Cisco Unified Communications Manager リリース 12.5(1) トラブルシューティング ガイド

初版：2017 年 12 月 7 日

最終更新：2019 年 10 月 15 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次

はじめに

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、関連資料を入手する方法を示します。

目的

『*Cisco Unified Communications Manager* トラブルシューティング ガイド』には、このリリースの Unified Communications Manager のトラブルシューティング手順が記載されています。

（注） このバージョンの『*Cisco Unified Communications Manager* トラブルシューティング ガイド』に記載されている情報は、以前のリリースの Cisco Unified Communications Manager ソフトウェアには該当しない場合があります。

このドキュメントでは、Unified Communications Manager システムで発生する可能性のあるすべての問題について説明するのではなく、Cisco Technical Assistance Center（TAC）で頻繁に対応している問題やニュースグループからの FAQ を中心に説明します。

対象読者

『*Cisco Unified Communications Manager* トラブルシューティング ガイド』では、Cisco Unified Communications Manager システムの管理を担当するネットワーク管理者、企業管理者、および

従業員にガイダンスを提供します。このマニュアルを使用するには、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。

構成

次の表に、このマニュアルの構成を示します。

表 *1*: このマニュアルの構成

章およびタイトル	説明
トラブルシューティングの概要 （1 ページ）	Cisco Unified Communications Manager のトラブルシューティングに使用できるツールおよびリソースの概要を示します。
トラブルシューティング ツール （5 ページ）	Unified Communications Manager の設定、監視、およびトラブルシューティングに使用できるツールとユーティリティについて説明し、テストの繰り返しや同じデータの再収集を回避するために、情報の収集に関する一般的なガイドラインを提供します。
Cisco Unified Communications Manager のシステムの問題 （37 ページ）	Unified Communications Manager システム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。
デバイスの問題 （71 ページ）	IP Phone およびゲートウェイ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。
ダイヤル プランとルーティングの問題 （95 ページ）	ダイヤルプラン、ルート パーティション、およびコーリング サーチ スペース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。
Cisco Unified Communications Manager のサービスの問題 （103 ページ）	会議ブリッジやメディア ターミネーション ポイントなど、サービス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。
ボイス メッセージングの問題 （109 ページ）	一般的な音声メッセージングの問題の解決方法について説明します。
トラブルシューティングの機能とサービス （113 ページ）	Unified Communications Manager の機能およびサービスに関連する一般的な問題の解決に役立つ情報を提供します。
SNMP のトラブルシューティング （167 ページ）	SNMP のトラブルシューティングを行う方法に関する情報を提供します。

章およびタイトル	説明
TAC とのケースのオープン （189 ページ）	TAC Case Open ツールのサービスを利用するために必要な情報について説明します。
ケース スタディ：Cisco Unified IP Phone コールのトラブルシューティング （197 ページ）	クラスタ内の 2 つの Cisco Unified IP Phone 間のコール フローについて詳細に説明します。
ケース スタディ：Cisco Unified IP Phone と Cisco IOS ゲートウェイ間のコールのトラブルシューティング （211 ページ）	ローカル PBX または公衆電話交換網（PSTN）で接続された電話機に Cisco IOS ゲートウェイを介してコールする Cisco Unified IP Phone について説明します。

関連資料

関連する Cisco IP テレフォニー アプリケーションおよび製品の詳細については、『*Cisco Unified Communications Manager Documentation Guide*』を参照してください。次の URL は、マニュアルへのパスの例です。

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

Cisco Unity に関連する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/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html

表記法

このマニュアルでは、以下の表記法を使用しています。

表記法	説明
太字フォント	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、イタリック体で表記されています。
[ ]	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。

表記法	説明
string	引用符を付けない一組の文字。string 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 string 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、山カッコ（<>）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 アドバイスは、次のように表しています。

ワンポイント アドバイス 「時間の節約に役立つ操作」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。

ヒントは、次のように表しています。

ヒント 役立つ「ヒント」の意味です。

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、次のように表しています。

警告 この警告マークは「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。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。

マニュアルの入手方法、テクニカルサポート、およびセキュリティ ガイド

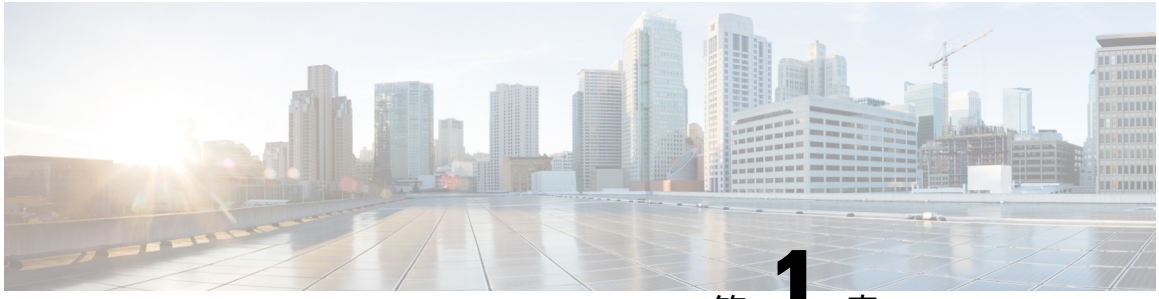
マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Cisco 製品のセキュリティ

本製品には暗号化機能が備わっており、輸入、輸出、配布および使用に適用される米国および他の国での法律を順守するものとします。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

米国の輸出規制の詳細については、http://www.access.gpo.gov/bis/ear/ear_data.html で参照できます。



第 1 章

トラブルシューティングの概要

ここでは、*Cisco Unified Communications Manager* のトラブルシューティングに必要な背景情報と使用できるリソースについて説明します。

Cisco Unified Serviceability

Cisco Unified Serviceability は、Unified Communications Manager 用の Web ベースのトラブルシューティング ツールです。このツールには、管理者がシステム問題をトラブルシューティングできるように次の機能が備えられています。

- トラブルシューティング用に Unified Communications Manager サービスのアラームとイベントを保存し、アラーム メッセージの定義を提供します。
- トラブルシューティング用に Unified Communications Manager サービスの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の設定、収集、および表示を行うことができます。
- リアルタイム監視ツール（RTMT）を使用して、Unified Communications Manager クラスタのコンポーネントの動作をリアルタイムで監視します。
- Unified Communications Manager CDR Analysis and Reporting（CAR）を使用して、Quality of Service、トラフィック、課金情報についてのレポートを生成します。
- [サービスの開始（Service Activation）] ウィンドウによりアクティブ化、非アクティブ化、および表示を行うことができる機能サービスを提供する。
- 機能とネットワーク サービスを開始および停止するためのインターフェイスを提供する。
- Cisco Unified Serviceability のツールに関連付けられているレポートをアーカイブします。

- Unified Communications Managerが、SNMPリモート管理とトラブルシューティング用の管理対象デバイスとして動作できるようにします。
- 1つのサーバ（またはクラスタ内のすべてのサーバ）のログパーティションのディスク使用を監視します。

Cisco Unified Serviceabilityにアクセスするには、[Unified Communications Manager Administration]ウィンドウで、[ナビゲーション（Navigation）]ドロップダウンリストボックスから[Cisco Unified Serviceability]を選択します。Unified Communications Managerソフトウェアをインストールすると、Cisco Unified Serviceabilityが自動的にインストールされて使用可能になります。

サービスアビリティツールの詳細と手順については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

CiscoUnifiedCommunicationsOperatingSystemAdministration

Cisco Unified Communications Operating System Administrationを使用すると、次のタスクを実行してCisco Unified Communications Operating Systemを設定および管理できます。

- ソフトウェアとハードウェアのステータスを確認する。
- IPアドレスの確認と更新を行う。
- 他のネットワークデバイスにpingを送信する。
- Network Time Protocolサーバの管理。
- システムソフトウェアおよびオプションをアップグレードする。
- システムを再起動する。

有用性ツールの詳細と設定手順については、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』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ネットワーク環境のトラブルシューティングを行う場合は、症状を定義し、その症状の原因と考えられるすべての問題を特定し、考えられる各問題を、症状がなくなるまで可能性の高い順に体系的に取り除いていきます。

次の手順は、問題解決プロセスで使用するガイドラインを示しています。

手順

1. ネットワークの問題を分析し、問題を明確に記述します。症状と潜在的な原因を定義します。
2. 潜在的な原因を特定するための事実を収集します。

3. 収集した事実を元に、潜在的な原因を検証します。
4. それらの原因に基づいて処置プランを作成します。最も可能性の高い問題から始め、単一の変数だけを操作するプランを考案します。
5. 処置プランを実施し、テストして症状が消えるかどうかを確認しながら、各手順を慎重に実行します。
6. 結果を分析し、問題が解決したかどうかを確認します。問題が解決している場合は、プロセスは完了です。
7. 問題が解決していない場合は、リストで次に可能性の高い原因に基づいて処置プランを作成します。4 （3 ページ） に戻り、問題が解決するまでプロセスを繰り返します。

処置プランの実施中に行った変更は、必ず元に戻してください。変数は一度に 1 つだけ変更します。

（注） 一般的な原因と処置（このマニュアルで概要を説明しているもの、または環境に応じて特定したもの）をすべて実施しても問題が解決しない場合は、Cisco TAC にお問い合わせください。

ネットワーク障害への事前準備

ネットワーク障害からの回復は、事前準備をしておくと容易に行うことができます。次の質問に答え、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確認します。

- ネットワーク上のすべてのデバイスの物理的な場所とそれらの接続方法の概要を示した、相互接続された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、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、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、およびエリアの正確な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把握していますか。
- どのプロトコルがブリッジングされているかを把握していますか。それらのブリッジに設定されているフィルタがありますか。また、その設定のコピーはありますか。そのコピーは Unified Communications Manager に適用できますか。
- インターネットへの接続も含め、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とパフォーマンスについて組織で文書化していますか。

これらの質問に「はい」と答えることができれば、障害から迅速に回復できます。

詳細情報の入手先

さまざまな IP テレフォニー トピックに関する情報については、次のリンクを使用してください。

- 関連する Cisco IP テレフォニー アプリケーションおよび製品に関する詳細については、『*Cisco Unified Communications Manager Documentation Guide*』を参照してください。次の URL は、マニュアルへのパスの例です。

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

- Cisco Unity に関連する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/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html

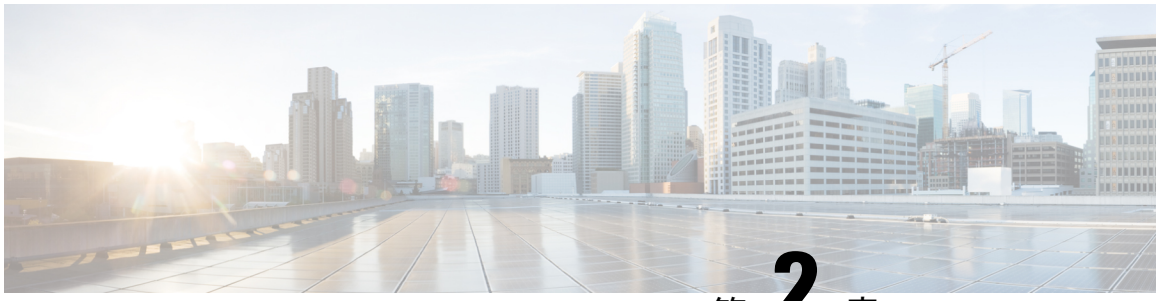
- Cisco Emergency Responder に関連するマニュアルについは、次の URL を参照してください。

- http://www.cisco.com/en/US/products/sw/voicesw/ps842/tsd_products_support_series_home.html

- Cisco Unified IP Phones に関連する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/en/US/products/hw/phones/ps379/tsd_products_support_series_home.html

- IP テレフォニー ネットワークの設計とトラブルシューティングについては、www.cisco.com/go/srnd にある『Cisco IP Telephony Solution Reference Network Design Guides』を参照してください。



第 2 章

トラブルシューティング ツール

ここでは、Unified Communications Manager の設定、監視、およびトラブルシューティングを行うために使用するツールやユーティリティについて説明し、テストの繰り返しや同一データの再収集を回避するために、データ収集に関する一般的なガイドラインを提供します。

（注） このマニュアルにリストされている URL サイトの一部にアクセスするには、登録ユーザとしてログインする必要があります。

Cisco Unified Serviceability トラブルシューティング ツール

Cisco Unified Serviceability には、さまざまな Unified Communications Manager システムを監視および分析するために、次のような各種ツールが用意されています。これらのツールの詳細については、『Cisco Unified Serviceability アドミニストレーション ガイド』を参照してください。

表 *2 : Serviceability* ツール

用語	定義
Cisco Unified Real-Time Monitoring Tool（RTMT）	このツールは、Unified Communications Manager のデバイスとパフォーマンス カウンタに関するリアルタイムな情報を提供するとともに、トレースの収集を可能にします。 パフォーマンス カウンタは、システム固有にすることも、Unified Communications Manager 固有にすることもできます。オブジェクトは、Cisco Unified IP Phone や Unified Communications Manager システム パフォーマンスなど、特定のデバイスまたは機能に対する同等のカウンタの論理的なグループで構成されます。カウンタによって、システム パフォーマンスのさまざまな側面が測定されます。登録済み電話機の数、試行されたコール数、進行中のコール数などの統計が測定されます。
アラーム	管理者は、アラームを使用して、Unified Communications Manager システムの実行時のステータスや状態情報を取得します。アラームには、説明や推奨処置など、システムの問題に関する情報が含まれています。 管理者は、アラーム定義データベースでアラーム情報を検索します。アラーム定義には、アラームの説明と推奨処置が含まれています。

用語	定義
トレース	管理者とシスコのエンジニアは、トレース ファイルを使用して、Unified Communications Manager サービスの問題に関する特定の情報を取得します。Cisco Unified Serviceability からトレース ログ ファイルに、設定済みトレース情報が送信されます。トレース ログ ファイルには、SDI と SDL の 2 種類があります。 各サービスには、デフォルトのトレース ログが含まれています。システムによって、サービスからのシステム診断インターフェイス（SDI）情報がトレースされ、実行時のイベントとトレースがログファイルに記録されます。 SDL トレース ログ 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。システムによって、コールの信号配信レイヤ（SDL）がトレースされ、状態遷移がログファイルに記録されます。 （注） 通常は、Cisco Technical Assistance Center（TAC）の指示に従って、SDL トレースだけを収集することになります。
Quality Report Tool	この用語は、Cisco Unified Serviceability の音声品質と一般的な問題をレポートするユーティリティを示しています。
Serviceability Connector	この製品を活用することで、シスコのテクニカル サポート スタッフがより迅速にインフラストラクチャの問題を診断できます。診断ログと情報を検出、取得して SR ケースに保存するタスク、および診断シグネチャに対する分析をトリガーするタスクを自動化することで、TAC がオンプレミスの機器に関する問題をより効率的に特定して解決できるようにします。

コマンドライン インターフェイス

コマンドライン インターフェイス（CLI）を使用すると、Unified Communications Manager システムにアクセスし、基本的なメンテナンスや障害からの回復を行うことができます。ハードワ

イヤされた端末（システム モニタとキーボード）を使用するか、または SSH セッションを実行することによってシステムにアクセスします。

インストール時に、アカウント名とパスワードが作成されます。パスワードはインストール後に変更できますが、アカウント名は変更できません。

コマンドとは、システムに特定の機能を実行させるテキスト命令を表します。コマンドは、単独で使用される場合と、必須または任意の引数を伴う場合があります。

レベルは、コマンドの集合で構成されます。たとえば、show はレベルを示し、show status はコマンドを示します。また、各レベルとコマンドには、特権レベルが関連付けられています。ユーザは、適切な特権レベルを持っている場合にだけ、コマンドを実行できます。

