用方法を説明するコンテンツについては、次の URL を参照してください。

http://www.cisco.com/public/support/tac/home.shtml

CCO の利用

CCO を利用した問い合せは、その他のすべての方法に優先して取り扱われます。優先度の高い問い合せ（P1 および P2）は、この規則の例外となります。

CCO を利用して問い合わせを行う際は、問題を正確に記述する必要があります。その記述により、それに応じた解決方法を提供すると考えられる URL リンクが返されます。

問題の解決方法が見つからない場合は、その問い合せ内容を TAC エンジニアに送信するプロセスに進みます。

添付ファイル

問い合せ内容に添付するレポートは、電子メールでエンジニアに送信します。100 KB よりも大きい文書の場合は zip ファイルを添付します。

次の URL で、*Manage a TAC Case* セクションを使用してください。*please login* リンクを使用して、登録ユーザとしてログインします。

http://www.cisco.com/public/support/tac/contact.shtml

Cisco Live!

暗号化されたセキュアな Java アプレットである Cisco Live! では、Collaborative Web Browsing および URL 共有、ホワイトボード、Telnet、およびクリップボードの各ツールを利用することによって、Cisco TAC エンジニアと協力して、より効果的に作業を進めることができます。

Cisco Live! には、次の URL でアクセスします。

http://c3.cisco.com/

リモート アクセス

リモート アクセスにより、必要なすべての機器対して、Terminal Services（リモート ポート 3389）、HTTP（リモート ポート 80）、および Telnet（リモート ポート 23）の各セッションを確立できます。

注意　ダイヤルインを設定するときは、**login:cisco** および **password:cisco** を使用しないでください。これらは、システムに脆弱性をもたらす要因となります。

次のいずれかの方法により、デバイスに対するリモート アクセスを TAC エンジニアに許可することで、多くの問題を非常に迅速に解決できます。

- パブリック IP アドレスを持つ機器
- ダイヤルイン アクセス：（優先順位の高いものから）アナログ モデム、Integrated Services Digital Network（ISDN; サービス総合デジタルネットワーク）モデム、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）
- Network Address Translation（NAT; ネットワーク アドレス変換）：プライベート IP アドレスを持つ機器に対するアクセスを許可する IOS および Private Internet Exchange（PIX）

エンジニアの介入時にファイアウォールが IOS トラフィックおよび PIX トラフィック を遮断しないこと、および Terminal Services などの必要なすべてのサービスがサーバ上で起動していることを確認してください。

（注）　TAC は、すべてのアクセス情報の取り扱いに最大限の注意を払います。また、お客様の同意なしにシステムに変更を加えることはありません。

Cisco Secure Telnet

Cisco Secure Telnet を使用すると、Cisco Service Engineer（CSE; シスコ サービス エンジニア）は、ファイアウォールを介してお客様のサイトの Cisco CallManager サーバに透過的にアクセスできます。

Cisco Secure Telnet が機能するためには、シスコシステムズのファイアウォールの内側にある Telnet クライアントが、お客様のファイアウォールの内側にある Telnet デーモンに接続できるようにする必要があります。このセキュアな接続により、ファイアウォールを変更せずに、お客様の Cisco CallManager サーバの監視およびメンテナンスをリモートで行うことができます。

（注）　シスコは、必ずお客様の許可を得た上で、お客様のネットワークにアクセスします。作業を開始する場合は、お客様のサイトでネットワーク管理者のご協力をお願いしています。

ファイアウォール保護

ほぼすべての内部ネットワークでは、ファイアウォール アプリケーションを使用して、内部ホスト システムに対する外部アクセスを制限しています。これらのアプリケーションは、ネットワークとパブリック インターネット間の IP 接続を制限することで、ネットワークを保護しています。

ファイアウォールの機能は、外部で開始された TCP/IP 接続を許可するように設定が変更されない限り、そのような接続を自動的にブロックすることです。

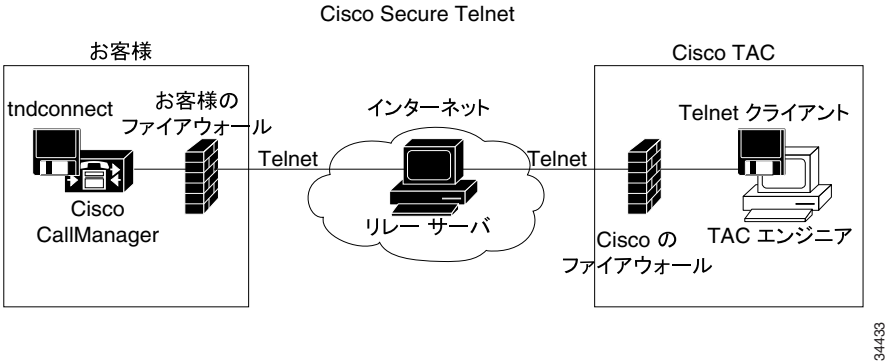
通常、企業ネットワークはパブリック インターネットとの通信を許可します。ただし、外部ホストへの接続がファイアウォールの内側で開始された場合に限ります。

Cisco Secure Telnet の設計

Cisco Secure Telnet では、Telnet 接続がファイアウォールの内側から簡単に開始できるという点を利用しています。外部のプロキシ マシンを使用して、システムはファイアウォールの内側から Cisco Technical Assistance Center（TAC）にある別のファイアウォールの内側のホストへ TCP/IP 通信をリレーします。

このリレー サーバを使用することで、保護されたリモート システム間のセキュアな通信がサポートされるとともに、両方のファイアウォールの整合性が維持されます。

図 A-1　Cisco Secure Telnet システム



Cisco Secure Telnet の構造

外部リレー サーバは Telnet トンネルを構築することにより、お客様のネットワークとシスコシステムズ間の接続を確立します。この処理によって、Cisco CallManager サーバの IP アドレスとパスワード識別情報を CSE に送信できるようになります。

（注）　パスワードは、お客様側の管理者と CSE が相互に同意したテキスト文字列で構成されます。

管理者は Telnet トンネルを起動してプロセスを開始します。この操作により、お客様側のファイアウォールの内側からパブリック インターネット上のリレー サーバへの TCP 接続が確立されます。その後、Telnet トンネルによって、お客様のローカル Telnet サーバへの別の接続が確立され、エンティティ間に双方向のリンクが作成されます。

（注）　Cisco TAC の Telnet クライアントは、Windows NT および Windows 2000 上のシステムまたは UNIX オペレーティング システムのもとで動作します。

お客様のサイトの Cisco CallManager がパスワードを受け入れた後、Cisco TAC で動作している Telnet クライアントは、お客様側のファイアウォールの内側で実行されている Telnet デーモンに接続します。その結果、透過的な接続が実現するので、ローカルでマシンを使用している場合と同様のアクセスが可能になります。

Telnet 接続が安定すると、CSE はすべてのリモート サービサビリティ機能を使用して、Cisco CallManager サーバに対してメンテナンス、診断、およびトラブルシューティングの各作業を実行できます。

CSE によって送信されたコマンドおよび Cisco CallManager サーバからの応答を表示することができますが、これらのコマンドおよび応答は必ずしも完全にフォーマットされているとは限りません。

その他の情報

詳細については、『*Cisco CallManager Serviceability アドミニストレーション ガイド*』を参照してください。

ケース スタディ：クラスタ内コール のトラブルシューティング

この付録のケース スタディでは、クラスタ内コールと呼ばれる、1 つのクラスタ内にある 2 台の Cisco IP Phone 間のコール フローについて詳細に説明します。また、このケース スタディでは、Cisco CallManager と Cisco IP Phone の初期化、登録、およびキープアライブの各プロセスについても取り上げます。クラスタ内コール フローに関する詳細な説明はその後に続きます。各プロセスの説明は、第 2 章「トラブルシューティング ツール」で取り上げているトレース ユーティリティおよびツールを使用して行われています。

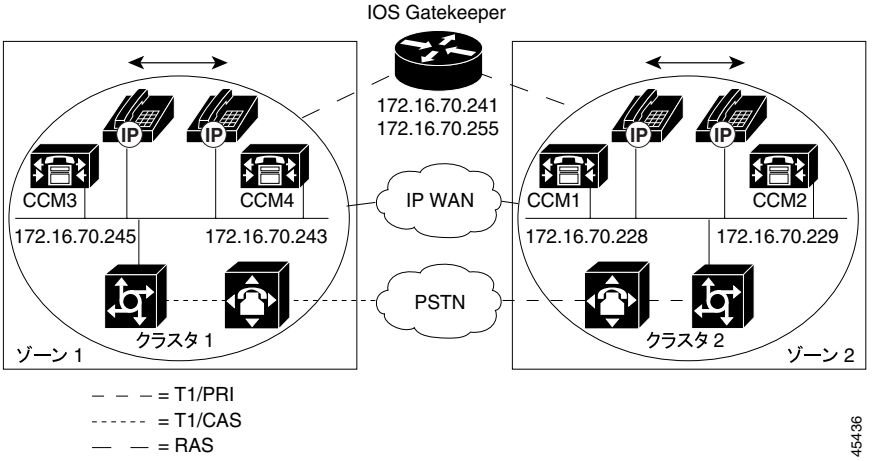
この章では、次のトピックについて取り上げます。

トポロジの例

Cluster 1 および Cluster 2 という 2 つのクラスタがあり、Cluster 1 には CCM3 および CCM4 という 2 つの Cisco CallManager 、Cluster 2 には CCM1 および CCM2 という 2 つの Cisco CallManager があると仮定します。

このケース スタディのトレースは、Cluster 2 にある CCM1 から収集されたものです（図 B-1 を参照）。コール フローのベースは、Cluster 2 にある 2 台の Cisco IP Phone です。これら 2 台の Cisco IP Phone の IP アドレスは、それぞれ、172.16.70.230（電話番号 1000）、172.16.70.231（電話番号 1001）です。

図 B-1　Cisco IP Phone と Cisco IP Phone 間のクラスタ内コールのトポロジの例



Cisco IP Phone の初期化プロセス

Cisco IP Phone の初期化（ブート アップ）プロセスの詳細な手順を次に示します。

手順

ステップ **1**　DHCP サーバで適切なオプション（Option 066、Option 150 など）が設定されていれば、Cisco IP Phone は初期化時に DHCP サーバに対して要求を送信し、IP アドレス、Domain Name System（DNS; ドメイン ネーム システム）サーバのアドレス、および TFTP サーバの名前またはアドレスを取得します。また、DHCP サーバで該当するオプション（Option 003）が設定されている場合は、デフォルト ゲートウェイのアドレスも取得します。

ステップ **2**　DHCP が TFTP サーバの DNS 名を送信する場合は、その名前を IP アドレスにマッピングするために DNS サーバの IP アドレスが必要になります。DHCP サーバが TFTP サーバの IP アドレスを送信する場合は、この手順を省略します。このケース スタディでは、DNS は設定されてないので、DHCP サーバは TFTP の IP アドレスを送信しました。

ステップ **3**　TFTP サーバ名が DHCP 応答に含まれていない場合、Cisco IP Phone はデフォルトのサーバ名を使用します。

ステップ **4**　設定ファイル（.cnf）は TFTP サーバから取得されます。すべての .cnf ファイルには、SEP<mac_address>.cnf という名前が付いています。この電話機を初めて Cisco CallManager に登録する場合は、デフォルト ファイルの SEPdefault.cnf が Cisco IP Phone にダウンロードされます。このケース スタディでは、1 台目の Cisco IP Phone は IP アドレス 172.16.70.230（MAC アドレスは SEP0010EB001720）、2 台目の Cisco IP Phone は IP アドレス 172.16.70.231（MAC アドレスは SEP003094C26105）をそれぞれ使用します。

ステップ **5**　すべての .cnf ファイルには、プライマリおよびセカンダリの Cisco CallManager の IP アドレスが含まれています。Cisco IP Phone は、この IP アドレスを使用してプライマリ Cisco CallManager に接続して登録します。

ステップ 6　Cisco IP Phone が Cisco CallManager に接続して登録すると、Cisco CallManager は、使用する実行ファイルのバージョン（ロード ID と呼ばれます）をその Cisco IP Phone に通知します。指定されたバージョンが Cisco IP Phone 上の実行ファイルのバージョンと一致しない場合、Cisco IP Phone は新しい実行ファイルのバージョンを TFTP サーバに要求し、自動的にリセットします。

Cisco CallManager の初期化プロセス

この項では、CCM1（IP アドレス 172.16.70.228 で識別される）から取り込んだトレースを使用して、Cisco CallManager の初期化プロセスについて説明します。前述のように、SDI トレースは、エンドポイント間で送信されたすべてのパケットに関する詳細情報を提供するので、非常に効果的なトラブルシューティング ツールです。

この項では、Cisco CallManager の初期化時に発生するイベントについて説明します。トレースの見方を理解していれば、Cisco CallManager の各プロセスのトラブルシューティング、およびそれらのプロセスがサービス（会議、転送など）に及ぼす影響のトラブルシューティングを適切に行うことができます。

次のメッセージは、Cisco CallManager SDI トレース ユーティリティから出力され、Cisco CallManager の 1 つ（このケース スタディでは CCM1）に対する初期化プロセスを示しています。

- 最初のメッセージは、Cisco CallManager が自分の初期化プロセスを開始したことを示しています。
- 2 番目のメッセージは、Cisco CallManager がデフォルト データベース（このケース スタディではプライマリ データベースまたはパブリッシャ データベース）の値を読み取ったことを示しています。
- 3 番目のメッセージは、Cisco CallManager が TCP ポート 8002 で各種メッセージを受信したことを示しています。
- 4 番目のメッセージは、それらのメッセージを受信した後に、Cisco CallManager が 2 つ目の Cisco CallManager（CCM2（172.16.70.229））を自分のリストに加えたことを示しています。
- 5 番目のメッセージは、Cisco CallManager が起動し、Cisco CallManager バージョン 3.1(1) を実行していることを示しています。

```
16:02:47.765 CCM|CMProcMon - CallManagerState Changed - Initialization
Started.
16:02:47.796 CCM|NodeId:  0, EventId: 107 EventClass: 3 EventInfo:
Cisco CM Database Defaults Read
16:02:49.937 CCM| SDL Info - NodeId: [1], Listen IP/Hostname:
[172.16.70.228], Listen Port: [8002]
16:02:49.984 CCM|dBProcs - Adding SdlLink to NodeId: [2], IP/Hostname:
[172.16.70.229]
16:02:51.031 CCM|NodeId:  1, EventId:  1 EventClass:  3 EventInfo:
Cisco CallManager Version=<3.1(1)> started
```

自己起動プロセス

Cisco CallManager は稼働状態になると、その内部で他のプロセスをいくつか起動します。それらのプロセスには、MulticastPoint Manager、UnicastBridge Manager、番号分析、ルート リストなどがあります。これらのプロセスの実行中に出力されるメッセージは、Cisco CallManager の機能に関連する問題のトラブルシューティングに非常に役立ちます。

たとえば、ルート リストが機能を停止して使用不可になっているとします。この問題のトラブルシューティングを行うには、これらのトレースを監視して、Cisco CallManager が RoutePlanManager をすでに起動したか、および RouteLists のロードを試行しているかを確認します。次に示す設定の例は、RouteListName="ipwan" および RouteGroupName="ipwan" がロードおよび起動していることを示しています。

```
16:02:51.031 CCM|MulicastPointManager - Started
16:02:51.031 CCM|UnicastBridgeManager - Started
16:02:51.031 CCM|MediaTerminationPointManager - Started
16:02:51.125 CCM|MediaCoordinator(1) - started
16:02:51.125 CCM|NodeId:    1, EventId: 1543 EventClass:  2 EventInfo:
Database manager started
16:02:51.234 CCM|NodeId:    1, EventId: 1542 EventClass:  2 EventInfo:
Link manager started
16:02:51.390 CCM|NodeId:    1, EventId: 1541 EventClass:  2 EventInfo:
Digit analysis started
16:02:51.406 CCM|RoutePlanManager - Started, loading RouteLists
16:02:51.562 CCM|RoutePlanManager - finished loading RouteLists
16:02:51.671 CCM|RoutePlanManager - finished loading RouteGroups
16:02:51.671 CCM|RoutePlanManager - Displaying Resulting RoutePlan
16:02:51.671 CCM|RoutePlanServer - RouteList Info, by RouteList and
RouteGroup Selection Order
16:02:51.671 CCM|RouteList - RouteListName=''ipwan''
16:02:51.671 CCM|RouteList - RouteGroupName=''ipwan''
16:02:51.671 CCM|RoutePlanServer - RouteGroup Info, by RouteGroup and
Device Selection Order
16:02:51.671 CCM|RouteGroup - RouteGroupName=''ipwan''
```

次のトレースは、RouteGroup がデバイス 172.16.70.245 を追加していることを示しています。このデバイスは Cluster 1 に配置された CCM3 で、H.323 デバイスであると見なされます。このケース スタディでは、RouteGroup は、Cisco IOS Gatekeeper の許可を得てコールを Cluster 1 の CCM3 にルーティングするために作成されています。Cluster 1 に配置された Cisco IP Phone へのコールのルーティ

ング中に問題が発生した場合、その原因を特定するには次のメッセージが役立ちます。

```
16:02:51.671 CCM|RouteGroup - DeviceName=''172.16.70.245''
16:02:51.671 CCM|RouteGroup -AllPorts
```

一部の初期化プロセスは、Cisco CallManager が「Dn」（電話番号）を追加していることを示しています。これらのメッセージを確認することで、Cisco CallManager がデータベースから電話番号を読み取ったかどうかを判別できます。

```
16:02:51.671 CCM|NodeId:    1, EventId: 1540 EventClass:  2 EventInfo:
Call control started
16:02:51.843 CCM|ProcessDb -        Dn = 2XXX,      Line = 0,
Display = ,  RouteThisPattern, NetworkLocation = OffNet,
DigitDiscardingInstruction = 1,   WhereClause =
16:02:51.859 CCM|Digit analysis: Add local pattern 2XXX , PID: 1,80,1
16:02:51.859 CCM|ForwardManager - Started
16:02:51.984 CCM|CallParkManager - Started
16:02:52.046 CCM|ConferenceManager - Started
```

次のトレースでは、Cisco CallManager の Device Manager が 2 つのデバイスを静的に初期化しています。IP アドレス 172.17.70.226 のデバイスはゲートキーパーを表し、IP アドレス 172.17.70.245 のデバイスは異なるクラスタにある別の Cisco CallManager を取得します。その Cisco CallManager は、H.323 Gateway としてこの Cisco CallManager に登録されます。

```
16:02:52.250 CCM|DeviceManager: Statically Initializing Device;
DeviceName=172.16.70.226
16:02:52.250 CCM|DeviceManager: Statically Initializing Device;
DeviceName=172.16.70.245
```

Cisco CallManager の登録プロセス

SDI トレースでは、登録プロセスも重要な要素です。デバイスは電源がオンになると、DHCP を介して情報を取得し、TFTP サーバに接続して自分の .cnf ファイルを取得し、その .cnf ファイルで指定されている Cisco CallManager に接続します。そのデバイスは、MGCP ゲートウェイ、Skinny ゲートウェイ、または Cisco IP Phone である可能性があります。したがって、Cisco AVVID ネットワークでデバイスが 正常に登録されたかどうかを検出できることが重要になります。

次のトレースでは、Cisco CallManager が登録のための新しい接続を受信しています。登録するデバイスは、MTP_nsa-cm1（CCM1 上の MTP サービス）および CFB_nsa-cm1（CCM1 上の Conference Bridge サービス）です。これらは Cisco CallManager で動作しているソフトウェア サービスですが、内部的には異なる外部サービスとして扱われるため、TCPHandle、ソケット番号、ポート番号、およびデバイス名が割り当てられます。

```
16:02:52.750 CCM|StationInit - New connection accepted. DeviceName=,
TCPHandle=0x4fbaa00, Socket=0x594, IPAddr=172.16.70.228, Port=3279,
StationD=[0,0,0]
16:02:52.750 CCM|StationInit - New connection accepted. DeviceName=,
TCPHandle=0x4fe05e8, Socket=0x59c, IPAddr=172.16.70.228, Port=3280,
StationD=[0,0,0]
16:02:52.781 CCM|StationInit - Processing StationReg. regCount: 1
DeviceName=MTP_nsa-cm1, TCPHandle=0x4fbaa00, Socket=0x594,
IPAddr=172.16.70.228, Port=3279, StationD=[1,45,2]
16:02:52.781 CCM|StationInit - Processing StationReg. regCount: 1
DeviceName=CFB_nsa-cm1, TCPHandle=0x4fe05e8, Socket=0x59c,
IPAddr=172.16.70.228, Port=3280, StationD=[1,96,2]
```