Unified Communications Manager の CLI コマンド セットの詳細については、『*Cisco Unified* ソリューション コマンドライン インターフェイス リファレンス ガイド』を参照してください。

Kerneldump ユーティリティ

Kerneldump ユーティリティにより、セカンダリ サーバを要求することなしに、該当するマシンでクラッシュ ダンプ ログをローカルに収集できます。

Unified Communications Manager クラスタでは、Kerneldump ユーティリティがサーバで有効であることを確認するだけで、クラッシュ ダンプ情報を収集できます。

（注） シスコでは、より効果的なトラブルシューティングを実現するため、Unified Communications Manager のインストール後に、Kerneldump ユーティリティが有効であることを確認するよう推奨しています。Kerneldump ユーティリティの設定をまだ行っていない場合は、Unified Communications Manager をサポート対象のアプライアンス リリースからアップグレードする前に行ってください。

重要 Kerneldump ユーティリティをイネーブル化またはディセーブル化を行うには、ノードのリブートが必要です。リブートが許容されるウィンドウ以外では、enable コマンドを実行しないでください。

Cisco Unified Communications オペレーティング システムのコマンドライン インターフェイス（CLI）を使用すると、Kerneldump ユーティリティのイネーブル化、ディセーブル化、ステータス確認を実行できます。

次の手順を利用して Kerneldump ユーティリティをイネーブル化します。

ユーティリティによって収集されるファイルの処理

Kerneldump ユーティリティから送信されたクラッシュ情報を表示するには、Cisco Unified Real-Time Monitoring Tool またはコマンドライン インターフェイス（CLI）を使用します。Cisco Unified Real-Time Monitoring Tool を使用して netdump ログを収集するには、[トレースおよびロ

グ セントラル（Trace & Log Central）] の [ファイルの収集（Collect Files）] オプションを選択します。[システム サービス/アプリケーションの選択（Select System Services/Applications）] タブで、[Kerneldump ログ（Kerneldump logs）] チェックボックスをオンにします。Cisco Unified Real-Time Monitoring Tool を使用したファイルの収集の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

CLI を使用して kerneldump ログを収集するには、クラッシュ ディレクトリのファイルに対して「「file」」CLI コマンドを使用します。これらは 「activelog」 のパーティションの下にあります。ログ ファイル名は、kerneldump クライアントの IP アドレスで始まり、ファイルが作成された日付で終わります。ファイル コマンドの詳細については、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』を参照してください。

Kerneldump ユーティリティの有効化

次の手順を利用して Kerneldump ユーティリティをイネーブル化します。カーネル クラッシュが発生した場合、ユーティリティは、クラッシュの収集とダンプのメカニズムを提供します。ローカル サーバまたは外部サーバにログをダンプするユーティリティを設定できます。

手順

ステップ 1 コマンドライン インターフェイスにログインします。

ステップ 2 次のいずれかを実行します。

- ローカル サーバ上のカーネル クラッシュをダンプするには、`utils os kernelcrash enable` CLI コマンドを実行します。
- 外部サーバにカーネル クラッシュをダンプするには、外部サーバの IP アドレスを指定して `utils os kerneldump ssh enable <ip_address>` CLI コマンドを実行します。

ステップ 3 サーバをリブートします。

例

（注） kerneldumpユーティリティを無効にする必要がある場合、`utils os kernelcrash disable` CLIコマンドを実行してローカル サーバのコア ダンプを無効にし、`utils os kerneldump ssh disable <ip_address>`CLIコマンドを実行して外部サーバ上のユーティリティを無効にします。

次のタスク

コア ダンプの指示に従ってリアルタイム モニタリング ツールで電子メール アラートを設定します。詳細については、コア ダンプの電子メール アラートの有効化 （10 ページ）を参照してください。

kerneldump ユーティリティおよびトラブルシューティングについては、『*Troubleshooting Guide for Cisco Unified Communications Manager*』を参照してください。

コア ダンプの電子メール アラートの有効化

コア ダンプが発生するたびに管理者に電子メールを送信するようにリアルタイム モニタリング ツールを設定するには、次の手順を使用します。

手順

ステップ 1 **[システム（System）] > [ツール（Tools）] > [アラート セントラル）Alert Central）]** の順に選択します。

ステップ 2 [CoreDumpFileFound] アラートを右クリックし、[アラート/プロパティの設定（Set Alert/Properties）] を選択します。

ステップ 3 ウィザードの指示に従って優先条件を設定します。

a) [アラート プロパティ：電子メール通知（Alert Properties: Email Notification）] ポップアップで、[電子メールの有効化（Enable Email）] がオンになっていることを確認し、[設定（Configure）] をクリックしてデフォルトのアラート アクションを設定します。これにより管理者に電子メールが送信されます。

b) プロンプトに従って、受信者電子メール アドレスを [追加（Add）]します。このアラートがトリガーされると、デフォルトのアクションは、このアドレスへの電子メールの送信になります。

c) **[保存（Save）]** をクリックします。

ステップ 4 デフォルトの電子メール サーバを設定します。

a) **[システム（System）] > [ツール（Tools）] > [アラート（Alert）] > [電子メール サーバの設定（Config Email Server）]** の順に選択します。

b) 電子メール サーバの設定を入力します。

c) [OK] をクリックします。

ネットワーク管理

Unified Communications Manager のリモート有用性には、ネットワーク管理ツールを使用します。

- システム ログ管理

- Cisco Discovery Protocol のサポート
- 簡易ネットワーク管理プロトコル（SNMP）のサポート

これらのネットワーク管理ツールの詳細については、それぞれの項に記載された URL にあるマニュアルを参照してください。

システム ログ管理

Resource Manager Essentials（RME）にパッケージされている Cisco Syslog Analysis は、他のネットワーク管理システムにも適応可能ですが、シスコ デバイスから送信される Syslog メッセージの管理に最適な方法を提供します。

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

これら 2 つの Cisco アプリケーションが連動し、Cisco Unified Communication ソリューションの集中型システム ログ サービスを提供します。

RME 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/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml

Cisco Discovery Protocol のサポート

Cisco Discovery Protocol がサポートされているため、Unified Communications Manager サーバの検出および管理が可能です。

RME 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/en/US/products/sw/cscowork/ps2073/products_tech_note09186a00800a7275.shtml

簡易ネットワーク管理プロトコル（SNMP）のサポート

ネットワーク管理システム（NMS）では、業界標準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が交換されます。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のパフォーマンスを管理し、ネットワークの問題を検出および解決し、ネットワークの拡張計画を立てることができます。

SNMP管理のネットワークは、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ています。

- 管理対象デバイスは、SNMPエージェントを含み、管理対象ネットワークに存在するネットワーク ノードを指します。管理対象デバイスには管理情報が収集および格納され、その情報は SNMP を使用することによって利用可能になります。

- 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存在します。エージェントには、管理情報のローカルな知識が蓄積され、SNMP と互換性のある形式に変換されます。
- 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が実行されるコンピュータで構成されています。NMS では、管理対象デバイスをモニタおよび制御するアプリケーションが実行されます。ネットワーク管理に必要な処理とメモリリソースの大部分は、NMS によって提供されます。次の NMS は Unified Communications Manager と互換性を持っています。
  - CiscoWorks Common Services Software
  - HP OpenView
  - SNMP および Unified Communications Manager 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

スニファ トレース

通常、スニファ トレースは、VLAN または問題の情報が含まれるポート（CatOS、Cat6K-IOS、XL-IOS）にまたがるように設定された Catalyst ポートに、ラップトップやその他のスニファ搭載デバイスを接続することによって収集します。利用可能なポートが空いていない場合は、スニファ搭載デバイスを、スイッチとデバイスの間に挿入されるハブに接続します。

ヒント　TAC のエンジニアがトレースを読解しやすいように、TAC で広く使用されている Sniffer Pro ソフトウェアを使用することを推奨します。

IP 電話、ゲートウェイ、Unified Communications Manager など、関連するすべての機器の IP/MAC アドレスを利用可能にしておいてください。

デバッグ

debug 特権 EXEC コマンドの出力は、プロトコルのステータスおよびネットワーク アクティビティ全般に関する、さまざまなネットワーク間イベントについての診断情報を提供します。

端末エミュレータ ソフトウェア（ハイパーターミナルなど）を設定し、デバッグ出力をファイルに取得できるようにしてください。ハイパーターミナルで、[転送（Transfer）] をクリックし、[テキストのキャプチャ（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 デバッグを実行する前に、
service timestamps debug datetime msec がゲートウェイでグローバルに設定されていることを確認してください。

（注） 運用時間中にライブ環境でデバッグを収集することは避けてください。

運用時間外にデバッグを収集することを推奨します。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、コンソール ポート（デフォルトの **logging console**）またはバッファ（**logging buffer**）でデバッグを直接収集します。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** コマンドまたは **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 Secure Telnet

シスコ サービス エンジニア（CSE）は、Cisco Secure Telnet を使用して、サイト上の Unified Communications Manager ノードに対して透過的にファイアウォール アクセスを実行できます。Cisco Secure Telnet は、強力な暗号化を使用して、シスコ内の特別な Telnet クライアントを、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、Unified Communications Manager 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。サイトに、このプロセスの開始を支援するネットワーク管理者を配置する必要があります。

パケット キャプチャ

ここでは、パケット キャプチャについて説明します。

関連トピック

パケット キャプチャの概要 （14 ページ）
パケット キャプチャの設定チェックリスト （14 ページ）
Standard Packet Sniffer Users アクセス コントロールグループへのエンド ユーザの追加 （15 ページ）
パケット キャプチャのサービス パラメータの設定 （16 ページ）
[電話の設定（Phone Configuration）] ウィンドウでのパケット キャプチャの設定 （16 ページ）
[ゲートウェイの設定（Gateway Configuration）] ウィンドウおよび [トランクの設定（Trunk Configuration）] ウィンドウでのパケット キャプチャの設定 （18 ページ）

パケット キャプチャの構成設定 （19 ページ）
キャプチャしたパケットの分析 （21 ページ）

パケット キャプチャの概要

メディアや TCP パケットをスニフィングするサードパーティ製トラブルシューティング ツールは、暗号化を有効にした後は機能しません。このため、問題が発生した場合は、Unified Communications Manager を使用して次のタスクを実行する必要があります。

- Unified Communications Manager とデバイス（Cisco Unified IP Phone（SIP および SCCP）、Cisco IOS MGCP ゲートウェイ、H.323 ゲートウェイ、H.323/H.245/H.225 トランク、または SIP トランク）との間で交換されるメッセージのパケットの分析。
- デバイス間の Secure Real Time Protocol（SRTP）パケットのキャプチャ。
- メッセージからのメディア暗号キー情報の抽出、およびデバイス間のメディアの復号化。

ヒント　このタスクを複数のデバイスに対して同時に実行すると、CPU使用率が高くなり、コール処理が中断される可能性があります。このタスクは、コール処理が中断される危険性が最も少ないときに実行することを強く推奨します。

詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

パケット キャプチャの設定チェックリスト

必要なデータを抽出し、分析するには、次の作業を実行します。

手順

1. エンド ユーザを Standard Packet Sniffer Users グループに追加します。
2. Unified Communications Manager Administration の [サービスパラメータ設定（Service Parameter Configuration）] ウィンドウで、パケット キャプチャのサービス パラメータを設定します。たとえば、Packet Capture Enable サービス パラメータを設定します。
3. [電話の設定（Phone Configuration）]、[ゲートウェイの設定（Gateway Configuration）]、または [トランクの設定（Trunk Configuration）] の各ウィンドウで、デバイスごとのパケット キャプチャの設定を行います。

（注）　パケット キャプチャは、複数のデバイスで同時にはイネーブルにしないことを強く推奨します。このタスクによって、ネットワークで使用されている CPU の使用率が上昇する可能性があるためです。

4. 該当するデバイス間でスニファ トレースを使用して、SRTPパケットをキャプチャします。使用しているスニファ トレースツールに対応したマニュアルを参照してください。
5. パケットをキャプチャしたら、Packet Capture Enable サービス パラメータを False に設定します。
6. パケットの分析に必要なファイルを収集します。
7. Cisco Technical Assistance Center（TAC）がパケットを分析します。このタスクについては、TAC に直接お問い合わせください。

関連トピック

Standard Packet Sniffer Users アクセス コントロールグループへのエンド ユーザの追加 （15 ページ）
キャプチャしたパケットの分析 （21 ページ）
[ゲートウェイの設定（Gateway Configuration）] ウィンドウおよび [トランクの設定（Trunk Configuration）] ウィンドウでのパケット キャプチャの設定 （18 ページ）
[電話の設定（Phone Configuration）] ウィンドウでのパケット キャプチャの設定 （16 ページ）
パケット キャプチャのサービス パラメータの設定 （16 ページ）
パケット キャプチャの構成設定 （19 ページ）

Standard Packet Sniffer Users アクセス コントロールグループへのエンド ユーザの追加

Standard Packet Sniffer Users グループに所属するユーザは、パケット キャプチャをサポートしているデバイスについて、パケット キャプチャ モードとパケット キャプチャ時間を設定できます。ユーザが Standard Packet Sniffer Users アクセス コントロール グループに含まれていない場合、そのユーザはパケット キャプチャを開始できません。

次の手順では、エンド ユーザを Standard Packet Sniffer アクセス コントロール グループに追加する方法について説明します。ここでは、『Cisco Unified Communications Manager アドミニストレーション ガイド』の説明に従って、Unified Communications Manager Administration でエンド ユーザが設定済みであることを前提としています。

手順

1. 『*Administration Guide for Cisco Unified Communications Manager*』の説明に従ってアクセス コントロール グループを検索します。
2. [検索/リスト（Find/List）] ウィンドウが表示されたら、[標準パケット スニファ ユーザ（Standard Packet Sniffer Users）] リンクをクリックします。
3. [グループにユーザを追加（Add Users to Group）] ボタンをクリックします。
4. 『*Administration Guide for Cisco Unified Communications Manager*』の説明に従ってエンドユーザを追加します。

5. ユーザを追加したら、[保存（Save）] をクリックします。

パケット キャプチャのサービス パラメータの設定

パケット キャプチャのパラメータを設定するには、次の手順を実行します。

手順

1. [Cisco Unified Communications Manager Administration] で、**[System]** > **[Service Parameters]** を選択します。
2. [サーバ（Server）] ドロップダウン リスト ボックスで、Cisco CallManager サービスをアクティブにした Active サーバを選択します。
3. [サービス（Service）] ドロップダウン リスト ボックスで、[Cisco CallManager（アクティブ）（Cisco CallManager (Active)）] サービスを選択します。
4. [TLS パケット キャプチャ設定（TLS Packet Capturing Configuration）] ペインまでスクロールして、パケット キャプチャを設定します。

ヒント　サービス パラメータについては、ウィンドウに表示されているパラメータ名または疑問符をクリックしてください。

（注）　パケット キャプチャを実行するには、Packet Capture Enable サービス パラメータを True に設定する必要があります。

5. 変更内容を有効にするには、[保存（Save）] をクリックします。
6. パケット キャプチャの設定を続行できます。

関連トピック

[ゲートウェイの設定（Gateway Configuration）] ウィンドウおよび [トランクの設定（Trunk Configuration）] ウィンドウでのパケット キャプチャの設定 （18 ページ）
[電話の設定（Phone Configuration）] ウィンドウでのパケット キャプチャの設定 （16 ページ）