Cisco CallManager の KeepAlive プロセス

ステーション、デバイス、またはサービスと Cisco CallManager は、それらの相互間の通信チャネルに関する情報を保持するために次のメッセージを使用します。このメッセージは、Cisco CallManager とステーション間の通信リンクがアクティブ状態を維持するための KeepAlive シーケンスを開始します。次のメッセージは、Cisco CallManager とステーションのどちらからでも発信できます。

```
16:03:02.328 CCM|StationInit - InboundStim - KeepAliveMessage -
Forward KeepAlive to StationD. DeviceName=MTP_nsa-cm2,
TCPHandle=0x4fa7dc0, Socket=0x568, IPAddr=172.16.70.229, Port=1556,
StationD=[1,45,1]
16:03:02.328 CCM|StationInit - InboundStim - KeepAliveMessage -
Forward KeepAlive to StationD. DeviceName=CFB_nsa-cm2,
TCPHandle=0x4bf8a70, Socket=0x57c, IPAddr=172.16.70.229, Port=1557,
StationD=[1,96,1]
16:03:06.640 CCM|StationInit - InboundStim - KeepAliveMessage -
Forward KeepAlive to StationD. DeviceName=SEP0010EB001720,
TCPHandle=0x4fbb150, Socket=0x600, IPAddr=172.16.70.230, Port=49211,
StationD=[1,85,2]
16:03:06.703 CCM|StationInit - InboundStim - KeepAliveMessage -
Forward KeepAlive to StationD. DeviceName=SEP003094C26105,
TCPHandle=0x4fbbc30, Socket=0x5a4, IPAddr=172.16.70.231, Port=52095,
StationD=[1,85,1]
```

次のトレースに含まれるメッセージは、Cisco CallManager とステーション間の通信リンクがアクティブであることを示す KeepAlive シーケンスを表しています。これらのメッセージも、Cisco CallManager とステーションのどちらからでも発信できます。

```
16:03:02.328 CCM|MediaTerminationPointControl -
stationOutputKeepAliveAck tcpHandle=4fa7dc0
16:03:02.328 CCM|UnicastBridgeControl - stationOutputKeepAliveAck
tcpHandle=4bf8a70
16:03:06.703 CCM|StationInit - InboundStim - IpPortMessageID:
32715(0x7fcb) tcpHandle=0x4fbbc30
16:03:06.703 CCM|StationD - stationOutputKeepAliveAck
tcpHandle=0x4fbbc30
```

Cisco CallManager のクラスタ内コール フローのトレース

この項の SDI トレースは、クラスタ内コール フローの詳細を示しています。コール フローの Cisco IP Phone は、電話番号（dn）、tcpHandle、および IP アドレスで識別できます。Cluster 2 に配置された Cisco IP Phone（dn：1001、tcpHandle：0x4fbbc30、IP アドレス：172.16.70.231）は、同一クラスタ内の別の Cisco IP Phone（dn：1000、tcpHandle：0x4fbb150、IP アドレス：172.16.70.230）にコールを発信しています。TCP ハンドル値、タイム スタンプ、またはデバイスの名前を調べることで、デバイスをトレース上で追跡できます。デバイスをリブートするかオフラインにするまで、デバイスの TCP ハンドル値は変わりません。

次のトレースは、Cisco IP Phone（1001）がオフフックになっていることを示しています。下記のトレースは、一意のメッセージ、TCP ハンドル、および着信側の番号を示しています。これらは Cisco IP Phone に表示されます。この時点では、まだユーザが番号をダイヤルしていないので、発信側の番号は表示されていません。下記の情報は、Cisco IP Phone と Cisco CallManager 間の Skinny Station メッセージの形式で表示されます。

```
16:05:41.625 CCM|StationInit - InboundStim - OffHookMessageID
tcpHandle=0x4fbbc30
16:05:41.625 CCM|StationD - stationOutputDisplayText
tcpHandle=0x4fbbc30, Display= 1001
```

次のトレースは、Cisco CallManager から Cisco IP Phone に発信された Skinny Station メッセージを示しています。最初のメッセージは、発信側の Cisco IP Phone のランプをオンにします。

```
16:05:41.625 CCM|StationD - stationOutputSetLamp stim: 9=Line
instance=1 lampMode=LampOn tcpHandle=0x4fbbc30
```

Cisco CallManager は、stationOutputCallState メッセージを使用して、特定のコールに関する情報をステーションに通知します。

```
16:05:41.625 CCM|StationD - stationOutputCallState tcpHandle=0x4fbbc30
```

Cisco CallManager は、stationOutputDisplayPromptStatus メッセージを使用して、コールに関するプロンプト メッセージを Cisco IP Phone に表示します。

```
16:05:41.625 CCM|StationD - stationOutputDisplayPromptStatus
tcpHandle=0x4fbbc30
```

Cisco CallManager は、stationOutputSelectSoftKey メッセージを使用して、Skinny Station で特定のソフトキーのセットを選択します。

```
16:05:41.625 CCM|StationD - stationOutputSelectSoftKeys
tcpHandle=0x4fbbc30
```

Cisco CallManager は、次のメッセージを使用して、表示用の正確な回線コンテキストについて Skinny Station に指示します。

```
16:05:41.625 CCM|StationD - stationOutputActivateCallPlane
tcpHandle=0x4fbbc30
```

次のメッセージでは、番号分析プロセスによって、着信番号の識別、およびデータベース内にルーティングの一致があるかどうかの確認ができる状態になっています。エントリ cn=1001 は発信側の番号を表しています。dd="" はダイヤルされた番号であり、着信側の番号を示してます。電話機が StationInit メッセージを送信し、Cisco CallManager が StationD メッセージを送信した後に、Cisco CallManager は番号分析を実行します。

```
16:05:41.625 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="")
16:05:41.625 CCM|Digit analysis:
potentialMatches=PotentialMatchesExist
```

次のデバッグ メッセージは、Cisco CallManager が発信側の Cisco IP Phone に内部発信音を鳴らしていることを示しています。

```
16:05:41.625 CCM|StationD - stationOutputStartTone: 33=InsideDialTone
tcpHandle=0x4fbbc30
```

Cisco CallManager は着信メッセージを検出し、Cisco IP Phone のキーパッド ボタン 1 が押されたことを認識すると、ただちに出力トーンを停止します。

```
16:05:42.890 CCM|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 1 tcpHandle=0x4fbbc30
16:05:42.890 CCM|StationD - stationOutputStopTone tcpHandle=0x4fbbc30
16:05:42.890 CCM|StationD - stationOutputSelectSoftKeys
tcpHandle=0x4fbbc30
16:05:42.890 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="1")
16:05:42.890 CCM|Digit analysis:
potentialMatches=PotentialMatchesExist
16:05:43.203 CCM|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 0 tcpHandle=0x4fbbc30
16:05:43.203 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="10")
16:05:43.203 CCM|Digit analysis:
potentialMatches=PotentialMatchesExist
16:05:43.406 CCM|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 0 tcpHandle=0x4fbbc30
16:05:43.406 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="100")
16:05:43.406 CCM|Digit analysis:
potentialMatches=PotentialMatchesExist
16:05:43.562 CCM|StationInit - InboundStim - KeypadButtonMessageID
kpButton: 0 tcpHandle=0x4fbbc30
16:05:43.562 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="1000")
```

Cisco CallManager は、一致していると判別できるだけの番号を受信すると、番号分析の結果をテーブル形式で表示します。一致するものがすでに見つかっているので、Cisco CallManager は、それ以降に電話機で押された番号をすべて無視します。

```
16:05:43.562 CCM|Digit analysis: analysis results
16:05:43.562 CCM||PretransformCallingPartyNumber=1001
|CallingPartyNumber=1001
|DialingPattern=1000
|DialingRoutePatternRegularExpression=(1000)
|PotentialMatches=PotentialMatchesExist
|DialingSdlProcessId=(1,38,2)
|PretransformDigitString=1000
|PretransformPositionalMatchList=1000
|CollectedDigits=1000
|PositionalMatchList=1000
|RouteBlockFlag=RouteThisPattern
```

次のトレースは、Cisco CallManager がこの情報を着信側の電話機に送信していることを示しています（電話機は tcpHandle 番号で識別されます）。

```
16:05:43.578 CCM|StationD - stationOutputCallInfo
CallingPartyName=1001,  CallingParty=1001, CalledPartyName=1000,
CalledParty=1000, tcpHandle=0x4fbb150
```

次のトレースは、Cisco CallManager が、着信側の Cisco IP Phone にある着信コール用ランプを点滅するように指示していることを示しています。

```
16:05:43.578 CCM|StationD - stationOutputSetLamp stim: 9=Line
instance=1 lampMode=LampBlink tcpHandle=0x4fbb150
```

次のトレースは、Cisco CallManager が、呼び出し音や表示通知などのコール関連の情報を着信側の Cisco IP Phone に提供しています。ここでも、トレース全体を通して同じ tcpHandle が使用されているので、すべてのメッセージが同じ Cisco IP Phone に送信されていることを確認できます。

```
16:05:43.578 CCM|StationD - stationOutputSetRinger: 2=InsideRing
tcpHandle=0x4fbb150
16:05:43.578 CCM|StationD - stationOutputDisplayNotify
tcpHandle=0x4fbb150
16:05:43.578 CCM|StationD - stationOutputDisplayPromptStatus
tcpHandle=0x4fbb150
16:05:43.578 CCM|StationD - stationOutputSelectSoftKeys
tcpHandle=0x4fbb150
```

Cisco CallManager が発信側の Cisco IP Phone にも同様の情報を提供していることに注意してください。ここでも、Cisco IP Phone は tcpHandle によって識別されます。

```
16:05:43.578 CCM|StationD - stationOutputCallInfo
CallingPartyName=1001,  CallingParty=1001, CalledPartyName=,
CalledParty=1000, tcpHandle=0x4fbbc30
16:05:43.578 CCM|StationD - stationOutputCallInfo
CallingPartyName=1001,  CallingParty=1001, CalledPartyName=1000,
CalledParty=1000, tcpHandle=0x4fbbc30
```

次のトレースでは、Cisco CallManager がアラート音または呼び出し音を発信側の Cisco IP Phone で鳴らし、接続が確立されたことを通知しています。

```
16:05:43.578 CCM|StationD - stationOutputStartTone: 36=AlertingTone
tcpHandle=0x4fbbc30
16:05:43.578 CCM|StationD - stationOutputCallState tcpHandle=0x4fbbc30
16:05:43.578 CCM|StationD - stationOutputSelectSoftKeys
tcpHandle=0x4fbbc30
16:05:43.578 CCM|StationD - stationOutputDisplayPromptStatus
tcpHandle=0x4fbbc30
```

この時点で、着信側の Cisco IP Phone はオフフックになるので、Cisco CallManager は発信側で呼び出し音を鳴らすのを停止します。

```
16:05:45.140 CCM|StationD - stationOutputStopTone tcpHandle=0x4fbbc30
```

次のメッセージでは、Cisco CallManager が Skinny Station に Unicast RTP ストリームの受信を開始するように指示しています。そのために、Cisco CallManager は着信側の IP アドレス、コーデック情報、およびパケット サイズ（ミリ秒）を提供します。PacketSize は、RTP パケットの作成に使用されるサンプリング時間（ミリ秒）の整数です。

（注）　通常、この値は 30 ミリ秒に設定されます。このケース スタディでは、20 ミリ秒に設定されています。

```
16:05:45.140 CCM|StationD - stationOutputOpenReceiveChannel
tcpHandle=0x4fbbc30 myIP: e74610ac (172.16.70.231)
16:05:45.140 CCM|StationD - ConferenceID: 0 msecPacketSize: 20
compressionType:(4)Media_Payload_G711Ulaw64k
```

同様に、Cisco CallManager は着信側（1000）に情報を提供します。

```
16:05:45.140 CCM|StationD - stationOutputOpenReceiveChannel
tcpHandle=0x4fbb150 myIP: e64610ac (172.16.70.230)
16:05:45.140 CCM|StationD - ConferenceID: 0 msecPacketSize: 20
compressionType:(4)Media_Payload_G711Ulaw64k
```

Cisco CallManager は、RTP ストリーム用のオープン チャネルを確立するために、着信側から確認応答メッセージを受信します。また、着信側の IP アドレスも受信します。このメッセージにより、Skinny Station に関する 2 種類の情報が Cisco CallManager に通知されます。1 つは、オープン アクションのステータスです。もう 1 つは、リモート エンドへの伝送に使用する受信ポートのアドレスと番号です。RTP ストリームのトランスミッタ（発信側）の IP アドレスは ipAddr で、PortNumber は RTP ストリーム トランスミッタ（発信側）の IP ポート番号です。

```
16:05:45.265 CCM|StationInit - InboundStim -
StationOpenReceiveChannelAckID tcpHandle=0x4fbb150, Status=0,
IpAddr=0xe64610ac, Port=17054, PartyID=2
```

Cisco CallManager は、次のメッセージを使用して、指定のリモート Cisco IP Phone の IP アドレスとポート番号に音声およびビデオ ストリームの伝送を開始するようにステーションに指示しています。

```
16:05:45.265 CCM|StationD - stationOutputStartMediaTransmission
tcpHandle=0x4fbbc30 myIP: e74610ac (172.16.70.231)
16:05:45.265 CCM|StationD - RemoteIpAddr: e64610ac (172.16.70.230)
RemoteRtpPortNumber: 17054 msecPacketSize: 20
compressionType:(4)Media_Payload_G711Ulaw64k

16:03:25.328 CCM|StationD(1):   TCPPid=[1.100.117.1]
OpenMultiReceiveChannel conferenceID=16777217 passThruPartyID=1000011
compressionType=101(Media_Payload_H263) qualifierIn=?.   myIP:
e98e6b80 (128.107.142.233)|<CT::1,100,11,1.1><IP::><DEV::>

16:03:25.375 CCM|StationInit: TCPPid=[1.100.117.1]
StationOpenMultiMediaReceiveChannelAck Status=0, IpAddr=0xe98e6b80,
Port=65346,
PartyID=16777233|<CT::1,100,105,1.215><IP::128.107.142.233>

16:03:25.375 CCM|StationD(2):   TCPPid = [1.100.117.2]
star_StationOutputStartMultiMediaTransmission conferenceID=16777218
passThruPartyID=16777250 remoteIpAddress=e98e6b80(66.255.0.0)
remotePortNumber=65346 compressType=101(Media_Payload_H263)
qualifierOut=?. myIP: e98e6b80
(128.107.142.233)|<CT::1,100,105,1.215><IP::128.107.142.233>
```

次のトレースでは、前述のメッセージが着信側に送信されています。RTP メディア ストリームが着信側と発信側の間で開始されたことを示すメッセージが、これらのメッセージの後に続きます。

```
16:05:45.312 CCM|StationD - stationOutputStartMediaTransmission
tcpHandle=0x4fbb150 myIP: e64610ac (172.16.70.230)
16:05:45.328 CCM|StationD - RemoteIpAddr: e74610ac (172.16.70.231)
RemoteRtpPortNumber: 18448 msecPacketSize: 20
compressionType:(4)Media_Payload_G711Ulaw64k
16:05:46.203 CCM|StationInit - InboundStim - OnHookMessageID
tcpHandle=0x4fbbc30
```

最後に、発信側の Cisco IP Phone がオンフックになります。そのため、Skinny Station と Cisco CallManager 間のすべての制御メッセージ、および Skinny Station 間の RTP ストリームが終了します。

```
16:05:46.203 CCM|StationInit - InboundStim - OnHookMessageID
tcpHandle=0x4fbbc30
```

ケース スタディ：Cisco IP Phone と Cisco IOS Gateway 間のコールのトラブルシューティング

付録 B「ケース スタディ：クラスタ内コール のトラブルシューティング」のケース スタディでは、クラスタ内コールのコール フローについて説明しました。この付録のケース スタディでは、ローカル PBX または Public Switched Telephone Network（PSTN; 公衆電話交換網）に接続された電話機に Cisco IOS Gateway を介してコールを発信する Cisco IP Phone について説明します。概念的には、コールが Cisco IOS Gateway に到達すると、ゲートウェイはそのコールを FXS ポートまたは PBX に接続された電話機のどちらかに転送します。コールが PBX に転送された場合、そのコールはローカル PBX に接続された電話機で終端するか、PBX によって PSTN に転送されて PSTN 上のどこかで終端します。

この章では、次のトピックについて取り上げます。

- コール フロー トレース
- Cisco IOS Gatekeeper のデバッグ メッセージと表示コマンド
- Cisco IOS Gateway のデバッグ メッセージと表示コマンド
- T1/PRI インターフェイスを使用する Cisco IOS Gateway
- T1/CAS インターフェイスを使用する Cisco IOS Gateway

コール フロー トレース

この項では、Cisco CallManager トレース ファイル CCM000000000 の例を使用して、コール フローについて説明します。付録 B「ケース スタディ：クラスタ内コール のトラブルシューティング」で詳細なトレース情報（初期化、登録、KeepAlive のメカニズムなど）についてはすでに説明したので、このケース スタディのトレースでは、コール フロー自体に焦点を絞っています。

このコール フローでは、Cluster 2 に配置された Cisco IP Phone（電話番号 1001）が、PSTN に配置された電話機（電話番号 3333）にコールを発信しています。TCP ハンドル値、タイム スタンプ、またはデバイスの名前を調べることで、デバイスをトレース上で追跡できます。デバイスをリブートするかオフラインにするまで、デバイスの TCP ハンドル値は変わりません。

次のトレースでは、Cisco IP Phone（1001）はオフフックになっています。このトレースは、一意のメッセージ、TCP ハンドル、および発信側の番号を示しています。これらは Cisco IP Phone に表示されます。この時点では、まだユーザが番号をダイヤルしていないので、着信側の番号は表示されていません。

```
16:05:46.37515:20:18.390 CCM|StationInit - InboundStim -
OffHookMessageID tcpHandle=0x5138d98

15:20:18.390 CCM|StationD - stationOutputDisplayText
tcpHandle=0x5138d98, Display=1001
```

次のトレースでは、ユーザが DN 3333 をダイヤルしています（数字を 1 つずつダイヤルしています）。3333 という番号は電話機の宛先番号であり、この電話機は PSTN ネットワークに配置されています。Cisco CallManager の番号分析プロセスは現在アクティブになっていて、コールのルーティング先を検出するために番号を分析しています。番号分析については、付録 B「ケース スタディ：クラスタ内コール のトラブルシューティング」で詳細に説明しています。

```
15:20:18.390 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="")
15:20:19.703 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="3")
15:20:20.078 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="33")
15:20:20.718 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="333")
15:20:21.421 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="3333")
15:20:21.421 CCM|Digit analysis: analysis results
```

次のトレースでは、番号分析が完了して発信側と着信側が一致し、情報の解析が完了しています。

```
|CallingPartyNumber=1001
|DialingPattern=3333
|DialingRoutePatternRegularExpression=(3333)
|PretransformDigitString=3333
|PretransformPositionalMatchList=3333
|CollectedDigits=3333
|PositionalMatchList=3333
```

次のトレースでは、番号 0 は発信元のロケーションを示し、番号 1 は宛先のロケーションを示しています。BW = -1 によって発信元のロケーションの帯域幅が決定されています。値 -1 は、帯域幅が無限であることを意味します。帯域幅が無限であるのは、LAN 環境に配置された Cisco IP Phone からコールが発信されたためです。BW = 64 によって宛先のロケーションの帯域幅が決定されています。コールの宛先には PSTN に配置された電話機が指定されていて、使用されるコーデック タイプは G.711（64 Kbps）です。

```
15:20:21.421 CCM|Locations:Orig=0 BW=-1 Dest=1 BW=64 (-1 implies
infinite bw available)
```