[電話の設定（Phone Configuration）] ウィンドウでのパケット キャプチャの設定

[サービスパラメータ（Service Parameter）] ウィンドウでパケット キャプチャを有効にしたら、Unified Communications Manager Administration の [電話の設定（Phone Configuration）] ウィンドウで、デバイスごとにパケット キャプチャを設定できます。

電話機ごとに、パケットキャプチャをイネーブルまたはディセーブルにします。パケットキャプチャのデフォルト設定は、None です。

注意 パケットキャプチャは、複数の電話機で同時にはイネーブルにしないことを強く推奨します。このタスクによって、ネットワークで使用されている CPU の使用率が上昇する可能性があるためです。

パケットをキャプチャしない場合、またはタスクを完了した場合は、Packet Capture Enable サービス パラメータを False に設定します。

電話機のパケット キャプチャを設定するには、次の手順を実行します。

手順

1. パケット キャプチャを設定する前に、パケット キャプチャの設定に関するトピックを参照してください。
2. 『*System Configuration Guide for Cisco Unified Communications Manager*』の説明に従って、SIP または SCCP 電話を検索します。
3. [電話の設定（Phone Configuration）] ウィンドウが表示されたら、「パケット キャプチャの設定値」の説明に従って、トラブルシューティングの設定を行います。
4. 設定が完了したら、[保存（Save）] をクリックします。
5. [リセット（Reset）] ダイアログボックスで、[OK] をクリックします。

ヒント Unified Communications Manager Administration からデバイスをリセットするように求められますが、パケットをキャプチャするためにデバイスをリセットする必要はありません。

この他の手順

該当するデバイス間でスニファ トレースを使用して、SRTP パケットをキャプチャします。

パケットをキャプチャしたら、Packet Capture Enable サービス パラメータを False に設定します。

関連トピック

キャプチャしたパケットの分析 （21 ページ）
パケット キャプチャの設定チェックリスト （14 ページ）

[ゲートウェイの設定（Gateway Configuration）] ウィンドウおよび [トランクの設定（Trunk Configuration）] ウィンドウでのパケット キャプチャの設定

次のゲートウェイおよびトランクは、Unified Communications Manager Administration でのパケット キャプチャをサポートしています。

- Cisco IOS MGCP ゲートウェイ
- H.323 ゲートウェイ
- H.323/H.245/H.225 トランク
- SIP トランク

ヒント　パケット キャプチャは、複数のデバイスで同時にはイネーブルにしないことを強く推奨します。このタスクによって、ネットワークで使用されている CPU の使用率が上昇する可能性があるためです。

パケットをキャプチャしない場合、またはタスクを完了した場合は、Packet Capture Enable サービス パラメータを False に設定します。

[ゲートウェイの設定（Gateway Configuration）] ウィンドウまたは [トランクの設定（Trunk Configuration）] ウィンドウでパケット キャプチャの設定を行うには、次の手順を実行します。

手順

1. パケット キャプチャを設定する前に、パケット キャプチャの設定に関するトピックを参照してください。
2. 次のいずれかの作業を実行します。
   - 『*System Configuration Guide for Cisco Unified Communications Manager*』の説明に従って、Cisco IOS MGCP ゲートウェイを検索します。
   - 『*System Configuration Guide for Cisco Unified Communications Manager*』の説明に従って、H.323 ゲートウェイを検索します。
   - 『*System Configuration Guide for Cisco Unified Communications Manager*』の説明に従って、H.323/H.245/H.225 トランクを検索します。
   - 『*System Configuration Guide for Cisco Unified Communications Manager*』の説明に従って、SIP トランクを検索します。
3. 設定ウィンドウが表示されたら、[パケット キャプチャ モード（Packet Capture Mode）] と [パケット キャプチャ時間（Packet Capture Duration）] の設定値を確認します。

ヒント Cisco IOS MGCP ゲートウェイが見つかった場合は、『*Cisco Unified Communications Manager* アドミニストレーション ガイド』の説明に従って、Cisco IOS MGCP ゲートウェイ用のポートが設定されていることを確認します。Cisco IOS MGCP ゲートウェイのパケット キャプチャ設定値は、エンドポイント識別子の [ゲートウェイの設定（Gateway Configuration）] ウィンドウに表示されます。このウィンドウにアクセスするには、音声インターフェイス カードのエンドポイント識別子をクリックします。

4. 「パケット キャプチャの設定値」の説明に従って、トラブルシューティングを設定します。
5. パケット キャプチャを設定したら、[保存（Save）] をクリックします。
6. [リセット（Reset）] ダイアログボックスで、[OK] をクリックします。

ヒント Unified Communications Manager Administration からデバイスをリセットするように求められますが、パケットをキャプチャするためにデバイスをリセットする必要はありません。

この他の手順

該当するデバイス間でスニファ トレースを使用して、SRTP パケットをキャプチャします。

パケットをキャプチャしたら、Packet Capture Enable サービス パラメータを False に設定します。

関連トピック

キャプチャしたパケットの分析 （21 ページ）
パケット キャプチャの設定チェックリスト （14 ページ）

パケット キャプチャの構成設定

次の表に、ゲートウェイ、トランク、および電話機にパケット キャプチャを設定する際の [パケット キャプチャ モード（Packet Capture Mode）] 設定と [パケット キャプチャ時間（Packet Capture Duration）] 設定について説明します。

設定	説明
パケット キャプチャ モード（Packet Capture Mode）	この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケットキャプチャを実行すると、CPU の使用率が上昇して、コール処理が妨げられる可能性があります。ドロップダウン リスト ボックスで、次のいずれかのオプションを選択します。 • [なし（None）]：このオプションは、パケット キャプチャが発生しないことを示します（デフォルト設定）。 パケットキャプチャが完了すると、Unified Communications Manager は [パケットキャプチャモード（Packet Capture Mode）] を [なし（None）] に設定します。 • [**バッチ処理モード（Batch Processing Mode**）]：Unified Communications Manager が、復号化されたメッセージや暗号化されていないメッセージをファイルに書き込み、システムが各ファイルを暗号化します。システムでは、毎日新しいファイルが新しい暗号キーを使用して作成されます。Unified Communications Manager はファイルを 7 日間保存し、さらにファイルを暗号化するキーを安全な場所に保存します。Unified Communications Manager は、PktCap 仮想ディレクトリにファイルを保存します。1 つのファイルの中に、タイムスタンプ、送信元 IP アドレス、送信元 IP ポート、宛先 IP アドレス、パケットのプロトコル、メッセージの長さ、およびメッセージが保持されます。TAC のデバッグ ツールでは、HTTPS、管理者のユーザ名とパスワード、および指定された日付を使用して、キャプチャされたパケットを保持している暗号化済みファイルを 1 つだけ要求します。同様にこのツールでは、暗号化ファイルを復号化するためのキー情報を要求します。 **ヒント** TAC にお問い合わせいただく前に、該当するデバイス間でスニファ トレースを使用して、SRTP パケットをキャプチャする必要があります。

設定	説明
パケット キャプチャ時間（Packet Capture Duration）	この設定値は、暗号化のトラブルシューティングを行う場合にだけ使用します。パケット キャプチャを実行すると、CPU の使用率が上昇して、コール処理が妨げられる可能性があります。 このフィールドには、1 つのパケット キャプチャ セッションに割り当てる時間の上限（分単位）を指定します。デフォルト設定は0で、範囲は 0 ～ 300 分です。 パケット キャプチャを開始するには、このフィールドに0以外の値を入力します。パケット キャプチャが完了すると、値 0 が表示されます。

関連トピック

[ゲートウェイの設定（Gateway Configuration）] ウィンドウおよび [トランクの設定（Trunk Configuration）] ウィンドウでのパケット キャプチャの設定 （18 ページ）
[電話の設定（Phone Configuration）] ウィンドウでのパケット キャプチャの設定 （16 ページ）

キャプチャしたパケットの分析

Cisco Technical Assistance Center（TAC）は、デバッグ ツールを使用してパケットを分析します。TACにお問い合わせいただく前に、該当するデバイス間でスニファ トレースを使用して、SRTP パケットをキャプチャしてください。次の情報を収集したら、TAC に直接お問い合わせください。

- パケット キャプチャ ファイル：**https://<IP アドレスまたはサーバ名>/pktCap/pktCap.jsp?file=mm-dd-yyyy.pkt**。サーバを参照し、西暦年と日付（mm-dd-yyyy）別のパケット キャプチャ ファイルを見つけます。
- ファイルのキー：**https://<IP アドレスまたはサーバ名>/pktCap/pktCap.jsp?key=mm-dd-yyyy.pkt**。サーバを参照し、西暦年と日付（mm-dd-yyyy）別のキーを見つけます。
- Standard Packet Sniffer Users グループに所属しているエンド ユーザのユーザ名とパスワード。

詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

一般的なトラブルシューティングのタスク、ツール、およびコマンド

この項では、ルート アクセスが無効になっている Unified Communications Manager サーバのトラブルシューティングに役立つコマンドおよびユーティリティのクイック リファレンスを提供します。次の表に、システムのさまざまな問題をトラブルシューティングするための情報収集に使用できる CLI コマンドと GUI をまとめます。

表 *3 : CLI* コマンドと *GUI* 選択のまとめ

情報	Linux コマンド	サービスアビリティの GUI ツール	CLI コマンド
CPU 使用率	top	RTMT [表示（View）] タブに移動し、**[サーバ（Server）] > [CPU とメモリ（CPU and Memory）]** を選択	プロセッサ CPU 使用率： show perf query class Processor すべてのプロセスのプロセス CPU 使用率： show perf query counter Process「% CPU Time」 個々のプロセス カウンタの詳細（CPU 使用率を含む） show perf query instance <Process task_name>
プロセスの状態	ps	RTMT [表示（View）] タブに移動し、**[サーバ（Server）]>[プロセス（Process）]** を選択	show perf query counter Process「Process Status」
ディスク使用量	df/du	RTMT [表示（View）] タブに移動し、**[サーバ（Server）] > [ディスク使用量（Disk Usage）]** を選択	show perf query counter Partition「% Used」 または show perf query class Partition
メモリ	free	RTMT [表示（View）] タブに移動し、**[サーバ（Server）] > [CPU とメモリ（CPU and Memory）]** を選択	show perf query class Memory
ネットワーク ステータス	netstats		show network status

情報	Linux コマンド	サービスアビリティの GUI ツール	CLI コマンド
サーバのリブート	reboot	サーバの [プラットフォーム（Platform）] Web ページにログイン **[サーバ（Server）]>[現在のバージョン（Current Version）]** に移動	utils system restart
トレース/ログの収集	Sftp、ftp	RTMT [ツール（Tools）] タブに移動し、**[トレース（Trace）]>[トレースおよびログ セントラル（Trace & Log Central）]** を選択	ファイルのリスト：file list ファイルのダウンロード：file get ファイルの表示：file view

次の表に、一般的な問題と、そのトラブルシューティングに使用するツールのリストを示します。

表 *4 : CLI* コマンドおよび *GUI* 選択オプションによる一般的な問題のトラブルシューティング

タスク	GUI ツール	CLI コマンド
データベースにアクセスする	none	admin としてログインし、次のいずれかの **show** コマンドを使用します。 • show tech database • show tech dbinuse • show tech dbschema • show tech devdefaults • show tech gateway • show tech locales • show tech notify • show tech procedures • show tech routepatterns • show tech routeplan • show tech systables • show tech table • show tech triggers • show tech version • show tech params* SQL コマンドを実行するには、**run** コマンドを使用します。 • run sql <sql command>

タスク	GUI ツール	CLI コマンド
ディスクの空き容量を増やす （注） Log パーティションにあるファイルだけ、削除できます。	RTMT クライアントアプリケーションを使用して、[ツール（Tools）] タブに移動し、**[トレースおよびログ セントラル（Trace & Log Central）]** > **[ファイルの収集（Collect Files）]** を選択します。 収集するファイルの選択基準を選択し、[ファイルの削除（Delete Files）] オプションのチェックボックスをオンにします。この操作を実行すると、ファイルが PC にダウンロードされ、Unified Communications Manager サーバ上のファイルは削除されます。	file delete
コア ファイルを表示する	コア ファイルは表示できませんが、RTMT アプリケーションを使用して **[Trace & Log Central）]** > **[クラッシュ ダンプの収集（Collect Crash Dump）]** を選択すると、コアファイルをダウンロードできます。	utils core [options]
Unified Communications Manager サーバをリブートする	サーバの [プラットフォーム（Platform）] ページにログインし、**[リスタート（Restart）]** > **[現在のバージョン（Current Version）]** に移動します。	utils system restart
トレースのデバッグレベルを変更する	`https://<server_ipaddress>:8443/ccmservice//` で Cisco Unity Connection Serviceability Administration にログインして、**[トレース（Trace）]** > **[設定（Configuration）]** を選択します。	set trace enable [Detailed, Significant, Error, Arbitrary, Entry_exit, State_Transition, Special] [syslogmib, cdpmib, dbl, dbnotify]
ネットワークのステータスを表示する	none	show network status

トラブルシューティングのヒント

次の各ヒントは、Unified Communications Manager のトラブルシューティングに役立ちます。

ヒント　既知の問題については、Unified Communications Manager のリリース ノートを参照してください。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。

Unified Communications Manager の各ログは、ローカルでファイルをトレースします。電話機またはゲートウェイが特定の Unified Communications Manager に登録されている場合、その Unified Communications Manager でコールが開始されると、コール処理はそこで実行されます。問題をデバッグするには、その Unified Communications Manager 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かかわらず、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 Unified Communications Manager 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確認します。

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確認していると、TAC が問題を迅速に特定するのに役立ちます。

Cisco Unified IP Phone 79xx の電話機統計情報は、**i** または **?** ボタンをアクティブ コール中に 2 回押すと取得できます。

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 Unified Communications Manager 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 **[表示（View）]** > **[更新（Refresh）]** を選択し、ファイルの日付と時刻を確認することです。

システム履歴ログ

システム履歴ログを使用すると、システムの初期インストール、システムのアップグレード、Cisco オプションのインストール、DRS バックアップと DRS 復元、バージョン切り替えとリブート履歴などの情報の概要を中央からすばやく把握できます。

関連トピック

システム履歴ログの概要 （26 ページ）
システム履歴ログのフィールド （27 ページ）
システム履歴ログへのアクセス （28 ページ）

システム履歴ログの概要

システム履歴ログは、**system-history.log** という単純な ASCII ファイルとして保管され、そのデータはデータベース内には保持されません。サイズが膨大ではないため、ローテーションされることはありません。

システム履歴ファイルには、次の機能があります。

- サーバ上のソフトウェアの初期インストールを記録します。
- ソフトウェアの各アップデート（Cisco オプション ファイルおよびパッチ）の成功、失敗、またはキャンセルを記録します。
- 実行される各 DRS バックアップと復元を記録します。
- CLI または GUI によって発行されるバージョン切り替えの各呼び出しを記録します。
- CLI または GUI によって発行される再起動およびシャットダウンの各呼び出しを記録します。
- システムの各ブートを記録します。再起動エントリまたはシャットダウン エントリと関連付けられていない場合のブートは、手動リブート、電源サイクル、またはカーネル パニックの結果として発生したものです。

- 初期インストール以降、または機能が利用可能になって以降のシステム履歴を単一ファイルに保持します。
- インストール フォルダに存在します。**file** コマンドか、または Real Time Monitoring Tool（RTMT）を使用して、CLI からログにアクセスできます。

システム履歴ログのフィールド

ログには、製品名、製品バージョン、およびカーネルイメージに関する情報を含む、次のような共通のヘッダーが表示されます。

==========

Product Name - Cisco Unified Communications Manager

Product Version - 7.1.0.39000-9023

Kernel Image - 2.6.9-67.EL

==========

システム履歴ログの各エントリには、次のようなフィールドがあります。

timestamp userid action description start/result

システム履歴ログのフィールドには、次のような値が含まれます。

- *timestamp*：サーバ上のローカルな日付と時刻が *mm/dd/yyyy hh:mm:ss* の形式で表示されます。
- *userid*：アクションを呼び出したユーザの名前が表示されます。
- *action*：次のいずれかのアクションが表示されます。
  - インストール
  - Windows アップグレード
  - インストール時のアップグレード
  - アップグレード
  - Cisco オプションのインストール
  - バージョン切り替え
  - システム再起動
  - Shutdown
  - ブート
  - DRS バックアップ
  - DRS 復元
- *description*：次のいずれかのメッセージが表示されます。

- *Version*：基本インストール、Windows アップグレード、インストール時のアップグレード、アップグレードの各アクションが表示されます。
- *Cisco Option file name*：Cisco オプションのインストールのアクションが表示されます。
- *Timestamp*：DRS バックアップと DRS 復元の各アクションが表示されます。
- *Active version to inactive version*：バージョン切り替えのアクションが表示されます。
- *Active version*：システム再起動、シャットダウン、およびブートの各アクションが表示されます。

- *result*：次の結果が表示されます。
  - 開始
  - 成功または失敗
  - キャンセル

次に、システム履歴ログの例を示します。

```
admin:file dump install system-history.log=====================================
 Product Name - Cisco Unified Communications Manager Product Version -
6.1.2.9901-117 Kernel Image - 2.4.21-47.EL.cs.3BOOT
===================================== 07/25/2008 14:20:06 | root: Install
6.1.2.9901-117 Start 07/25/2008 15:05:37 | root: Install 6.1.2.9901-117 Success
 07/25/2008 15:05:38 | root: Boot 6.1.2.9901-117 Start 07/30/2008 10:08:56 |
root: Upgrade 6.1.2.9901-126 Start 07/30/2008 10:46:31 | root: Upgrade
6.1.2.9901-126 Success 07/30/2008 10:46:43 | root: Switch Version 6.1.2.9901-117
 to 6.1.2.9901-126 Start 07/30/2008 10:48:39 | root: Switch Version
6.1.2.9901-117 to 6.1.2.9901-126 Success 07/30/2008 10:48:39 | root: Restart
6.1.2.9901-126 Start 07/30/2008 10:51:27 | root: Boot 6.1.2.9901-126 Start
08/01/2008 16:29:31 | root: Restart 6.1.2.9901-126 Start 08/01/2008 16:32:31
| root: Boot 6.1.2.9901-126 Start
```

システム履歴ログへのアクセス

システム履歴ログにアクセスするには、CLI または RTMT を使用できます。

CLI の使用

次のように CLI の **file** コマンドを使用すると、システム履歴ログにアクセスできます。

- **file view install system-history.log**
- **file get install system-history.log**

CLI **ファイル** コマンドの詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions*』を参照してください。

RTMT の使用

RTMT を使用してシステム履歴ログにアクセスすることもできます。[Trace and Log Central] タブで、[インストール ログの収集（Collect Install Logs）] を選択します。

RTMT の使用の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

監査ロギング

集中型の監査ロギングにより、Unified Communications Manager システムに対する設定変更は個別の監査ログ ファイルに記録されます。監査イベントは、記録する必要があるすべてのイベントを指します。監査イベントは次の Unified Communications Manager コンポーネントで生成されます。

- Unified Communications Manager Administration
- Cisco Unified Serviceability
- Unified Communications Manager CDR Analysis and Reporting
- Cisco Unified Real-Time Monitoring Tool
- Cisco Unified Communications Operating System
- Disaster Recovery System
- データベース
- コマンドライン インターフェイス
- Remote Support Account Enabled（テクニカル サポート チームによって発行される CLI コマンド）

Cisco Business Edition 5000 では、次の Cisco Unity Connection コンポーネントによっても監査イベントが生成されます。

- Cisco Unity Connection Administration
- Cisco Personal Communications Assistant（Cisco PCA）
- Cisco Unity Connection Serviceability
- Representational State Transfer（REST）API を使用する Cisco Unity Connection クライアント

次に、監査イベントの例を示します。

```
CCM_TOMCAT-GENERIC-3-AuditEventGenerated: Audit Event Generated
UserID:CCMAdministrator Client IP Address:172.19.240.207 Severity:3
EventType:ServiceStatusUpdated ResourceAccessed: CCMService
EventStatus:Successful Description: Call Manager Service status is stopped App
 ID:Cisco Tomcat Cluster ID:StandAloneCluster Node ID:sa-cm1-3
```

監査イベントに関する情報が含まれている監査ログは、共通のパーティションに書き込まれます。これらの監査ログのパージは、トレース ファイルと同様に、Log Partition Monitor（LPM）によって管理されます。デフォルトでは、LPM によって監査ログがパージされますが、監査ユーザは Cisco Unified Serviceability の [監査ユーザ設定（Audit User Configuration）] ウィンドウからこの設定を変更できます。共通パーティションのディスク使用量がしきい値を超えると、LPM によってアラートが送信されますが、アラートには、ディスクが監査ログまたはトレース ファイルによっていっぱいであるかどうかに関する情報は含まれていません。

ヒント 監査ロギングをサポートするネットワーク サービスである Cisco Audit Event Service は、Cisco Unified Serviceability のコントロール センターのネットワーク サービスに表示されます。監査ログへの書き込みが行われない場合は、Cisco Unified Serviceability で **[ツール（Tools）] > [コントロール センターのネットワーク サービス（Control Center-Network Services）]** を選択し、このサービスを停止してから開始します。

すべての監査ログは、Cisco Unified Real-Time Monitoring Tool の Trace and Log Central から収集、表示、および削除します。RTMT の Trace and Log Central で監査ログにアクセスします。**[システム（System）] > [リアルタイム トレース（Real-Time Trace）] > [監査ログ（Audit Logs）] > [ノード（Nodes）]** に移動します。ノードを選択したら、別のウィンドウに **[システム（System）] > [Cisco 監査ログ（Cisco Audit Logs）]** が表示されます。

RTMT には、次のタイプの監査ログが表示されます。

- アプリケーション ログ
- データベース ログ
- オペレーティング システム ログ
- リモート SupportAccEnabled ログ

アプリケーション ログ

RTMT の AuditApp フォルダに表示されるアプリケーション監査ログには、Unified Communications Manager Administration、Cisco Unified Serviceability、CLI、Cisco Unified リアルタイム監視ツール（RTMT）、ディザスタ リカバリ システム、および Cisco Unified CDR Analysis and Reporting（CAR）の設定変更が記録されます。Cisco Business Edition 5000 の場合、アプリケーション監査ログには Cisco Unity Connection Administration、Cisco Personal Communications Assistant（Cisco PCA）、Cisco Unity Connection Serviceability、および Representational State Transfer（REST）API を使用するクライアントに対する変更も記録されます。

アプリケーション ログはデフォルトでイネーブルになっていますが、Cisco Unified Serviceability で **[ツール（Tools）] > [監査ログ設定（Audit Log Configuration）]** を選択することによって設定を変更できます。設定可能な監査ログの設定については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

Cisco Unified Serviceability で監査ログがディセーブルになると、新しい監査ログは作成されません。

ヒント 監査のロールを割り当てられたユーザだけが監査ログの設定を変更する権限を持っています。新規のインストールまたはアップグレード後には、デフォルトで CCMAdministrator に監査のロールが割り当てられます。CCMAdministrator は、監査のために作成した新規ユーザを「「Standard Audit Users」」グループに割り当てることができます。その後、CCMAdministrator を監査ユーザ グループから削除できます。「「Standard Audit Log Configuration」」ロールには、監査ログを削除する権限と、Cisco Unified Real-Time Monitoring Tool、Trace Collection Tool、RTMT Alert Configuration、[コントロール センターのネットワーク サービス（Control Center - Network Services）] ウィンドウ、RTMT Profile Saving、[監査の設定（Audit Configuration）] ウィンドウ、および Audit Traces という新規リソースへの読み取り/更新権限が与えられます。Cisco Business Edition 5000 の Cisco Unity Connection の場合、インストール時に作成されたアプリケーション管理アカウントは、Audit Administrator ロールに割り当てられます。このアカウントは、他の管理者ユーザをこのロールに割り当てることができます。

Unified Communications Manager では、1 つのアプリケーション監査ログ ファイルが作成され、設定済みの最大ファイル サイズに到達すると、そのファイルが閉じられて新しいアプリケーション監査ログ ファイルが作成されます。システムでログ ファイルのローテーションが指定されている場合は、設定された数のファイルが Unified Communications Manager によって保存されます。ログ イベントの一部は、RTMT SyslogViewer を使用して表示できます。

Unified Communications Manager Administration では、次のイベントが記録されます。

- ユーザのログイン/ログアウト。
- ユーザのロール メンバーシップの更新（ユーザの追加、ユーザの削除、またはユーザのロールの更新）。
- ロールの更新（新しいロールの追加、削除、または更新）。
- デバイスの更新（電話機およびゲートウェイ）。
- サーバ設定の更新（アラームまたはトレースの設定、サービス パラメータ、エンタープライズ パラメータ、IP アドレス、ホスト名、イーサネット設定の変更、および Unified Communications Manager サーバの追加または削除）。

Cisco Unified Serviceability では、次のイベントが記録されます。

- Serviceability ウィンドウからのサービスのアクティブ化、非アクティブ化、開始、または停止。
- トレース設定およびアラーム設定の変更。
- SNMP 設定の変更。
- CDR 管理の変更。
- Serviceability レポートのアーカイブのレポートの参照。このログはレポーター ノードで表示します。

RTMT では、次のイベントが監査イベント アラームとともに記録されます。

- アラートの設定。
- アラートの中断。
- 電子メールの設定。
- ノード アラート ステータスの設定。
- アラートの追加。
- アラートの追加アクション。
- アラートのクリア。
- アラートのイネーブル化。
- アラートの削除アクション。
- アラートの削除。

Unified Communications Manager CDR Analysis and Reporting では、次のイベントが記録されます。

- CDR Loader のスケジュール。
- 日次、週次、月次のユーザ レポート、システム レポート、およびデバイス レポートのスケジュール。
- メール パラメータの設定。
- ダイヤル プランの設定。
- ゲートウェイの設定。
- システム プリファレンスの設定。
- 自動消去の設定。
- 接続時間、時刻、および音声品質の評価エンジンの設定。
- QoS の設定。
- 事前生成レポートの自動生成/アラートの設定。
- 通知限度の設定。

ディザスタ リカバリ システムでは、次のイベントが記録されます。

- 開始に成功または失敗したバックアップ
- 開始に成功または失敗した復元
- 正しくキャンセルされたバックアップ
- 完了に成功または失敗したバックアップ
- 完了に成功または失敗した復元

- バックアップ スケジュールの保存、更新、削除、イネーブル化、ディセーブル化
- バックアップの宛先デバイスの保存、更新、削除

Cisco Business Edition 5000 の場合、Cisco Unity Connection の管理では、次のイベントが記録されます。

- ユーザのログイン/ログアウト。
- すべての設定変更（ユーザ、連絡先、コール管理オブジェクト、ネットワーク、システム設定、テレフォニーなど）。
- タスク管理（タスクの有効化/無効化）。
- 一括管理ツール（一括作成、一括削除）。
- カスタム キーパッド マップ（マップの更新）

Cisco Business Edition 5000 の場合、Cisco PCA では、次のイベントが記録されます。

- ユーザのログイン/ログアウト。
- Messaging Assistant で行われたすべての設定変更。

Cisco Business Edition 5000 の場合、Cisco Unity Connection Serviceability では、次のイベントが記録されます。

- ユーザのログイン/ログアウト。
- すべての設定変更。
- サービスのアクティブ化、非アクティブ化、開始、または停止。

Cisco Business Edition 5000 の場合、REST API を使用するクライアントでは、次のイベントが記録されます。

- ユーザのログイン（ユーザの API 認証）。
- Cisco Unity Connection プロビジョニング インターフェイス（CUPI）を使用する API 呼び出し。

データベース ログ

RTMT の informix フォルダに表示されるデータベース監査ログでは、データベースの変更がレポートされます。このログは、デフォルトではイネーブルになっていませんが、Cisco Unified Serviceability で **[ツール（Tools）] > [監査ログ設定（Audit Log Configuration）]** を選択することによって設定を変更できます。設定可能な監査ログの設定については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

このログは、アプリケーションの設定変更を記録するアプリケーション監査ログとは異なり、データベースの変更を記録します。Cisco Unified Serviceability でデータベース監査がイネーブルに設定されるまで、informix フォルダは RTMT に表示されません。

オペレーティング システム ログ

RTMT の vos フォルダに表示されるオペレーティング システム監査ログでは、オペレーティング システムによってトリガーされるイベントがレポートされます。デフォルトでは、イネーブルになっていません。**utils auditd** CLI コマンドによって、イネーブルまたはディセーブルにしたり、イベントのステータスを提供したりできます。

CLI で監査がイネーブルに設定されるまで、vos フォルダは RTMT に表示されません。

CLI の詳細については、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』を参照してください。

リモート サポート アカウント イネーブル化ログ

RTMT の vos フォルダに表示されるリモート サポート アカウント イネーブル化ログでは、テクニカル サポート チームによって発行される CLI コマンドがレポートされます。このログの設定は変更できません。このログは、テクニカル サポート チームによってリモート サポート アカウントがイネーブルに設定された場合にだけ作成されます。

Cisco Unified Communications Manager サービスが稼働しているかどうかの確認

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

1. Unified Communications Manager Administration から、**[ナビゲーション（Navigation）]** > **[Cisco Unified Serviceability]** を選択します。
2. **[ツール（Tools）]** > **[サービス アクティベーション（Service Activation）]** を選択します。
3. [サーバ（Server）] カラムから必要なサーバを選択します。

   選択したサーバが [現在のサーバ（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一連のボックスが表示されます。

   Cisco CallManager 行の [アクティベーション ステータス（Activation Status）] カラムに、[アクティブ化（Activated）] または [非アクティブ（Deactivated）] と表示されます。

   [アクティブ化（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、指定した Cisco CallManager サービスがアクティブのままになっています。

   [非アクティブ（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。
4. 目的の Cisco CallManager サービスのチェックボックスをオンにします。
5. [更新（Update）] ボタンをクリックします。

指定した Cisco CallManager サービス行の [アクティベーション ステータス（Activation Status）] カラムに [アクティブ化（Activated）] と表示されます。

これで、選択したサーバ上の指定したサービスがアクティブになります。

Cisco CallManager サービスがアクティブであるかどうか、およびサービスが現在動作しているかどうかを確認するには、次の手順を実行します。

手順

1. Unified Communications Manager Administration から、**[ナビゲーション（Navigation）] > [Cisco Unified Serviceability]** を選択します。

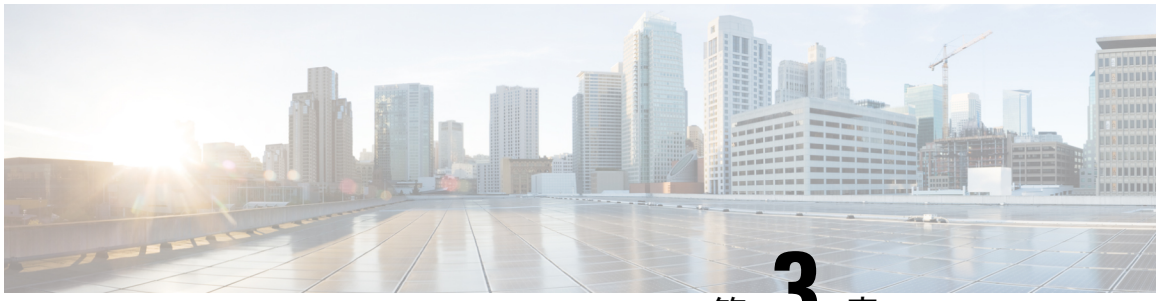
   [Cisco Unified Serviceability] ウィンドウが表示されます。