次のトレースは、発信側と着信側の情報を示しています。この例では、管理者が John Smith などの表示名を設定していないので、発信側の名前と番号は同じです。

```
15:20:21.421 CCM|StationD - stationOutputCallInfo
CallingPartyName=1001,  CallingParty=1001, CalledPartyName=,
CalledParty=3333, tcpHandle=0x5138d98
```

次のトレースは、H.323 コードが初期化されて H.225 セットアップ メッセージを送信していることを示しています。従来の HDLC SAPI メッセージ、着信側の 16 進表記の IP アドレス、およびポート番号も確認できます。

```
15:20:21.421 CCM|Out Message -- H225SetupMsg -- Protocol= H225Protocol
15:20:21.421 CCM|MMan_Id= 1. (iep=  0 dsl=  0 sapi=  0 ces=  0
IpAddr=e24610ac IpPort=47110)
```

次のトレースは、発信側と着信側の情報および H.225 アラート メッセージを示しています。また、Cisco IP Phone の 16 進数値と IP アドレスのマッピングも示しています。Cisco IP Phone（1001）の IP アドレスは 172.16.70.231 です。

```
15:20:21.437 CCM|StationD - stationOutputCallInfo
CallingPartyName=1001,  CallingParty=1001, CalledPartyName=,
CalledParty=3333, tcpHandle=0x5138d98
15:20:21.453 CCM|In  Message -- H225AlertMsg -- Protocol= H225Protocol
15:20:21.953 CCM|StationD - stationOutputOpenReceiveChannel
tcpHandle=0x5138d98 myIP: e74610ac (172.16.70.231)
```

次のトレースは、このコールに使用される圧縮タイプ（G.711 mu-law）を示しています。

```
15:20:21.953 CCM|StationD - ConferenceID: 0 msecPacketSize: 20
compressionType:(4)Media_Payload_G711Ulaw64k
```

H.225 アラート メッセージが送信された後、H.323 は H.245 を初期化します。次のトレースは、発信側と着信側の情報および H.245 メッセージを示しています。TCP ハンドル値はこれまでと変わらず、同一コールが継続していることを示しています。

```
ONE FOR EACH Channel- 16:53:36.855 CCM|H245Interface(3) paths
established ip = e98e6b80, port =
1304|<CT::1,100,105,1.1682><IP::128.107.142.233>
ONE FOR EACH Channel- 16:53:37.199 CCM|H245Interface(3) OLC outgoing
confirm ip = b870701, port = 49252|<CT::1,100,128,3.9><IP::1.7.135.11>

H323 EP has answered the call and H245 channel setup in progress:
16:53:13.479 CCM|In  Message -- H225ConnectMsg -- Protocol=
H225Protocol|

16:03:25.359 CCM|StationD(1):  TCPPid = [1.100.117.1] CallInfo
callingPartyName='' callingParty=13001 cgpnVoiceMailbox=
calledPartyName='' calledParty=11002 cdpnVoiceMailbox=
originalCalledPartyName='' originalCalledParty=11002
originalCdpnVoiceMailbox= originalCdpnRedirectReason=0
lastRedirectingPartyName='' lastRedirectingParty=11002
lastRedirectingVoiceMailbox= lastRedirectingReason=0
callType=2(OutBound) lineInstance=1 callReference=16777217. version:
0|<CT::1,100,11,2.1><IP::><DEV::>

16:03:25.328 CCM|StationD(1):   TCPPid = [1.100.117.1]
OpenReceiveChannel conferenceID=16777217 passThruPartyID=16777233
millisecondPacketSize=20
compressionType=4(Media_Payload_G711Ulaw64k) qualifierIn=?. myIP:
e98e6b80 (128.107.142.233)|<CT::1,100,11,1.1><IP::><DEV::>
16:03:25.359 CCM|StationD(2):   TCPPid = [1.100.117.2]
StartMediaTransmission conferenceID=16777218 passThruPartyID=16777249
remoteIpAddress=e98e6b80(64.255.0.0)    remotePortNumber=65344
milliSecondPacketSize=20 compressType=4(Media_Payload_G711Ulaw64k)
qualifierOut=?. myIP: e98e6b80
(128.107.142.233)|<CT::1,100,105,1.213><IP::128.107.142.233>
16:03:25.375 CCM|StationD(2):   TCPPid = [1.100.117.2]
star_StationOutputStartMultiMediaTransmission conferenceID=16777218
passThruPartyID=16777250 remoteIpAddress=e98e6b80(66.255.0.0)
remotePortNumber=65346 compressType=101(Media_Payload_H263)
qualifierOut=?. myIP: e98e6b80
(128.107.142.233)|<CT::1,100,105,1.215><IP::128.107.142.233>
16:03:25.328 CCM|StationD(1):   TCPPid=[1.100.117.1]
OpenMultiReceiveChannel conferenceID=16777217 passThruPartyID=1000011
compressionType=101(Media_Payload_H263) qualifierIn=?.   myIP:
e98e6b80 (128.107.142.233)|<CT::1,100,11,1.1><IP::><DEV::>
```

次のトレースは、H.225 接続メッセージおよびその他の情報を示しています。H.225 接続メッセージが受信されると、コールが接続されます。

```
15:20:22.968 CCM|In  Message -- H225ConnectMsg -- Protocol=
H225Protocol
15:20:22.968 CCM|StationD - stationOutputCallInfo
CallingPartyName=1001,  CallingParty=1001, CalledPartyName=,
CalledParty=3333, tcpHandle=0x5138d98
15:20:22.062 CCM|MediaCoordinator - wait_AuConnectInfoInd
15:20:22.062 CCM|StationD - stationOutputStartMediaTransmission
tcpHandle=0x5138d98 myIP: e74610ac (172.16.70.231)
15:20:22.062 CCM|StationD - RemoteIpAddr: e24610ac (172.16.70.226)
RemoteRtpPortNumber: 16758 msecPacketSize: 20
compressionType:(4)Media_Payload_G711Ulaw64k
15:20:22.062 CCM|Locations:Orig=0 BW=-1Dest=1 BW=6(-1 implies infinite
bw available)
16:03:25.359 CCM|MediaManager(1) - wait_AuConnectInfo - recieved
response, fowarding,
CI(16777217,16777218)|<CT::1,100,105,1.213><IP::128.107.142.233>
16:03:25.359 CCM|MediaCoordinator -
wait_AuConnectInfoInd|<CT::1,100,105,1.213><IP::128.107.142.233>
16:03:25.359 CCM|ConnectionManager - wait_AuConnectInfoInd,
CI(16777217,16777218)|<CT::1,100,105,1.213><IP::128.107.142.233>
```

次のメッセージは、Cisco IP Phone（1001）からのオンフック メッセージが受信されていることを示しています。オンフック メッセージが受信されるとすぐに、H.225 メッセージと Skinny Station デバイス接続解除メッセージが送信され、H.225 メッセージ全体が表示されます。最後のメッセージは、コールが終了したことを示しています。

```
15:20:27.296 CCM|StationInit - InboundStim - OnHookMessageID
tcpHandle=0x5138d98
15:20:27.296 CCM|ConnectionManager -wait_AuDisconnectRequest
(16777247,16777248): STOP SESSION
15:20:27.296 CCM|MediaManager - wait_AuDisconnectRequest - StopSession
sending disconnect to (64,5) and remove connection from list
15:20:27.296 CCM| Device SEP003094C26105 , UnRegisters with SDL Link
to monitor NodeID= 1
15:20:27.296 CCM|StationD - stationOutputCloseReceiveChannel
tcpHandle=0x5138d98 myIP: e74610ac (172.16.70.231)
15:20:27.296 CCM|StationD - stationOutputStopMediaTransmission
tcpHandle=0x5138d98 myIP: e74610ac (172.16.70.231)
15:20:28.328 CCM|In  Message -- H225ReleaseCompleteMsg -- Protocol=
H225Protocol
16:03:33.344 CCM|StationInit - InboundStim - StationOnHookMessageID:
Msg Size(received, defined) = 4,
12|<CT::1,100,105,1.219><IP::128.107.142.233>
16:03:33.359 CCM|ConnectionManager -
wait_AuDisconnectRequest(16777217,16777218): STOP
SESSION|<CT::1,100,105,1.219><IP::128.107.142.233>
16:03:33.359 CCM|StationD(2):   TCPPid = [1.100.117.2]
CloseReceiveChannel conferenceID=16777218 passThruPartyID=16777249.
myIP: e98e6b80
(128.107.142.233)|<CT::1,100,105,1.219><IP::128.107.142.233>
16:03:33.359 CCM|StationD(2):   TCPPid = [1.100.117.2]
StopMediaTransmission conferenceID=16777218 passThruPartyID=16777249.
myIP: e98e6b80
(128.107.142.233)|<CT::1,100,105,1.219><IP::128.107.142.233>
16:03:33.359 CCM|StationD(2):   TCPPid = [1.100.117.2]
star_StationOutputCloseMultiMediaReceiveChannel conferenceID=16777218
passThruPartyID=16777249.  myIP: e98e6b80
(128.107.142.233)|<CT::1,100,105,1.219><IP::128.107.142.233>
16:03:33.359 CCM|StationD(2):   TCPPid = [1.100.117.2]
star_StationOutputStopMultiMediaTransmission conferenceID=16777218
passThruPartyID=16777250.  myIP: e98e6b80
(128.107.142.233)|<CT::1,100,105,1.219><IP::128.107.142.233>
```

Cisco IOS Gatekeeper のデバッグ メッセージと表示コマンド

「コール フロー トレース」では、Cisco CallManager SDI トレースについて詳細に説明しました。このケース スタディのトポロジでは、debug ras コマンドが Cisco IOS Gatekeeper でオンになっています。

次のデバッグ メッセージは、Cisco IOS Gatekeeper が Cisco CallManager（172.16.70.228）に対する admission request（ARQ; アドミッション要求）を受信し、その他の正常な Remote Access Server（RAS）メッセージがその後に続いていることを示しています。最後に、Cisco IOS Gatekeeper が admission confirmed（ACF; アドミッション確認）メッセージを Cisco CallManager に送信します。

```
*Mar 12 04:03:57.181: RASLibRASRecvData ARQ (seq# 3365) rcvd from
[172.16.70.228883] on sock [0x60AF038C]
*Mar 12 04:03:57.181: RASLibRAS_WK_TInit ipsock [0x60A7A68C] setup
successful
*Mar 12 04:03:57.181: RASlibras_sendto msg length 16 from
172.16.70.2251719 to 172.16.70.228883
*Mar 12 04:03:57.181: RASLibRASSendACF ACF (seq# 3365) sent to
172.16.70.228
```