2. **[ツール（Tools）] > [コントロール センターの機能サービス（Control Center – Feature Services）]** を選択します。

3. [サーバ（Server）] 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。

   [ステータス（Status）] カラムに、選択したサーバでどのサービスが動作しているかが表示されます。



第 3 章

Cisco Unified Communications Manager のシステムの問題

この項では、Unified Communications Manager システムに関連する次のような最も一般的な問題の解決策について説明します。

Cisco Unified Communications Manager システムが応答しない

この項では、応答しない *Unified Communications Manager* システムに関する問題について説明します。

関連トピック

Cisco Unified Communications Manager システムが応答を停止する （38 ページ）

Cisco Unified Communications Manager Administration が表示されない （39 ページ）

Cisco Unified Communications Manager Administration へのアクセス時にエラーが発生する （39 ページ）

後続のノードで Cisco Unified Communications Manager Administration へのアクセス時にエラーが発生する （40 ページ）

表示権限がない （40 ページ）

Cisco Unified Communications Manager でのユーザの表示または追加における問題 （41 ページ）

名前からアドレスへの解決が失敗する （42 ページ）
ブラウザと Cisco Unified Communications Manager サーバとの間でポート 80 がブロックされる （42 ページ）
リモート マシンのネットワーク設定が正しくない （43 ページ）
サーバの応答が遅い （55 ページ）

Cisco Unified Communications Manager システムが応答を停止する

症状

Unified Communications Manager システムが応答しません。

Cisco CallManager サービスが応答しなくなった場合は、次のメッセージがシステム イベント ログに表示されます。

```
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.
```

この場合では、その他にも次のメッセージが表示されることがあります。

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

Cisco Communications Manager が、次のエラーにより起動しませんでした。

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

この状態で Cisco Unified IP Phone やゲートウェイなどのデバイスが Unified Communications Manager から登録解除されると、ユーザが受信するダイヤル トーンが遅延したり、高い CPU 使用率が原因で Unified Communications Manager 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、Unified Communications Manager のイベント ログを参照してください。

考えられる原因

サービスが機能するために十分なリソース（CPU やメモリなど）がない場合には、Cisco CallManager サービスは応答を停止できます。一般に、その時点でサーバの CPU 使用率は 100% になります。

推奨処置

発生している中断のタイプに応じて、その中断の根本原因の確認に役立つさまざまなデータを収集する必要があります。

リソースの不足による中断が発生した場合は、次の手順を使用します。

手順

1. 中断の前後 15 分間の Cisco CallManager トレースを収集します。
2. 中断の前後 15 分間の Specification and Description Language（SDL）トレースを収集します。
3. ある場合は、perfmon トレースを収集します。
4. トレースがない場合は、perfmon トレースの収集を開始し、サーバ上で実行されている各プロセスのメモリと CPU の使用率をトラッキングします。これらは、リソースの不足による中断が再度発生した場合に役立ちます。

Cisco Unified Communications Manager Administration が表示されない

症状

Unified Communications Manager Administration 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

Cisco CallManager サービスがサーバ上でアクティブであり、実行されていることを確認します。関連トピックまたは『*Cisco Unified Serviceability Administration Guide*』を参照してください。

関連トピック

Cisco Unified Communications Manager サービスが稼働しているかどうかの確認 （34 ページ）

Cisco Unified Communications Manager Administration へのアクセス時にエラーが発生する

症状

Unified Communications Manager Administration にアクセスしようとすると、エラー メッセージが表示されます。

考えられる原因

必要なサービスが自動的に開始されていません。Unified Communications Manager Administration が表示されない最も一般的な理由は、サービスのいずれかが停止していることです。

推奨処置

停止しているサービスを開始します。

後続のノードで Cisco Unified Communications Manager Administration へのアクセス時にエラーが発生する

症状

Unified Communications Manager Administration にアクセスしようとすると、エラー メッセージが表示されます。

考えられる原因

Unified Communications Manager の後続ノードがオフラインのときに第 1 ノードの IP アドレスが変更されると、後続ノードで Unified Communications Manager Administration にログインできなくなることがあります。

推奨処置

このエラーが発生した場合は、「*Changing the IP Address and Host Name for Unified Communications Manager*」の説明に従って、Unified Communications Manager の後続ノードの IP アドレスを変更します。

表示権限がない

症状

Unified Communications Manager Administration にアクセスしたときに、次のいずれかのメッセージが表示されます。

- このページを表示する権限がありません（You Are Not Authorized to View This Page）
- 指定したクレデンシャルを使用してこのディレクトリまたはページを表示する権限がありません（You do not have permission to view this directory or page using the credentials you supplied.）
- サーバ アプリケーション エラー（Server Application Error.）要求の処理時におけるアプリケーションのロード中に、サーバでエラーが発生しました（The server has encountered an error while loading an application during the processing of your request.）詳細については、イベント ログを参照してください（Please refer to the event log for more detailed information.）サーバ管理者にお問い合わせください（Please contact the server administrator for assistance.）
- エラー：アクセスが拒否されました（Error: Access is Denied.）

考えられる原因

不明

推奨処置

TAC にお問い合わせください。

Cisco Unified Communications Manager でのユーザの表示または追加における問題

症状

Unified Communications Manager Administration で、ユーザを追加したり、検索を実行したりすることができません。

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）を含むサーバ上にインストールされた Unified Communications Manager を使用しているか、Microsoft Internet Explorer 5.5 SP2 および Q313675 パッチ以上を使用していると、次の問題が発生することがあります。

- 基本検索を実行して [送信（Submit）] をクリックしても、同じページが再表示されます。
- 新規ユーザの挿入を試みると、次のメッセージが表示されます。

```
コマンド実行時に次のエラーが発生し、セッション オブジェクトがタイムアウトしました。ここをクリックして新しい検索を開始してください（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

Unified Communications Manager 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と（Call_Manager など）、Unified Communications Manager Administration でユーザを追加したり、検索を実行したりすることができなくなる場合があります。ドメイン ネーム システム（DNS）でサポートされている文字は、アルファベット（A ～ Z、a ～ z）、数字（0 ～ 9）、およびハイフン（-）です。特殊文字は許可されていません。ブラウザに Q313675 パッチがインストールされている場合は、DNS でサポートされていない文字が URL に含まれないようにしてください。

Q313675 パッチの詳細については、「[MS01-058] Internet Explorer 5.5 と Internet Explorer 6 のファイルの脆弱性に対する対策」を参照してください。

次のいずれかの方法を使用して、この問題を解決できます。

- サーバの IP アドレスを使用して Unified Communications Manager Administration にアクセスする。

- DNS でサポートされていない文字をサーバ名で使用しない
- URL で localhost または IP アドレスを使用する

名前からアドレスへの解決が失敗する

症状

次の URL へのアクセスを試みたときに、次のいずれかのメッセージが表示されます。

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

- Internet Explorer：ページを表示できません（This page cannot be displayed）
- Netscape：見つかりません。（Not Found.）要求された URL `/ccmadmin` がこのサーバ上に見つかりませんでした。（The requested URL /ccmadmin was not found on this server.）

Cisco Communications Manager の名前の代わりに IP アドレスを使用して同じ URL にアクセスすると（`http://10.48.23.2/ccmadmin`）、ウィンドウが表示されます。

考えられる原因

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

推奨処置

DNS を使用するように設定している場合は、DNS を確認して、*your-cm-server-name* のエントリに Unified Communications Manager サーバの正しい IP アドレスが設定されているかどうかを調べます。正しくない場合は変更します。

DNS を使用していない場合、ローカル マシンでは、「「hosts」」ファイルを確認することによって、*your-cm-server-name* のエントリが存在するかどうか、およびサーバ名に関連付けられている IP アドレスが確認されます。ファイルを開き、Unified Communications Manager のサーバ名と IP アドレスを追加します。「「hosts」」ファイルは、`C:\WINNT\system32\drivers\etc\hosts` にあります。

ブラウザと Cisco Unified Communications Manager サーバとの間でポート 80 がブロックされる

症状

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がファイアウォールによってブロックされている場合は、次のメッセージが表示されます。

- Internet Explorer：ページを表示できません（This page cannot be displayed）

- Netscape：応答がありません（There was no response.）サーバがダウンしているか、応答していない可能性があります（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により、ローカル ネットワークからサーバ ネットワークへの HTTP アクセスがブロックされています。

推奨処置

1. Unified Communications Manager サーバへの他のタイプのトラフィック（ping や Telnet など）が許可されているかどうかを確認します。いずれかのタイプのアクセスに成功した場合は、リモート ネットワークから Unified Communications Manager Web サーバへの HTTP アクセスがブロックされていることになります。
2. ネットワーク管理者にセキュリティ ポリシーを確認してください。
3. サーバが配置されているネットワークと同じネットワークから再試行します。

リモート マシンのネットワーク設定が正しくない

症状

Unified Communications Manager に接続できないか、または Unified Communications Manager と同じネットワーク内の他のデバイスに接続できません。

他のリモート マシンから同じ操作を試みると、Unified Communications Manager Administration 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値が正しくない場合は、Web サーバのネットワークに対して接続できないか、または部分的にしか接続できないため、Web ページが表示されない場合があります。

推奨処置

1. 接続できないことを確認するために、Unified Communications Manager サーバおよびその他のデバイスの IP アドレスに対して ping を実行します。
2. ローカルネットワークの外部にあるすべてのデバイスに対する接続に失敗する場合は、ステーションのネットワーク設定、およびケーブルとコネクタの整合性を確認してください。詳細については、該当するハードウェア マニュアルを参照してください。

   接続に LAN 経由で TCP/IP を使用している場合は、次の手順を実行して、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。
3. **[スタート（Start）] > [設定（Setting）] > [ネットワークとダイヤルアップ接続（Network and Dial-up connections）]** を選択します。

4. [ローカル エリア接続（Local Area Connection）]、[プロパティ（Properties）] の順に選択します。

   通信プロトコルのリストがチェックボックスとともに表示されます。

5. [インターネット プロトコル（TCP/IP）（Internet Protocol (TCP/IP)）] を選択して、再度 [プロパティ（Properties）] をクリックします。

6. ネットワークに応じて、[IP アドレスを自動的に取得する（Obtain an ip address automatically）] または**アドレス、マスク、およびデフォルト ゲートウェイの手動設定**を選択します。

   また、ブラウザ固有の設定が誤っている可能性もあります。

7. Internet Explorer ブラウザの **[ツール（Tools）]** > **[インターネット オプション（Internet Options）]** を選択します。

8. [接続（Connections）] タブを選択して、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設定されていません。Windows の一般的なネットワーク設定が使用されます。

9. Unified Communications Manager 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あ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てください。

（注） この手順を実行してもリモート サーバからのブラウジングができない場合は、TAC に連絡して、問題の詳細な調査を依頼してください。

Cisco RAID の動作の影響を管理する

Cisco 冗長ディスク アレイ（RAID） コントローラは、整合性検査（CC）、バックグラウンド初期化（BGI）、再構成（RBLD）、ボリューム拡張と再構築（RLM）、Patrol Real（PR）などのさまざまなバックグラウンド処理を行います。

これらのバックグラウンド処理は、I/O 操作に対する影響を抑制するように設計されています。ただし、フォーマットや類似の I/O 操作など、実行中の操作によっては影響が大きくなる場合がありました。このようなケースでは、I/O 操作とバックグラウンド処理の両方で大量の CPU リソースが消費される可能性があります。CC および Patrol Read のジョブは、負荷が比較的低いときに実行するようにスケジュールすることを推奨します。高負荷の処理が同時に動作する CallManager サーバが存在する場合は、同時実行される可能性のあるバックグラウンド処理とその他の集中的な I/O 操作を制限することを推奨します。

データベース レプリケーション

この項では、Unified Communications Manager システムにおけるデータベース レプリケーションに関する問題について説明します。

関連トピック

パブリッシャ サーバとサブスクライバ サーバとの間のレプリケーションに失敗する （45 ページ）
失われたノードで接続が復元されてもデータベース レプリケーションが実行されない （49 ページ）
データベース テーブルで同期が外れてもアラートがトリガーされない （50 ページ）
古い製品リリースに戻す場合のデータベース レプリケーションのリセット （51 ページ）

パブリッシャサーバとサブスクライバサーバとの間のレプリケーションに失敗する

データベースの複製は、Unified Communications Manager クラスタのコア機能です。データベースのマスター コピーを備えたサーバはパブリッシャ（最初のノード）として機能し、データベースを複製するサーバはサブスクライバ（以降のノード）を構成します。

ヒント サブスクライバ サーバに Unified Communications Manager をインストールする前に、Unified Communications Manager Administration で [サーバの設定（Server Configuration）] ウィンドウにサブスクライバを追加して、パブリッシャ データベース サーバ上のデータベースをサブスクライバが確実に複製できるようにする必要があります。サブスクライバ サーバを [サーバの設定（Server Configuration）] ウィンドウに追加し、Unified Communications Manager をサブスクライバにインストールすると、サブスクライバはパブリッシャ サーバ上のデータベースのコピーを受け取ります。

症状

パブリッシャ サーバ上の変更が、サブスクライバ サー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 サーバとサブスクライバ サーバの間の複製に失敗する。

推奨処置

データベースの複製を確認し、必要に応じて、次の手順に従って修正します。

手順

1. データベースのレプリケーションを確認します。データベース レプリケーションは、CLI、Cisco Unified Reporting、または RTMT を使用して確認できます。
   - CLI を使用した確認については、2 （46 ページ）を参照してください。
   - Cisco Unified Reporting を使用した確認については、3 （46 ページ）を参照してください。
   - RTMT を使用した確認については、4 （47 ページ）を参照してください。
2. CLI を使用してデータベース レプリケーションを確認するには、CLI にアクセスし、次のコマンドを発行して、各ノードにおけるレプリケーションを確認します。各ノードでこの CLI コマンドを実行し、その複製のステータスを確認する必要があります。また、サブスクライバをインストールしたあと、サブスクライバの数によっては、2 のステータスになるまでにかなりの時間がかかる場合があります。

```
admin:  show perf query class "Number of Replicates Created and State of Replication"
  ==>query class: - Perf class (Number of Replicates Created and State of
Replication) has instances and values: ReplicateCount -> Number of Replicates
 Created = 344 ReplicateCount -> Replicate_State = 2
```

   この場合、Replicate_State オブジェクトが値 2 を示すことに注意してください。次に、Replicate_State が取ることのできる値を示します。
   - 0：この値は、複製が開始されていないことを示します。後続のノード（サブスクライバ）がありません。または、Cisco Database Layer Monitor サービスが、サブスクライバのインストール後から実行されていません。
   - 1：この値は、複製が作成されているにもかかわらず、カウントが間違っていることを示します。
   - 2：この値は、複製の状態が良好であることを示します。
   - 3：この値は、クラスタで複製に問題があることを示します。
   - 4：この値は、複製の設定に失敗したことを示します。
3. Cisco Unified Reporting を使用してデータベース レプリケーションを確認するには、次のタスクを実行します。
   1. Cisco Unified Communications Manager Administration の右上隅にある [ナビゲーション（Navigation）] ドロップダウン リスト ボックスから、[Cisco Unified Reporting] を選択します。
   2. Cisco Unified Reporting が表示されたら、[システム レポート（System Reports）] をクリックします。
   3. データベース レプリケーションのデバッグ情報を示す [Unified CM データベース ステータス（Unified CM Database Status）] レポートを生成および表示します。

      レポートを生成したあと、レポートを開いて、[Unified CM データベース ステータス（Unified CM Database Status）] を確認します。ここには、クラスタ内の全サーバの

RTMT レプリケーション カウンタが含まれます。すべてのサーバの複製状態は 2 になっていなければならず、すべてのサーバで同じ数の複製が作成されている必要があります。

前述のステータスの確認でレプリケーションの状態が 2 になっていない場合は、このレポートの「「レプリケーション サーバ リスト（Replication Server List）」」を参照してください。ここには、接続され、各ノードとやり取りしているサーバが表示されます。リストにおいて、各サーバは、自身をローカルとして示し、その他のサーバをアクティブに接続されているサーバとして示します。いずれかのサーバの接続が切断されていると表示されている場合は、通常、ノード間に通信上の問題が発生しています。

4. 必要に応じて、Unified Communications Manager データベースの正常性のスナップショットを提供する Unified CM データベース ステータス レポートを生成して確認します。

4. RTMT を使用してデータベース レプリケーションを確認するには、次のタスクを実行します。

   1. Cisco Unified Real-Time Monitoring Tool（RTMT）を開きます。
   2. [CallManager] タブをクリックします。
   3. [データベースの要約（Database Summary）] をクリックします。[レプリケーション ステータス（Replication Status）] ペインが表示されます。

   [レプリケーション ステータス（Replication Status）] ペインに表示される値を次に示します。

   - 0：この値は、複製が開始されていないことを示します。後続のノード（サブスクライバ）がありません。または、Cisco Database Layer Monitor サービスが、サブスクライバのインストール後から実行されていません。
   - 1：この値は、複製が作成されているにもかかわらず、カウントが間違っていることを示します。
   - 2：この値は、複製の状態が良好であることを示します。
   - 3：この値は、クラスタで複製に問題があることを示します。
   - 4：この値は、複製の設定に失敗したことを示します。
   - Replicate_State パフォーマンス モニタリング カウンタを表示するには、**[システム（System）] > [パフォーマンス（Performance）] > [パフォーマンス モニタリングを開く（Open Performance Monitoring）]** を選択します。パブリッシャ データベース サーバ（最初のノード）をダブルクリックし、パフォーマンス モニタを拡張します。[作成された複製の数と複製の状態（Number of Replicates Created and State of Replication）] をクリックします。[Replicate_State] をダブルクリックします。[オブジェクト インスタンス（Object Instances）] ウィンドウの [ReplicateCount] をクリックし、[追加（Add）] をクリックします。

ヒント　カウンタの定義を表示するには、カウンタ名を右クリックし、[カウンタの説明（Counter Description）] を選択します。

5. すべてのサーバでRTMTのステータスが良好であるにもかかわらず、データベースが同期していないことが疑われる場合は、CLI コマンド **utils dbreplication status** を実行します

   （いずれかのサーバで RTMT ステータスが 4 と表示される場合は、ステップ 6 に進みます）。

   このステータス コマンドは、**utils dbreplication status all** を使用してすべてのサーバで、

   または **utils dbreplication status** <*hostname*> を使用して 1 つのサブスクライバで実行できます。

   ステータス レポートは、疑わしいテーブルがあるかどうかを示します。疑わしいテーブルがある場合は、複製修正CLIコマンドを使用し、パブリッシャ サーバからサブスクライバ サーバにデータを同期します。

   複製の修正は、次のコマンドを使用して、すべてのサブスクライバ サーバで実行することも（**all** パラメータを使用）、1 つのサブスクライバ サーバだけで実行することもできます。

   utils dbreplication repair usage:utils dbreplication repair [nodename]|all

   複製の修正を実行した後（数分間かかることがある）、別のステータス コマンドを実行して、すべてのテーブルが同期されたことを確認できます。

   修正後にテーブルが同期されていれば、複製の修正は成功です。

（注）　サーバの 1 つで RTMT のステータスが 4 の場合、またはステータス 0 の状態が 4 時間を超えた場合に限り、ステップ 6 を実行します。

6. データベース レプリケーションのデバッグ情報を示す [Unified CM データベース ステータス（Unified CM Database Status）] レポートを生成および表示します。RTMT のステータスが不良と表示される各サブスクライバで、hosts、rhosts、sqlhosts、およびサービス ファイルに適切な情報が含まれることを確認します。

   [Cisco Unified CM クラスタの概要（Cisco Unified CM Cluster Overview）] レポートを生成し、表示します。サブスクライバ サーバのバージョンが同一であること、接続が正常であること、時間遅延が許容値内であることを確認します。

   前述の条件が許容できるものである場合、次の手順を実行して、そのサブスクライバ サーバ上でレプリケーションをリセットします。

   1. サブスクライバ サーバで、CLI コマンド **utils dbreplication stop** を実行します。

      これを、RTMT の値が 4 のすべてのサブスクライバ サーバで実行します。

2. パブリッシャ サーバで、CLI コマンド **utils dbreplication stop** を実行します。
3. パブリッシャ サーバで、CLI コマンド **utils dbreplication reset** <*hostname*> を実行します。

   ここで、<*hostname*> はリセットする必要のあるサブスクライバ サーバのホスト名です。すべてのサブスクライバ サーバをリセットする必要がある場合は、コマンド **utils dbreplication reset all** を使用します。

詳細情報

『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』

『*Cisco Unified Reporting Administration Guide*』

『*Command Line Interface Reference Guide for Cisco Unified Solutions*』

失われたノードで接続が復元されてもデータベースレプリケーションが実行されない

症状

失われたノードの回復時に接続が復元されても、データベースのレプリケーションが行われません。レプリケーションに失敗した場合に、レプリケーションの状態を確認する方法については、関連トピックを参照してください。ノードですでに複製のリセットを試み、その操作に失敗している場合に限り、次の手順を使用します。

考えられる原因

デバイス テーブルでの削除により、CDR チェックがループに入っている。

推奨処置

1. 影響を受けているサブスクライバで **utils dbreplication stop** を実行します。これはすべて同時に実行できます。
2. 手順 1 が完了するまで待ち、次に、影響を受けているパブリッシャ サーバで **utils dbreplication stop** を実行します。
3. 影響を受けているパブリッシャ サーバから **utils dbreplication clusterreset** を実行します。このコマンドを実行すると、ログ名がログ ファイルにリストされます。このファイルを確認し、プロセスのステータスをモニタします。パスは次のとおりです。

   `/var/log/active/cm/trace/dbl/sdi`
4. 影響を受けているパブリッシャから **utils dbreplication reset all** を実行します。
5. クラスタ内のすべてのサブスクライバ サーバですべてのサービスを停止し、再起動して（または、すべてのシステム（サブスクライバ サーバ）を再起動/リブートして）、サー

ビスを変更します。この操作は必ず、**utils dbreplication status** で 2 のステータスが表示されてから実行します。

関連トピック

パブリッシャ サーバとサブスクライバ サーバとの間のレプリケーションに失敗する （45 ページ）

データベーステーブルで同期が外れてもアラートがトリガーされない

（注） 「「同期外れ」」とは、クラスタ内の2つのサーバの特定のデータベーステーブルに同じ情報が含まれていないという意味です。

症状

Unified Communications Manager バージョン 6.x 以降では、この症状には予期しないコール処理の動作が含まれます。コールが、予期したようにルーティングまたは処理されません。この症状は、パブリッシャ サーバとサブスクライバ サーバのいずれかで発生することがあります。

Unified Communications Manager バージョン 5.x では、この症状には予期しないコール処理の動作が含まれます。コールのルーティングと処理は予想どおりに実行されませんが、これは、パブリッシャ サーバがオフラインになっているときに限ります。

この症状が発生したときに CLI で **utils dbrepication status** を実行すると、**`Out of sync`** とレポートされます。

`Out of sync` と表示されない場合、問題はありません。

考えられる原因

ノード間でデータベーステーブルの同期が外れたままになっています。複製アラートは、複製プロセスの障害だけを示し、データベーステーブルの同期が外れた時期は示しません。通常、複製が正しく行われている場合は、テーブルの同期は維持されているはずです。場合によっては、レプリケーションが正しく行われているように見えるにもかかわらず、データベーステーブルが「「同期外れ」」の状況が発生することがあります。

推奨処置

1. CLI コマンドを使用してクラスタの複製をリセットします。この処置を実行するためには、クラスタ内のサーバがオンラインで、IP 接続が完全に確立されていることが必要です。クラスタ内のすべてのサーバがオンラインであるかどうかは、プラットフォームの CLI および Cisco Unified Reporting を使用して確認します。
2. サーバの複製の状態が 2 の場合は、パブリッシャ サーバで次のコマンドを実行します。
3. **utils dbreplication repair** *server name*
4. サーバの複製の状態が 2 ではない場合は、

5. すべてのサブスクライバ サーバで次のコマンドを実行します。
6. **utils dbreplication stop**
7. 次に、すべてのパブリッシャ サーバで次のコマンドを実行します。
8. **utils dbreplication stop**
9. 次に
10. **utils dbreplication reset all**

古い製品リリースに戻す場合のデータベース レプリケーションのリセット

古い製品リリースを実行できるようにクラスタ内のサーバを元に戻す場合は、クラスタ内部でデータベース レプリケーションを手動でリセットする必要があります。すべてのクラスタ サーバを古い製品リリースに戻したあとにデータベース レプリケーションをリセットするには、パブリッシャ サーバで CLI コマンド **utils dbreplication reset all** を入力します。

Cisco Unified Communications Operating System Administration または CLI を使用してバージョンを切り替えると、古い製品バージョンに戻すときに、データベース レプリケーションのリセット要件に関するメッセージが表示されます。

utils dbreplication clusterreset

このコマンドを使用すると、クラスタ全体でデータベース レプリケーションがリセットされます。

コマンドの構文

utils dbreplication clusterreset

使用上のガイドライン

このコマンドを実行する前に、utils dbreplication stop コマンドをすべてのサブスクライバ サーバで実行し、その後、パブリッシャ サーバでも実行します。

要件

コマンド特権レベル：0

アップグレード時の使用：可能

utils dbreplication dropadmindb

このコマンドは、クラスタ内のすべてのサーバにある Informix の syscdr データベースをドロップします。

コマンドの構文

utils dbreplication dropadmindb

使用上のガイドライン

このコマンドは、データベース レプリケーションのリセットまたはクラスタのリセットが失敗し、複製を再起動できない場合にのみ使用します。

要件

コマンド特権レベル：0

アップグレード時の使用：可能

LDAP 認証の失敗

この項では、LDAP 認証に失敗した場合の一般的な問題について説明します。

症状

エンドユーザのログインに失敗します。ユーザがログインする前に、認証タイムアウトが発生します。

考えられる原因

Cisco Unified Communications Manager Administration の [LDAP 認証（LDAP Authentication）] ウィンドウにおける [LDAP ポート（LDAP Port）] の設定が誤っています。

推奨処置

社内ディレクトリの設定に応じて、[LDAP ポート（LDAP Port）] フィールドに入力するポート番号が決まります。たとえば、[LDAP ポート（LDAP Port）] フィールドを設定する前に、LDAP サーバがグローバル カタログ サーバとして動作するかどうかや、設定に LDAP over SSL が必要であるかどうかを確認します。たとえば、次のようなポート番号を入力します。

例：LDAP サーバがグローバル カタログ サーバではない場合の LDAP ポート

- 389：SSL が必要でない場合（このポート番号は、[LDAP ポート（LDAP Port）] フィールドに表示されるデフォルトです）。
- 636：SSL が必要な場合（このポート番号を入力する場合は、[SSL を使用（Use SSL）] チェックボックスがオンであることを確認します）。

例：LDAP サーバがグローバル カタログ サーバである場合の LDAP ポート

- 3268：SSL が必要でない場合。

• 3269：SSL が必要な場合。（このポート番号を入力する場合は、[SSL を使用（Use SSL）] チェックボックスがオンであることを確認します）。

ヒント　設定によっては、上記の例に示した番号以外のポート番号を入力する必要がある場合があります。[LDAP ポート（LDAP Port）] フィールドを設定する前に、ディレクトリ サーバの管理者に問い合わせて、入力する正しいポート番号を確認してください。

LDAP over SSL の問題

この項では、LDAP over SSL を使用する場合の一般的な問題について説明します。

症状

LDAP over SSL が動作しません。

考えられる原因

ほとんどの場合、LDAP over SSL の問題は、Unified Communications Manager サーバ上の証明書（チェーン）が無効であるか、誤っているか、または不完全であることが原因です。

説明

SSL には、複数の証明書を使用する場合があります。ほとんどの場合、LDAP over SSL を動作させるには、ディレクトリ信頼証明書として AD ルート証明書をアップロードするだけで済みます。ただし、異なるディレクトリ信頼証明書がアップロードされた場合、つまりルート証明書以外の証明書がアップロードされた場合は、その証明書をルート証明書などの上位レベルの証明書によって確認する必要があります。この場合、複数の証明書が関係するため、証明書チェーンが作成されます。たとえば、証明書チェーンには、次の証明書が含まれている場合があります。

- ルート証明書：信頼チェーンにおける最上位の CA 証明書です。この証明書の発行者と被認証者は同じです。
- 中間証明書：信頼チェーンの一部を構成する CA 証明書です（最上位以外）。中間証明書によって、階層のルートから最下位の中間証明書までがつながります。
- リーフ証明書：1 つ上の階層の中間証明書によって署名された、サービスやサーバに発行される証明書です。

企業における証明書チェーンには、たとえば 2 つの証明書および 1 つのルート証明書があります。次に、証明書の内容を示します。

Data:

Version: 3 (0x2)

Serial Number:

- 77:a2:0f:36:7c:07:12:9c:41:a0:84:5f:c3:0c:64:64

Signature Algorithm: sha1WithRSAEncryption
Issuer: DC=com, DC=DOMAIN3, CN=jim
Validity

- Not Before: Apr 13 14:17:51 2009 GMT
- Not After: Apr 13 14:26:17 2014 GMT

Subject: DC=com, DC=DOMAIN3, CN=jim

推奨処置

2 ノードのチェーンの場合、チェーンにはルート証明書とリーフ証明書が含まれています。この場合は、ディレクトリ信頼ストアにルート証明書をアップロードするだけで済みます。

3 つ以上のノードのチェーンの場合、チェーンには、ルート証明書、リーフ証明書、および中間証明書が含まれています。この場合は、ルート証明書、およびリーフ証明書を除くすべての中間証明書をディレクトリ信頼ストアにアップロードする必要があります。

証明書チェーンの最上位（ルート証明書）の Issuer（発行者）フィールドと Subject（被認証者）フィールドが同じであることを確認します。Issuer フィールドと Subject フィールドが同じでない場合、証明書はルート証明書ではなく中間証明書となります。この場合は、ルートから最下位中間証明書までのチェーン全体を特定して、チェーン全体をディレクトリ信頼ストアにアップロードします。

また、Validity フィールドを確認して、証明書の有効期限が切れていないことを確認します。中間証明書の有効期限が切れている場合は、新しいチェーン、および新しいチェーンを使用して署名された新しいリーフ証明書を認証機関から取得します。リーフ証明書の有効期限だけが切れている場合は、署名された新しいリーフ証明書を取得します。

OpenLDAP で LDAP サーバに接続するための証明書を確認できない

症状

CTI クライアントまたは JTAPI クライアント経由でのエンドユーザ認証に失敗しますが、Unified CM へのユーザ認証は動作します。

考えられる原因

OpenLDAP では、LDAP サーバに接続するための証明書を確認できません。

説明

証明書は、完全修飾ドメイン名（FQDN）を使用して発行されます。OpenLDAP の検証プロセスでは、FQDN がアクセス先のサーバと照合されます。アップロードされている証明書では FQDN が使用され、Web フォームでは IP アドレスが使用されているため、OpenLDAP はサーバに接続できません。

推奨処置

- 可能な場合には、DNS を使用します。

  証明書署名要求（CSR）プロセス時に、被認証者 CN の一部として FQDN を指定します。この CSR を使用して自己署名証明書または CA 証明書を取得すると、通常名には同じ FQDN が含まれます。したがって、CTI や CTL などのアプリケーションで LDAP 認証がイネーブル化された場合でも、信頼証明書がディレクトリ信頼ストアにインポートされていれば、問題は発生しません。

- DNS を使用していない場合は、Unified Communications Manager Administration の [LDAP認証設定（LDAP Authentication Configuration）] ウィンドウに IP アドレスを入力します。その後、`/etc/openldap/ldap.conf` に次の 1 行を追加します。

  TLS_REQCERT never

  このファイルを更新するには、リモートアカウントが必要です。このように設定すると、OpenLDAP ライブラリで、サーバの証明書が確認されません。ただし、後続の通信は引き続き SSL を使用して行われます。

サーバの応答が遅い

この項では、全二重ポートの設定が一致しないためにサーバからの応答が遅くなることに関連した問題について説明します。

症状

サーバからの応答が遅くなります。

考えられる原因

スイッチの全二重ポート設定が Unified Communications Manager サーバの全二重ポート設定と一致していない場合、応答が遅くなる可能性があります。

推奨処置

1. 最適なパフォーマンスを得るために、スイッチおよびサーバの両方を **100/Full** に設定します。

   スイッチまたはサーバで Auto 設定を使用することは推奨しません。

2. この変更を有効にするには、Unified Communications Manager サーバを再起動する必要があります。

JTAPI サブシステム起動の問題

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 Unified Communications Manager と通信し、テレフォニー コール制御を担当します。CRS プラットフォームには、Cisco Unified Auto-Attendant、Cisco IP ICD、Cisco Unified IP-IVR などのテレフォニー アプリケーションがホストされます。この項ではこれらのアプリケーションに固有の内容については説明しませんが、JTAPI サブシステムはこれらすべてのアプリケーションで使用される基本的なコンポーネントであることに注意する必要があります。

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 バージョンが互換性のあるものであることを確認します。互換性を確認するには、使用しているバージョンの Unified Communications Manager の*Cisco Unified Communications Manager* リリース ノートを参照してください。

CRS のバージョンを確認するには、`http://servername/appadmin` と入力して AppAdmin にログインします。ここで、*servername* には、CRS がインストールされているサーバの名前を指定します。メイン メニューの右下隅で現在のバージョンを確認します。

JTAPI サブシステムが OUT_OF_SERVICE になる

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

関連トピック

MIVR-SS_TEL-4-ModuleRunTimeFailure （56 ページ）
MIVR-SS_TEL-1-ModuleRunTimeFailure （59 ページ）

MIVR-SS_TEL-4-ModuleRunTimeFailure

トレース ファイルで、**`MIVR-SS_TEL-1-ModuleRunTimeFailure`** ストリングを検索します。行の末尾に、例外の理由が表示されます。

次に、最も一般的なエラーを示します。

関連トピック

プロバイダーを作成できない：不正なログインまたはパスワード （57 ページ）
プロバイダーを作成できない：接続の拒否 （57 ページ）
プロバイダーを作成できない：Login= （58 ページ）
プロバイダーを作成できない：ホスト名 （58 ページ）
プロバイダーを作成できない：操作のタイムアウト （58 ページ）
プロバイダーを作成できない：Null （59 ページ）

プロバイダーを作成できない：不正なログインまたはパスワード

考えられる原因

管理者が、JTAPI 設定に誤ったユーザ名またはパスワードを入力しました。

エラー メッセージの全文

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

推奨処置

ユーザ名およびパスワードが正しいかどうかを確認します。Unified CM で [Unified CM ユーザ（Unified CM User）] ウィンドウ（http://servername/ccmuser）へのログインを試みて、Unified CM を正しく認証できないことを確認してください。

プロバイダーを作成できない：接続の拒否

考えられる原因

Unified Communications Manager で、JTAPI から Unified Communications Manager への接続が拒否されました。

エラー メッセージの全文

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-timefailure in JTAPI subsystem:
Module=JTAPI Subsystem, Failure Cause=7,Failure Module=JTAPI_PROVIDER_INIT,
Exception=com.cisco.jtapi.PlatformExceptionImpl: 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 Unified Serviceability コントロール センターで、CTI Manager サービスが実行されていることを確認します。

プロバイダーを作成できない：Login=

考えられる原因

JTAPI 設定ウィンドウで何も設定されていません。

エラー メッセージの全文

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-timefailure 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 設定ウィンドウで、JTAPI プロバイダーを設定します。

プロバイダーを作成できない：ホスト名

考えられる原因

CRS エンジンで Unified Communications Manager のホスト名を解決できません。

エラー メッセージの全文