次のデバッグ メッセージは、コールが進行中であることを示しています。

```
*Mar 12 04:03:57.181: RASLibRASRecvData successfully rcvd message of
length 55 from 172.16.70.228883
```

次のデバッグ メッセージは、Cisco IOS Gatekeeper が Cisco CallManager（172.16.70.228）から disengaged request (DRQ; 解除要求）を受信し、Cisco IOS Gatekeeper が disengage confirmed（DCF; 解除確認）を Cisco CallManager に送信したことを示しています。

```
*Mar 12 04:03:57.181: RASLibRASRecvData DRQ (seq# 3366) rcvd from
[172.16.70.228883] on sock [0x60AF038C]
*Mar 12 04:03:57.181: RASlibras_sendto msg length 3 from
172.16.70.2251719 to 172.16.70.228883
*Mar 12 04:03:57.181: RASLibRASSendDCF DCF (seq# 3366) sent to
172.16.70.228
*Mar 12 04:03:57.181: RASLibRASRecvData successfully rcvd message of
length 124 from 172.16.70.228883
```

Cisco IOS Gatekeeper に対するコマンド show gatekeeper endpoints は、4 つの Cisco CallManager がすべて Cisco IOS Gatekeeper に登録されていることを表示します。このケース スタディのトポロジでは、各クラスタに 2 つずつ、計 4 つの Cisco CallManager が存在することに注意してください。この Cisco IOS Gatekeeper には 2 つのゾーンがあり、各ゾーンには 2 つの Cisco CallManager があります。

```
R2514-1#show gatekeeper endpoints

                    GATEKEEPER ENDPOINT REGISTRATION
                    ================================
CallSignalAddr  Port  RASSignalAddr   Port  Zone Name          Type
--------------- ----- --------------- ----- ---------          ----
172.16.70.228       2     172.16.70.228       1493  gka.cisco.com
VOIP-GW
    H323-ID: ac1046e4->ac1046f5
172.16.70.229       2     172.16.70.229        3923  gka.cisco.com
VOIP-GW
    H323-ID: ac1046e5->ac1046f5
172.16.70.245       1     172.16.70.245        1041  gkb.cisco.com
VOIP-GW
    H323-ID: ac1046f5->ac1046e4
172.16.70.243        1     172.16.70.243       2043  gkb.cisco.com
VOIP-GW
    H323-ID: ac1046f5->ac1046e4
Total number of active registrations = 4
```

Cisco IOS Gateway のデバッグ メッセージと表示コマンド

「Cisco IOS Gatekeeper のデバッグ メッセージと表示コマンド」では、Cisco IOS Gatekeeper の表示コマンドとデバッグ出力について詳細に説明しました。この項では、Cisco IOS Gateway のデバッグ出力と表示コマンドについて取り上げます。このケース スタディのトポロジでは、コールは Cisco IOS Gateway を経由します。Cisco IOS Gateway は、T1/CAS または T1/PRI のいずれかのインターフェイスで PSTN または PBX に接続しています。次の例は、debug voip ccapi inout、debug H225 events、debug H225 asn1 などのコマンドのデバッグ出力を示しています。

次のデバッグ出力では、Cisco IOS Gateway が Cisco CallManager（172.16.70.228）からの TCP 接続要求を H.225 用のポート 2328 で受け入れます。

```
*Mar 12 04:03:57.169: H225Lib::h225TAccept: TCP connection accepted
from 172.16.70.228:2328 on socket [1]
*Mar 12 04:03:57.169: H225Lib::h225TAccept: Q.931 Call State is
initialized to be [Null].
*Mar 12 04:03:57.177: Hex representation of the received
TPKT030000650800000100
```

次のデバッグ出力は、この TCP セッションで Cisco CallManager から H.225 データが到達していることを示しています。このデバッグ出力では、使用されている H.323 バージョンを指定する protocolIdentifier に注意してください。次のデバッグは、H.323 バージョン 2 が使用されていることを示しています。この例は、着信側と発信側の番号も示しています。

```
- Source Address H323-ID
- Destination Address e164
*Mar 12 04:03:57.177:       H225Lib::h225RecvData: Q.931 SETUP
received from socket [1]value H323-UserInformation ::=
*Mar 12 04:03:57.181: {
*Mar 12 04:03:57.181:   h323-uu-pdu
*Mar 12 04:03:57.181:   {
*Mar 12 04:03:57.181:     h323-message-body setup :
*Mar 12 04:03:57.181:       {
*Mar 12 04:03:57.181:         protocolIdentifier { 0 0 8 2250 0 2 },
*Mar 12 04:03:57.181:         sourceAddress
*Mar 12 04:03:57.181:         {
*Mar 12 04:03:57.181:           h323-ID : "1001"
*Mar 12 04:03:57.181:         },
*Mar 12 04:03:57.185:         destinationAddress
*Mar 12 04:03:57.185:         {
*Mar 12 04:03:57.185:           e164 : "3333"
*Mar 12 04:03:57.185:         },
*Mar 12 04:03:57.189:       H225Lib::h225RecvData: State changed to
[Call Present].
```

次のデバッグ出力は、Call Control Application Programming Interface（CCAPi）を示しています。Call Control APi は着信コールを指定します。次の出力では、着信側と発信側の情報も確認できます。CCAPi はダイヤルピア 0 と一致します。0 はデフォルトのダイヤルピアです。CCAPi がダイヤルピア 0 と一致するのは、発

信側の番号について他のダイヤルピアが見つからなかったので、デフォルトのダイヤルピアを使用しているためです。

```
*Mar 12 04:03:57.189: cc_api_call_setup_ind (vdbPtr=0x616C9F54,
callInfo={called=3333, calling=1001, fdest=1 peer_tag=0},
callID=0x616C4838)
*Mar 12 04:03:57.193: cc_process_call_setup_ind (event=0x617A2B18)
handed call to app "SESSION"
*Mar 12 04:03:57.193: sess_appl: ev(19=CC_EV_CALL_SETUP_IND), cid(17),
disp(0)
*Mar 12 04:03:57.193: ccCallSetContext (callID=0x11,
context=0x61782BBC)
Mar 12 04:03:57.193: ssaCallSetupInd finalDest cllng(1001),
clled(3333)
*Mar 12 04:03:57.193: ssaSetupPeer cid(17) peer list:  tag(1)
*Mar 12 04:03:57.193: ssaSetupPeer cid(17), destPat(3333), matched(4),
prefix(), peer(6179E63C)
*Mar 12 04:03:57.193: ccCallSetupRequest (peer=0x6179E63C, dest=,
params=0x61782BD0 mode=0, *callID=0x617A87C0)
*Mar 12 04:03:57.193: callingNumber=1001, calledNumber=3333,
redirectNumber=
*Mar 12 04:03:57.193: accountNumber=,finalDestFlag=1,
guid=0098.89c8.9233.511d.0300.cddd.ac10.46e6
```

CCAPi は、ダイヤルピア 1 と宛先パターン（着信側の番号 3333）を一致させます。peer_tag はダイヤルピアを意味することに留意してください。要求パケット内の発信側と着信側の番号に注目してください。

```
*Mar 12 04:03:57.193: peer_tag=1
*Mar 12 04:03:57.197: ccIFCallSetupRequest: (vdbPtr=0x617BE064, dest=,
callParams={called=3333, calling=1001, fdest=1, voice_peer_tag=1},
mode=0x0)
```

次のデバッグ出力は、H.225 アラート メッセージが Cisco CallManager に返されていることを示しています。

```
*Mar 12 04:03:57.197: ccCallSetContext (callID=0x12,
context=0x61466B30)
*Mar 12 04:03:57.197: ccCallProceeding (callID=0x11, prog_ind=0x0)
*Mar 12 04:03:57.197: cc_api_call_proceeding(vdbPtr=0x617BE064,
callID=0x12, prog_ind=0x0)
*Mar 12 04:03:57.197: cc_api_call_alert(vdbPtr=0x617BE064,
callID=0x12, prog_ind=0x8, sig_ind=0x1)
*Mar 12 04:03:57.201: sess_appl: ev(17=CC_EV_CALL_PROCEEDING),
cid(18), disp(0)
*Mar 12 04:03:57.201: ssa:
cid(18)st(1)oldst(0)cfid(-1)csize(0)in(0)fDest(0)-cid2(17)st2(1)oldst2
(0)
*Mar 12 04:03:57.201: ssaIgnore cid(18), st(1),oldst(1), ev(17)
*Mar 12 04:03:57.201: sess_appl: ev(7=CC_EV_CALL_ALERT), cid(18),
disp(0)
*Mar 12 04:03:57.201: ssa:
cid(18)st(1)oldst(1)cfid(-1)csize(0)in(0)fDest(0)-cid2(17)st2(1)oldst2
(0)
*Mar 12 04:03:57.201: ssaFlushPeerTagQueue cid(17) peer list: (empty)
*Mar 12 04:03:57.201: ccCallAlert (callID=0x11, prog_ind=0x8,
sig_ind=0x1)
*Mar 12 04:03:57.201: ccConferenceCreate (confID=0x617A8808,
callID1=0x11, callID2=0x12, tag=0x0)
*Mar 12 04:03:57.201: cc_api_bridge_done (confID=0x7,
srcIF=0x616C9F54, srcCallID=0x11, dstCallID=0x12, disposition=0,
tag=0x0)value H323-UserInformation
*Mar 12 04:03:57.201: {
*Mar 12 04:03:57.201:   h323-uu-pdu
*Mar 12 04:03:57.201:   {
*Mar 12 04:03:57.201:     h323-message-body alerting :
*Mar 12 04:03:57.201:       {
*Mar 12 04:03:57.201:         protocolIdentifier { 0 0 8 2250 0 2 },
*Mar 12 04:03:57.205:         destinationInfo
*Mar 12 04:03:57.205:         {
*Mar 12 04:03:57.205:           mc FALSE,
*Mar 12 04:03:57.205:           undefinedNode FALSE
*Mar 12 04:03:57.205:         },
```