```
%M%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-timefailure 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 エンジンからの DNS 名前解決が正しく動作しているかどうかを確認します。DNS 名の代わりに IP アドレスを使用します。

プロバイダーを作成できない：操作のタイムアウト

考えられる原因

CRS エンジンから Unified Communications Manager への IP 接続がありません。

エラー メッセージの全文

```
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 サーバの 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 サーバおよび Unified Communications Manager のデフォルト ゲートウェイ設定を確認します。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 Unified Communications Manager に ping を実行して、接続をテストします。

プロバイダーを作成できない：Null

考えられる原因

JTAPIプロバイダーのIPアドレスやホスト名が設定されていないか、または正しいバージョンの JTAPI クライアントを使用していません。

エラー メッセージの全文

```
%MIVR-SS_TEL-4-ModuleRunTimeFailure:Real-timefailure 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 バージョンが正しくない場合は、Unified Communications Manager の [プラグイン（Plugins）] ウィンドウから JTAPI クライアントをダウンロードして、CRS サーバにインストールします。

MIVR-SS_TEL-1-ModuleRunTimeFailure

症状

通常、この例外は、JTAPI サブシステムでどのポートも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 Unified Communications Manager と通信できますが、JTAPI を通して 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 メッセージの全文

```
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

Unified Communications Manager の JTAPI ユーザを確認して、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 になる

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 サブシステムで、1 つ以上の 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 メッセージの全文

```
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

トレースのメッセージには、どの CTI ポートまたはルート ポイントが初期化できないかが示されます。このデバイスが Unified Communications Manager の設定に存在すること、および Unified Communications Manager の JTAPI ユーザに関連付けられていることを確認します。

セキュリティの問題

この項では、セキュリティ関連の測定についての情報、およびセキュリティ関連の問題をトラブルシューティングするための一般的なガイドラインについて説明します。

（注） この項では、Cisco Unified IP Phone が不適切な負荷やセキュリティに関するバグなどによって機能しなくなった場合のリセット方法については説明していません。電話機のリセットの詳細については、電話機のモデルに応じた『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』を参照してください。

Cisco Unified IP Phone のモデル 7960、および 7940 のみから CTL ファイルを削除する方法については、電話機のモデルに応じた『Cisco Unified Communications Manager セキュリティ ガイド』または『Cisco Unified IP Phone アドミニストレーション ガイド for Cisco Unified Communications Manager』を参照してください。

関連トピック

セキュリティ アラーム （61 ページ）
セキュリティ パフォーマンス モニタ カウンタ （61 ページ）
セキュリティ ログ ファイルおよびトレース ファイルの確認 （63 ページ）
証明書のトラブルシューティング （63 ページ）
CTL セキュリティ トークンのトラブルシューティング （63 ページ）
CAPF のトラブルシューティング （65 ページ）
電話機および Cisco IOS MGCP ゲートウェイの暗号化のトラブルシューティング （67 ページ）

セキュリティ アラーム

Cisco Unified Serviceability では、X.509 名の不一致、認証エラー、および暗号化エラーに対して、セキュリティ関連アラームが生成されます。Cisco Unified Serviceability によってアラーム定義が提供されます。

TFTP サーバ エラーおよび CTL ファイル エラーが発生した場合は、電話機でアラームが生成される可能性があります。電話機で生成されるアラームについては、電話機のモデルとタイプ（SCCP または SIP）に応じた『*Cisco Unified IP Phone Administration Guide for Cisco Unified Communications Manager*』を参照してください。

セキュリティ パフォーマンス モニタ カウンタ

パフォーマンス モニタ カウンタでは、Unified Communications Manager に登録された認証済み電話機の数、完了した認証済みコールの数、および任意の時点でアクティブな認証済みコールの数が監視されます。次の表に、セキュリティ機能に該当するパフォーマンス カウンタを示します。

表 *5:* セキュリティ パフォーマンス カウンタ

オブジェクト	カウンタ
Unified Communications Manager	AuthenticatedCallsActive AuthenticatedCallsCompleted AuthenticatedPartiallyRegisteredPhone AuthenticatedRegisteredPhones EncryptedCallsActive EncryptedCallsCompleted EncryptedPartiallyRegisteredPhones EncryptedRegisteredPhones SIPLineServerAuthorizationChallenges SIPLineServerAuthorizationFailures SIPTrunkServerAuthenticationChallenges SIPTrunkServerAuthenticationFailures SIPTrunkApplicationAuthorization SIPTrunkApplicationAuthorizationFailures TLSConnectedSIPTrunk
SIP スタック	StatusCodes4xxIns StatusCodes4xxOuts 次に、例を示します。 401 権限なし（HTTP 認証が必要） 403 禁止 405 メソッドが許可されない 407 プロキシ認証が必要
TFTP サーバ（TFTP Server）	BuildSignCount EncryptCount

RTMT でのパフォーマンス モニタへのアクセス、perfmon ログの設定、およびカウンタの詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。

CLI コマンド**show perf**を使用すると、パフォーマンス監視情報が表示されます。CLIインターフェイスの使用方法の詳細については、『*Command Line Interface Reference Guide for Cisco Unified Solutions*』を参照してください。

セキュリティ ログ ファイルおよびトレース ファイルの確認

Unified Communications Manager では、ログ ファイルとトレース ファイルが複数のディレクトリ（cm/log、cm/trace、tomcat/logs、tomcat/logs/security など）に保存されます。

（注） 暗号化をサポートするデバイスでは、SRTP キー情報はトレース ファイルに出力されません。

Cisco Unified Real-Time Monitoring Tool または CLI コマンドのトレース収集機能を使用すると、ログ ファイルおよびトレース ファイルを検索、表示、および操作できます。

証明書のトラブルシューティング

Cisco Unified Communications Platform Administration の証明書管理ツールを使用すると、証明書の表示、証明書の削除、証明書の再生成、証明書の有効期限の監視、証明書と CTL ファイルのダウンロードやアップロードを行うことができます。たとえば、更新した CTL ファイルを Unity にアップロードできます。CLI を使用すると、自己署名証明書および信頼証明書を一覧表示または表示したり、自己署名証明書を再生成したりできます。

CLI コマンド **show cert**、**show web-security**、**set cert regen**、および **set web-security** を使用すると、CLI インターフェイスで証明書を管理できます。たとえば、**set cert regen tomcat** のように使用します。GUI または CLI を使用した証明書の管理方法の詳細については、『*Administration Guide for Cisco Unified Communications Manager*』および『*Command Line Interface Reference Guide for Cisco Unified Solutions*』を参照してください。

CTL セキュリティ トークンのトラブルシューティング

ここでは、CTL セキュリティ トークンに関するトラブルシューティングの情報を示します。

すべてのセキュリティ トークン（eToken）が失われた場合は、Cisco TAC に問い合わせてください。

関連トピック

連続して誤ったセキュリティ トークン パスワードを入力したあとにロックされたセキュリティ トークンのトラブルシューティング （64 ページ）
1 つのセキュリティ トークン（eToken）が失われた場合のトラブルシューティング （64 ページ）
両方のトークン（eToken）が失われた場合のトラブルシューティング

連続して誤ったセキュリティトークンパスワードを入力したあとにロックされたセキュリティ トークンのトラブルシューティング

（注） CLI コマンド セット **utils ctl** でクラスタ セキュリティを管理する場合は、これらのトラブルシューティング手順は必要ありません。

各セキュリティ トークンには再試行カウンタが含まれています。このカウンタには、eToken の[パスワード（Password）] ウィンドウでログインを連続して試行できる回数が指定されています。セキュリティ トークンの再試行カウンタ値は 15 です。カウンタ値を超える回数のログインが連続して試みられた場合、つまり 16 回連続してログインに失敗した場合は、セキュリティ トークンがロックされて使用できなくなったことを示すメッセージが表示されます。ロックされたセキュリティ トークンは、再度イネーブル化することができません。

『*Cisco Unified Communications Manager Security Guide*』の説明に従って、追加のセキュリティ トークンを入手して CTL ファイルを設定します。必要に応じて、新しいセキュリティ トークンを購入して、ファイルを設定します。

（注） パスワードの入力に成功すると、カウンタはゼロにリセットされます。

1 つのセキュリティ トークン（eToken）が失われた場合のトラブルシューティング

（注） CLI コマンド セット **utils ctl** でクラスタ セキュリティを管理する場合は、この手順は必要ありません。

1 つのセキュリティ トークンが失われた場合は、次の手順を実行します。

手順

1. 新しいセキュリティ トークンを購入します。
2. CTL ファイルを署名したトークンを使用し、次のタスクを実行することによって CTL ファイルを更新します。
3. 新しいトークンを CTL ファイルに追加します。
4. 失われたトークンを CTL ファイルから削除します。

   これらのタスクの実行方法の詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。
5. 『*Cisco Unified Communications Manager Security Guide*』の説明に従って、すべての電話機をリセットします。

すべてのセキュリティ トークン（eToken）が失われた場合のトラブルシューティング

セキュリティ トークンが失われ、CTL ファイルを更新する必要がある場合は、次の手順を実行します。

ヒント　次の手順は、変更を反映させるためにクラスタ内のすべてのサーバをリブートする必要があるため、定期メンテナンス期間中に実行してください。

手順

ステップ 1　すべての Cisco Unified CallManager、Cisco TFTP、または代替 TFTP サーバ上で、OS SSH コマンドラインから CTLFile.tlv が存在することを確認します。

file list tftp *CTLFile.tlv*

ステップ 2　CTLFile.tlv を削除します。

file delete tftp *CTLFile.tlv*

ステップ 3　ステップ 1 およびステップ 2 をすべての Cisco Unified CallManager、Cisco TFTP、および代替 TFTP サーバに対して繰り返します。

ステップ 4　新しいセキュリティ トークンを 2 つ以上取得します。

ステップ 5　Cisco CTL クライアントを使用し、「「Cisco CTL クライアントのインストール」」および「「Cisco CTL クライアントの設定」」の説明に従って CTL ファイルを作成します。