このパケットでは、Cisco IOS が H.245 アドレスとポート番号も Cisco CallManager に送信していることに注意してください。Cisco IOS Gateway は到達不能なアドレスを送信する場合があるため、無音声または単方向音声になることがあります。

```
*Mar 12 04:03:57.205:          h245Address ipAddress :
*Mar 12 04:03:57.205:            {
*Mar 12 04:03:57.205:              ip 'AC1046E2'H,
*Mar 12 04:03:57.205:              port 011008
*Mar 12 04:03:57.205:            },
*Mar 12 04:03:57.213: Hex representation of the ALERTING TPKT to
send.0300003D0100
*Mar 12 04:03:57.213:
*Mar 12 04:03:57.213:       H225Lib::h225AlertRequest: Q.931 ALERTING
sent from socket [1]. Call state changed to [Call Received].
*Mar 12 04:03:57.213: cc_api_bridge_done (confID=0x7,
srcIF=0x617BE064, srcCallID=0x12, dstCallID=0x11, disposition=0,
tag=0x0)
```

次のデバッグ出力は、H.245 セッションが開始していることを示しています。コーデック ネゴシエーションの機能表示および各音声パケットに含まれるバイト数を確認できます。

```
*Mar 12 04:03:57.217: cc_api_caps_ind (dstVdbPtr=0x616C9F54,
dstCallId=0x11, srcCallId=0x12, caps={codec=0xEBFB, fax_rate=0x7F,
vad=0x3, modem=0x617C5720 codec_bytes=0, signal_type=3})
*Mar 12 04:03:57.217: sess_appl: ev(23=CC_EV_CONF_CREATE_DONE),
cid(17), disp(0)
*Mar 12 04:03:57.217: ssa:
cid(17)st(3)oldst(0)cfid(7)csize(0)in(1)fDest(1)-cid2(18)st2(3)oldst2(
1)
*Mar 12 04:03:57.653: cc_api_caps_ind (dstVdbPtr=0x617BE064,
dstCallId=0x12, srcCallId=0x11, caps={codec=0x1, fax_rate=0x2,
vad=0x2, modem=0x1, codec_bytes=160, signal_type=0})
```

次のデバッグ出力は、両方の側が正常にネゴシエートし、160 バイトのデータを持つ G.711 コーデックで合意したことを示しています。

```
*Mar 12 04:03:57.653: cc_api_caps_ack (dstVdbPtr=0x617BE064,
dstCallId=0x12, srcCallId=0x11, caps={codec=0x1, fax_rate=0x2,
vad=0x2, modem=0x1, codec_bytes=160, signal_type=0})
*Mar 12 04:03:57.653: cc_api_caps_ind (dstVdbPtr=0x617BE064,
dstCallId=0x12, srcCallId=0x11, caps={codec=0x1, fax_rate=0x2,
vad=0x2, modem=0x, codec_bytes=160, signal_type=0})
*Mar 12 04:03:57.653: cc_api_caps_ack (dstVdbPtr=0x617BE064,
dstCallId=0x12, srcCallId=0x11, caps={codec=0x1, fax_rate=0x2,
vad=0x2, modem=0x1, codec_bytes=160, signal_type=0})
*Mar 12 04:03:57.657: cc_api_caps_ack (dstVdbPtr=0x616C9F54,
dstCallId=0x11, srcCallId=0x12, caps={codec=0x1, fax_rate=0x2,
vad=0x2, modem=0x1, codec_bytes=160, signal_type=0})
*Mar 12 04:03:57.657: cc_api_caps_ack (dstVdbPtr=0x616C9F54,
dstCallId=0x11, srcCallId=0x12, caps={codec=0x1, fax_rate=0x2,
vad=0x2, modem=0x1, codec_bytes=160, signal_type=0})
```

H.323 接続および接続解除のメッセージがこの後に続きます。

```
*Mar 12 04:03:59.373: cc_api_call_connected(vdbPtr=0x617BE064,
callID=0x12)
*Mar 12 04:03:59.373: sess_appl: ev(8=CC_EV_CALL_CONNECTED), cid(18),
disp(0)
*Mar 12 04:03:59.373: ssa:
cid(18)st(4)oldst(1)cfid(7)csize(0)in(0)fDest(0)-cid2(17)st2(4)oldst2(
3)
*Mar 12 04:03:59.373: ccCallConnect (callID=0x11)
*Mar 12 04:03:59.373: {
*Mar 12 04:03:59.373:   h323-uu-pdu
*Mar 12 04:03:59.373:   {
*Mar 12 04:03:59.373:     h323-message-body connect :
*Mar 12 04:03:59.373:       {
*Mar 12 04:03:59.373:         protocolIdentifier { 0 0 8 2250 0 2 },
*Mar 12 04:03:59.373:         h245Address ipAddress :
*Mar 12 04:03:59.373:           {
*Mar 12 04:03:59.377:             ip 'AC1046E2'H,
*Mar 12 04:03:59.377:             port 011008
*Mar 12 04:03:59.377:           },
*Mar 12 04:03:59.389: Hex representation of the CONNECT TPKT to
send.03000052080
*Mar 12 04:03:59.393: H225Lib::h225SetupResponse: Q.931 CONNECT sent
from socket [1]
*Mar 12 04:03:59.393: H225Lib::h225SetupResponse: Q.931 Call State
changed to [Active].
*Mar 12 04:04:08.769: cc_api_call_disconnected(vdbPtr=0x617BE064,
callID=0x12, cause=0x10)
*Mar 12 04:04:08.769: sess_appl: ev(12=CC_EV_CALL_DISCONNECTED),
cid(18), disp(0)
```

T1/PRI インターフェイスを使用する Cisco IOS Gateway

前述したように、2 つのタイプのコールが Cisco IOS Gateway を経由し、Cisco IOS Gateway は、T1/CAS または T1/PRI のいずれかのインターフェイスで PSTN または PBX に接続しています。次の例は、Cisco IOS Gateway が T1/PRI インターフェイスを使用する場合のデバッグ出力を示しています。

Cisco IOS Gateway で debug isdn q931 コマンドがオンになっていて、ISDN 環境にある D チャネル用のレイヤ 3 シグナリング プロトコルである Q.931 が有効になっています。T1/PRI インターフェイスからコールが発信されるたびに、セットアップ パケットが送信される必要があります。セットアップ パケットには必ずプロトコル記述子 pd = 8 が含まれており、callref 用にランダムな 16 進数値が生成されます。callref はコールを追跡します。たとえば、2 つのコールが発信された場合、callref の値によって、RX（受信済み）メッセージの対象になっているコールを判別できます。ベアラ機能 0x8890 は 64 Kbps データ コールを意味します。これが 0x8890218F だった場合は、56 Kbps データ コールになり、音声コールでは 0x8090A3 になります。下記のデバッグ出力では、ベアラ機能は 0x8090A3（音声用）です。この例は、着信側と発信側の番号を示しています。

callref では、最初の数字に異なる値が使用され（TX と RX を区別するため）、2 番目の値は同じです（SETUP には最後の数字に 0 が設定され、CONNECT_ACK にも 0 が設定されています）。ルータは PSTN または PBX に完全に依存して Bearer チャネル（B チャネル）を割り当てます。PSTN または PBX がルータにチャネルを割り当てない場合、コールはルーティングされません。このケース スタディでは、ALERTING 用に受信されたものと同じ参照番号（0x800B）を使用して、CONNECT メッセージが交換機から受信されます。最後に、コールが接続解除されるとき、DISCONNECT メッセージの交換の後に、RELEASE メッセージおよび RELEASE _COMP メッセージが続きます。RELEASE_COMP メッセージの後には、コール拒否の理由 ID が続きます。理由 ID は 16 進数値です。理由の内容は、16 進数値のデコードとプロバイダーのフォローアップによって確認できます。

```
 *Mar  1 225209.694 ISDN Se115 TX ->  SETUP pd = 8  callref = 0x000B
 *Mar  1 225209.694         Bearer Capability i = 0x8090A3
 *Mar  1 225209.694         Channel ID i = 0xA98381
 *Mar  1 225209.694         Calling Party Number i = 0x2183, '1001'
 *Mar  1 225209.694         Called Party Number i = 0x80, '3333'
 *Mar  1 225209.982 ISDN Se115 RX <-  ALERTING pd = 8  callref =
0x800B
 *Mar  1 225209.982         Channel ID i = 0xA98381
 *Mar  1 225210.674 ISDN Se115 RX <-  CONNECT pd = 8  callref = 0x800B
 *Mar  1 225210.678 ISDN Se115 TX ->  CONNECT_ACK pd = 8  callref =
0x000B
 *Mar  1 225215.058 ISDN Se115 RX <-  DISCONNECT pd = 8  callref =
0x800B
 *Mar  1 225215.058         Cause i = 0x8090 - Normal call clearing
225217 %ISDN-6
DISCONNECT Int S10  disconnected from unknown , call lasted 4 sec
 *Mar  1 225215.058 ISDN Se115 TX ->  RELEASE pd = 8  callref = 0x000B
 *Mar  1 225215.082 ISDN Se115 RX <-  RELEASE_COMP pd = 8  callref =
0x800B
*Mar  1 225215.082  Cause i = 0x829F - Normal, unspecified or Special
intercept, call blocked group restriction
```

T1/CAS インターフェイスを使用する Cisco IOS Gateway

2 つのタイプのコールが Cisco IOS Gateway を経由し、Cisco IOS Gateway は、T1/CAS または T1/PRI のいずれかのインターフェイスで PSTN または PBX に接続しています。次の例は、Cisco IOS Gateway が T1/CAS インターフェイスを使用する場合のデバッグ出力を示しています。Cisco IOS Gateway で debug cas はオンになっています。

次のデバッグ メッセージは、Cisco IOS Gateway がオフフック信号を交換機に送信していることを示しています。

```
Apr  5 17:58:21.727: from NEAT(0): (0/15): Tx LOOP_CLOSURE (ABCD=1111)
```

次のデバッグ メッセージは、交換機が Cisco IOS Gateway から閉ループ信号を受信した後にウィンクを送信していることを示しています。

```
Apr  5 17:58:21.859: from NEAT(0): (0/15): Rx LOOP_CLOSURE (ABCD=1111)
Apr  5 17:58:22.083: from NEAT(0): (0/15): Rx LOOP_OPEN (ABCD=0000)
```

次のデバッグ メッセージは、Cisco IOS Gateway がオフフックしようとしていることを示しています。

```
Apr  5 17:58:23.499: from NEAT(0): (0/15): Rx LOOP_CLOSURE (ABCD=1111)
```

次の出力は、コール進行中の Cisco IOS Gateway での show call active voice brief を示しています。この出力は、着信側と発信側の番号およびその他の有用な情報も示しています。

```
R5300-5#show call active voice brief
<ID>: <start>hs.<index> +<connect> pid:<peer_id> <dir> <addr> <state>
tx:<packets>/<bytes> rx:<packets>/<bytes> <state>
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms
lost:<lost>/<early>/<late>  delay:<last>/<min>/<max>ms <codec>
 FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
sig:<on/off> <codec> (payload size)
 Tele <int>: tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l>
i/o:<l>/<l> dBm
511D : 156043737hs.1 +645 pid:0 Answer 1001 active
 tx:1752/280320 rx:988/158080
 IP172.16.70.228:18888 rtt:0ms pl:15750/80ms lost:0/0/0
delay:25/25/65ms g711ulaw
511D : 156043738hs.1 +644 pid:1 Originate 3333 active
 tx:988/136972 rx:1759/302548
 Tele 1/0/0 (30): tx:39090/35195/0ms g711ulaw noise:-43 acom:0
i/0:-36/-42 dBm
```

ケース スタディ：クラスタ間コールのトラブルシューティング

この付録のケース スタディでは、異なるクラスタに配置された別の Cisco IP Phone にコールを発信する Cisco IP Phone について説明します。このタイプのコールは、クラスタ間 Cisco IP Phone コールとも呼ばれます。

この章では、次のトピックについて取り上げます。

トポロジの例

このケース スタディでは、次に示すトポロジの例を使用します。2 つのクラスタがあり、各クラスタには 2 つの Cisco CallManager があります。また、Cisco IOS Gateways と Cisco IOS Gatekeeper も配置されています。

クラスタ間 H.323 通信

Cluster 1 の Cisco IP Phone が Cluster 2 の Cisco IP Phone にコールを発信します。クラスタ間 Cisco CallManager 通信は、H.323 バージョン 2 プロトコルを使用して行われます。Cisco IOS Gatekeeper もアドミッション制御に使用されます。

Cisco IP Phone は Skinny Station プロトコルを使用して Cisco CallManager に接続でき、Cisco CallManager は H.323 Registration, Admission, and Status（RAS）プロトコルを使用して Cisco IOS Gatekeeper に接続できます。admission request（ARQ; アドミッション要求）メッセージが Cisco IOS Gatekeeper に送信され、この Gatekeeper は H.323 バージョン 2 プロトコルを使用してクラスタ間コールが発信できることを確認した後、admission confirmed（ACF; アドミッション確認）メッセージを送信します。この処理が実行されると、RTP プロトコルを使用して、異なるクラスタにある Cisco IP Phone 間に音声パスが作成されます。

コール フロー トレース

この項では、CCM000000000 ファイルに取り込んだ SDI トレースの例を使用して、コール フローについて説明します。このケース スタディで取り上げるトレースでは、コール フロー自体に焦点を絞っています。

このコール フローでは、Cluster 2 に配置された Cisco IP Phone（2002）が Cluster 1 に配置された Cisco IP Phone（1001）にコールを発信しています。TCP ハンドル値、タイム スタンプ、またはデバイスの名前を調べることで、デバイスをトレース上で追跡できます。デバイスをリブートするかオフラインにするまで、デバイスの TCP ハンドル値は変わりません。

次のトレースでは、Cisco IP Phone（2002）はオフフックになっています。このトレースは、一意のメッセージ、TCP ハンドル、および発信側の番号を示しています。これらは Cisco IP Phone に表示されます。次のデバッグ出力は、着信側の番号（1001）、H.225 接続、および H.245 確認メッセージを示しています。コーデック タイプは G.711 mu-law です。

```
16:06:13.921 CCM|StationInit - InboundStim - OffHookMessageID
tcpHandle=0x1c64310
16:06:13.953 CCM|Out Message -- H225ConnectMsg -- Protocol=
H225Protocol
16:06:13.953 CCM|Ie - H225UserUserIe IEData= 7E 00 37 05 02 C0 06
16:06:13.953 CCM|StationD - stationOutputCallInfo CallingPartyName=,
CallingParty=2002, CalledPartyName=1001, CalledParty=1001,
tcpHandle=0x1c64310
16:06:14.015 CCM|H245Interface(2) OLC indication chan number = 2
16:06:14.015 CCM|StationD - stationOutputOpenReceiveChannel
tcpHandle=0x1c64310 myIP: e74610ac (172.16.70.231)
16:06:14.015 CCM|StationD - ConferenceID: 0 msecPacketSize: 20
compressionType:(4)Media_Payload_G711Ulaw64k
16:06:14.062 CCM|StationInit - InboundStim -
StationOpenReceiveChannelAckID tcpHandle=0x1c64310, Status=0,
IpAddr=0xe74610ac, Port=20444, PartyID=2
16:06:14.062 CCM|H245Interface(2) paths established ip = e74610ac,
port = 20444
16:06:14.187 CCM|H245Interface(2) OLC outgoing confirm ip = fc4610ac,
port = 29626
```

次のトレースは、発信側と着信側の番号を示しています。これらの番号は IP アドレスおよび 16 進数値に関連付けられています。

```
16:06:14.187 CCM|StationD - stationOutputStartMediaTransmission
tcpHandle=0x1c64310 myIP: e74610ac (172.16.70.231)
16:06:14.187 CCM|StationD - RemoteIpAddr: fc4610ac (172.16.70.252)
```

次のトレースは、Cisco IP Phone（2002）のパケット サイズと MAC アドレスを示しています。このトレースの後に接続解除メッセージが続き、その後にオンフック メッセージが続きます。

```
RemoteRtpPortNumber: 29626 msecPacketSize: 20
compressionType:(4)Media_Payload_G711Ulaw64k
16:06:16.515 CCM| Device SEP003094C26105 , UnRegisters with SDL Link
to monitor NodeID= 1
16:06:16.515 CCM|StationD - stationOutputCloseReceiveChannel
tcpHandle=0x1c64310 myIP: e74610ac (172.16.70.231)
16:06:16.515 CCM|StationD - stationOutputStopMediaTransmission
tcpHandle=0x1c64310 myIP: e74610ac (172.16.70.231)
16:06:16.531 CCM|In  Message -- H225ReleaseCompleteMsg -- Protocol=
H225Protocol
16:06:16.531 CCM|Ie - Q931CauseIe -- IEData= 08 02 80 90
16:06:16.531 CCM|Ie - H225UserUserIe -- IEData= 7E 00 1D 05 05 80 06
16:06:16.531 CCM|Locations:Orig=1 BW=64Dest=0 BW=-1 (-1 implies
infinite bw available)
16:06:16.531 CCM|MediaManager - wait_AuDisconnectRequest - StopSession
sending disconnect to (64,2) and remove connection from list
16:06:16.531 CCM|MediaManager - wait_AuDisconnectReply - received all
disconnect replies, forwarding a reply for party1(16777219) and
party2(16777220)
16:06:16.531 CCM|MediaCoordinator - wait_AuDisconnectReply - removing
MediaManager(2) from connection list
16:06:16.734 CCM|StationInit - InboundStim - OnHookMessageID
tcpHandle=0x1c64310
```

コール フローの失敗

この項では、SDI トレースを確認しながら、クラスタ間コール フローの失敗について説明します。次のトレースでは、Cisco IP Phone（1001）はオフフックになります。TCP ハンドルが Cisco IP Phone に割り当てられます。

```
16:05:33.468 CCM|StationInit - InboundStim - OffHookMessageID
tcpHandle=0x4fbbc30
16:05:33.468 CCM|StationD - stationOutputDisplayText
tcpHandle=0x4fbbc30, Display= 1001
16:05:33.484 CCM|StationD - stationOutputSetLamp stim: 9=Line
instance=1 lampMode=LampOn tcpHandle=0x4fbbc30
```

次のトレースでは、ユーザが着信側の Cisco IP Phone の番号（2000）をダイヤルし、番号分析プロセスが番号を一致させようとしています。

```
16:05:33.484 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="")
16:05:33.484 CCM|Digit analysis:
potentialMatches=PotentialMatchesExist
16:05:35.921 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="2")
16:05:35.921 CCM|Digit
analysis:potentialMatches=ExclusivelyOffnetPotentialMatchesExist
16:05:36.437 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="20")
16:05:36.437 CCM|Digit
analysis:potentialMatches=ExclusivelyOffnetPotentialMatchesExist
16:05:36.656 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="200")
16:05:36.656 CCM|Digit
analysis:potentialMatches=ExclusivelyOffnetPotentialMatchesExist
16:05:36.812 CCM|Digit analysis: match(fqcn="", cn="1001", pss="",
dd="2000")
```

これで番号分析が完了しました。次のトレースは、その結果を示しています。次の PotentialMatches=NoPotentialMatchesExist 参照は、Cisco CallManager がこの電話番号と一致しないことを示しています。この点に注意することが重要です。最後に、リオーダー音が発信側（1001）に送信され、その後にオンフック メッセージが続きます。

```
16:05:36.812 CCM|Digit analysis: analysis results
16:05:36.812 CCM||PretransformCallingPartyNumber=1001
|CallingPartyNumber=1001
|DialingPattern=2XXX
|DialingRoutePatternRegularExpression=(2XXX)
|PotentialMatches=NoPotentialMatchesExist
|CollectedDigits=2000
16:05:36.828 CCM|StationD - stationOutputCallInfo
CallingPartyName=1001,  CallingParty=1001, CalledPartyName=,
CalledParty=2000, tcpHandle=0x4fbbc30
16:05:36.828 CCM|StationD - stationOutputStartTone: 37=ReorderTone
tcpHandle=0x4fbbc30
16:05:37.953 CCM|StationInit - InboundStim - OnHookMessageID
tcpHandle=0x4fbbc30
```

Numerics

A

C

D

I

P

R

S

T

U

あ