ヒント　クラスタ全体のセキュリティ モードが混合モードになっている場合、Cisco CTL クライアントに「サーバ上に CTL ファイルが存在しませんが、CallManager クラスタ セキュリティ モードが混合モードになっています（No CTL File exists on the server but the CallManager Cluster Security Mode is in Mixed Mode）」というメッセージが表示されます。システムが機能するには、CTL ファイルを作成し、CallManager クラスタを混合モードに設定する必要があります。[OK] をクリックし、[CallManager クラスタを混合モードに設定する（Set CallManager Cluster to Mixed Mode）] を選択して CTL ファイルの設定を完了します。

ステップ 6　クラスタ内のすべてのサーバをリブートします。

ステップ 7　すべてのサーバ上に CTL ファイルを作成し、クラスタ内のすべてのサーバをリブートした後、「「Cisco Unified IP Phone の CTL ファイルの削除」」の説明に従って、電話から CTL ファイルを作成します。

CAPF のトラブルシューティング

ここでは、CAPF のトラブルシューティングについて説明します。

関連トピック

電話機の認証文字列のトラブルシューティング （66 ページ）
ローカルで有効な証明書の確認に失敗した場合のトラブルシューティング （66 ページ）
CAPF 証明書がクラスタ内のすべてのサーバにインストールされていることの確認 （66 ページ）
電話機にローカルで有効な証明書が存在することの確認 （67 ページ）
電話機に製造元でインストールされる証明書（MIC）が存在することの確認 （67ページ）
CAPF エラー コード （68 ページ）

電話機の認証文字列のトラブルシューティング

電話機に誤った認証文字列を入力すると、電話機にメッセージが表示されます。電話機に、正しい認証文字列を入力してください。

ヒント

電話機が Unified Communications Manager に登録されていることを確認します。電話機が Unified Communications Manager に登録されていないと、電話機に認証文字列を入力することができません。

電話機のデバイス セキュリティ モードが非セキュアであることを確認します。

電話機に適用されているセキュリティ プロファイルの認証モードが [認証ストリング（By Authentication String）] に設定されていることを確認します。

CAPF では、電話機に認証文字列を連続して入力できる回数が制限されています。10回連続して誤った認証文字列を入力した場合は、10分間以上待機してから再度正しい認証文字列を入力します。

ローカルで有効な証明書の確認に失敗した場合のトラブルシューティング

電話機では、証明書がCAPFによって発行されたバージョンではない場合、証明書の有効期限が切れている場合、CAPF 証明書がクラスタ内のすべてのサーバに存在しない場合、CAPF 証明書が CAPF ディレクトリに存在しない場合、電話機が Cisco Unified Communications Manager に登録されていない場合などに、ローカルで有効な証明書の確認が失敗します。ローカルで有効な証明書の確認に失敗した場合は、SDL トレース ファイルおよび CAPF トレース ファイルでエラーを確認します。

CAPF 証明書がクラスタ内のすべてのサーバにインストールされていることの確認

Cisco Certificate Authority Proxy Function サービスをアクティブにすると、CAPF 固有のキー ペアおよび証明書が CAPF によって自動的に生成されます。Cisco CTL クライアントがクラスタ内のすべてのサーバにコピーする CAPF 証明書の拡張子は .0 です。CAPF 証明書が存在することを確認するには、Cisco Unified Communications プラットフォームの GUI で CAPF 証明書を表示するか、または CLI を使用します。

- DER 符号化形式：CAPF.cer

- PEM 符号化形式：CAPF.cer と同じ通常名ストリングを含む拡張子が .0 のファイル

電話機にローカルで有効な証明書が存在することの確認

[モデル情報（Model Information）] または [セキュリティ設定（Security Configuration）] 電話機メニューでLSC設定を表示することによって、電話機にローカルで有効な証明書がインストールされていることを確認できます。詳細については、電話機のモデルとタイプ（SCCP または SIP）に応じた『*Cisco Unified IP Phone Administration Guide*』を参照してください。

電話機に製造元でインストールされる証明書（MIC）が存在することの確認

[モデル情報（Model Information）] または [セキュリティ設定（Security Configuration）] 電話機メニューで MIC 設定を表示することによって、電話機に MIC が存在することを確認できます。詳細については、電話機のモデルとタイプ（SCCP または SIP）に応じた『*Cisco Unified IP Phone Administration Guide*』を参照してください。

電話機および Cisco IOS MGCP ゲートウェイの暗号化のトラブルシューティング

ここでは、電話機および Cisco IOS MGCP ゲートウェイの暗号化のトラブルシューティングについて説明します。

関連トピック

パケット キャプチャの使用 （67 ページ）

パケット キャプチャの使用

メディアやTCPパケットをスニッフィングするサードパーティ製トラブルシューティング ツールは、SRTP暗号化を有効にした後は機能しません。このため、問題が発生した場合は、Unified Communications Manager Administration を使用して次のタスクを実行する必要があります。

- Unified Communications Manager とデバイスとの間で交換されるメッセージのパケットの分析（Cisco Unified IP Phone（SCCP および SIP）、Cisco IOS MGCP ゲートウェイ、H.323 ゲートウェイ、H.323/H.245/H.225 トランク、または SIP トランク）。

（注） SIP トランクでは、SRTP はサポートされていません。

- デバイス間の SRTP パケットのキャプチャ。
- メッセージからのメディア暗号キー情報の抽出、およびデバイス間のメディアの復号化。

パケット キャプチャの使用または設定、およびSRTPを使用して暗号化されたコール（およびその他すべてのコール タイプ）のキャプチャしたパケットの分析に関する詳細については、パケット キャプチャに関するトピックを参照してください。

ヒント　このタスクを複数のデバイスに対して同時に実行すると、CPU使用率が高くなり、コール処理が中断される可能性があります。このタスクは、コール処理が中断される危険性が最も少ないときに実行することを強く推奨します。

Unified Communications Managerのこのリリースと互換性がある一括管理ツールを使用することによって、電話機のパケット キャプチャ モードを設定できます。このタスクの実行方法の詳細については、『*Cisco Unified Communications Manager Bulk Administration Guide*』を参照してください。

ヒント　*Cisco Unified Communications Manager Bulk Administration* でこのタスクを実行すると、CPU 使用率が高くなり、コール処理が中断される可能性があります。このタスクは、コール処理が中断される危険性が最も少ないときに実行することを強く推奨します。

関連トピック

パケット キャプチャ （13 ページ）

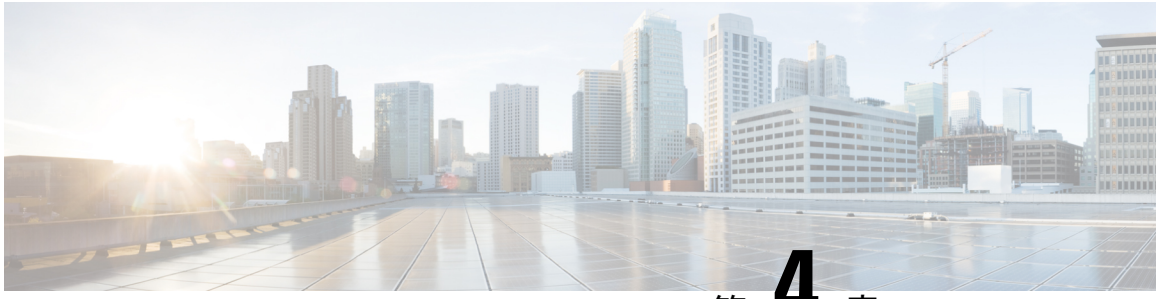
CAPF エラー コード

次の表に、CAPF ログ ファイルに出力される可能性がある CAPF エラー コード、および各コードに対応する修正処置を示します。

表 *6 : CAPF* エラー コード

エラー コード	説明	修正処置
0	CAPF_OP_SUCCESS /*Success */	修正処置は必要ありません。
1	CAPF_FETCH_SUCCESS_BUT_NO_CERT /* Fetch is successful; however there is no cert */	電話機に証明書をインストールします。詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。
2	CAPF_OP_FAIL /* Fail */	修正処置はありません。
3	CAPF_OP_FAIL_INVALID_AUTH_STR /* Invalid Authentication string */	電話機に、正しい認証文字列を入力してください。詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。

エラー コード	説明	修正処置
4	CAPF_OP_FAIL_INVALID_LSC /* Invalid LSC */	電話機のローカルで有効な証明書（LSC）を更新します。詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。
5	CAPF_OP_FAIL_INVALID_MIC, /* Invalid MIC */	このコードは、製造元でインストールされる証明書（MIC）が無効になったことを示しています。LSC をインストールする必要があります。詳細については、『*Cisco Unified Communications Manager Security Guide*』を参照してください。
6	CAPF_OP_FAIL_INVALID_CRENDENTIALS, /* Invalid credential */	正しいクレデンシャルを入力します。
7	CAPF_OP_FAIL_PHONE_COMM_ERROR, /* Phone Communication Failure*/	修正処置はありません。
8	CAPF_OP_FAIL_OP_TIMED_OUT, /* Operation timeout */	操作を再スケジュールします。
11	CAPF_OP_FAIL_LATE_REQUEST /* User Initiated Request Late */	CAPF 操作を再スケジュールします。



第 4 章

デバイスの問題

ここでは、Cisco Unified IP Phone、ゲートウェイ、および関連デバイスで発生する可能性のある一般的な問題について説明します。

音声品質

電話コール中に音声信号がなくなる、または歪むなどの音声品質の問題が発生する場合があります。ここでは、一般的な音声品質の問題について説明します。

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

- ゲートウェイ
- 電話機
- ネットワーク

関連トピック

音声の消失または歪み （72 ページ）
Cisco Unified IP Phone の音声問題の修正 （73 ページ）
エコー （75 ページ）
片通話または無音声 （76 ページ）

音声の消失または歪み

症状

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

考えられる原因

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

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

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

推奨処置

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

Unified Communications Manager Administration でサービスを無効にし、**[システム（System）] > [サービスパラメータ（Service Parameters）]** を選択します。ここで、サーバおよび Cisco CallManager サービスを選択します。

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

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

次の表は、完全なトレースを示しています。

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

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

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

Cisco Unified IP Phone の音声問題の修正

症状

音声の問題は、コールの進行中に発生します。

考えられる原因

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

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

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

推奨処置

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

- アクティブ コールで ***i*** または ***?*** ボタンを 2 回すばやく押して、統計を送受信するパケットと、平均および最大ジッタ コンテナを含む情報スクリーンを電話機に表示できます。

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

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

適切な修正を適用したあと、次の手順を実行して音声品質を確認します。

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

関連トピック

音声の消失または歪み （72 ページ）

エコー

症状

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

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

考えられる原因

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

推奨処置

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

ゲートウェイのテスト

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

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

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

エコー ログの保持

4. エコーが発生したすべてのコールのログを保持する必要があります。

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

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

ロードの確認

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

片通話または無音声

症状

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

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

考えられる原因

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

推奨処置

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

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

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

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

voice-ios-gwy(config)#ip routing

基本 IP ルーティングの確認

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

次の条件を確認してください。

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

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

- Cisco Unified IP Phone モデル 7960/40：[設定（Settings）] ボタンを押し、オプション 3 を選択して、[デフォルト ルータ（Default Router）] フィールドが表示されるまで下方向にスクロールします。

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

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

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

この問題を回避するには、H.323 シグナリングを特定の送信元アドレスにバインドします。この送信元アドレスは物理インターフェイスまたは仮想インターフェイスに割り当てることができます（ループバック）。インターフェイス コンフィギュレーション モードで使用するコマンド構文は、次のとおりです。

h323-gateway voip bind srcaddr<ip address>。Unified Communications Manager が指す IP アドレスを持つインターフェイスで、このコマンドを設定します。

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

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

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

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

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

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

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

この問題は、1 つ以上の Cisco IOS ルータ/ゲートウェイがボイス パスに含まれ、かつ Compressed RTP（cRTP）が使用されるトールバイパスなどのシナリオが該当します。cRTP または RTP Header Compression では、帯域幅取得のために VoIP パケット ヘッダをより小さくする方式が指定されます。cRTP は、VoIP パケットで 40 バイト IP/UDP/RTP ヘッダを使用し、パケットあたり 2 ~ 4 バイトに圧縮します。これにより、cRTP による G.729 のエンコード済みコールで、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、ホップごとに圧縮解除および再圧縮が行われます。ルーティングを行うにはそれぞれのパケット ヘッダーを検査する必要があるため、IP リンクの両側で cRTP をイネーブルにします。

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

要約すると、次のような履歴になります。

- Cisco IOS Software Release 12.0.5T までは、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 スイッチングとシスコ エクスプレス フォワーディング（CEF）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、アルゴリズムによるパフォーマンス改善が導入されています。

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

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

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

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

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

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

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

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

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

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

保留または転送などの補足サービスが使用されている場合、voice-fastpath コマンドを使用すると、ルータは、保留中のコールが再開されたあとや転送が完了したあとに生成された新しい論

理チャネル情報を無視して、キャッシュされている IP アドレスおよび UDP ポートに音声を送ります。この問題を回避するには、論理チャネルの再定義が考慮され、音声が新しい IP アドレスと UDP ポートのペアに送られるように、トラフィックを常にアプリケーション層に転送する必要があります。このような理由で、voice-fastpath をディセーブルにして補足サービスをサポートする必要があります。

SoftPhone を使用した VPN IP アドレスの設定

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

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

確認

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

```
voice-ios-gwy#debug cch323 rtp RTP packet tracing is enabled voice-ios-gwy#
voice-ios-gwy# voice-ios-gwy# voice-ios-gwy# voice-ios-gwy# !--- これは未応答の
発信コールです。!--- 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 *****
XXXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr

XrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
 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 *****
XXXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr

XrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr

XXrrrrrXrXrXrXrXrXrXrXrXrXrXrXrrXXrrXrXrXrXrXrXXXXXXXXXXXXXXXXrXXXXXXXXrXrXrXXrrXr
 XrXrXrXrXrXrXrXrXXrrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr !-- At this point the remote
 end picks up the phone. *Mar 3 23:53:30.378: ****** cut through in BOTH
direction *****
XRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXR

XRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXR

XXRRRXRXRXXRRXRXRXRXRXXRXRXRXRXRXRXRXXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR

XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
 XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXRXRXRXR

XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR

RRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
 XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR

XXRRRRRRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
```

```
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
 XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRRXR !-- End of conversation.
```

コーデックおよびリージョンのミスマッチ

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

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

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

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

（注） 次のリストに、各デバイスにサポートされているコーデックを示します。

- Cisco Unified IP Phone モデル 7960：G.711A-law/mu-law、G.729、G729A、G.729Annex-B
- Cisco Access Gateway DE30 および DT-24+：G.711a-law/mu-law、G.723.1

ロケーションおよび帯域幅

ユーザが番号をダイヤルした後にリオーダー トーンを受信する場合、原因として、コール エンド デバイスのいずれかのロケーションに対する Unified Communications Manager の帯域幅割り当てを超過した可能性があります。Unified Communications Manager は、コールを発信する前にデバイスごとに使用可能な帯域幅を確認します。使用可能な帯域幅がない場合、Unified Communications Manager はコールをセットアップせず、ユーザはリオーダー トーンを受信します。

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

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

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

電話機の問題

ここでは、電話機の問題について説明します。

関連トピック

電話機のリセット （82 ページ）
ドロップされたコール （83 ページ）
電話機が登録されない （84 ページ）

電話機のリセット

症状

電話機がリセットされます。

考えられる原因

電話機は次の2つの理由で電源が再投入されるか、またはリセットされます。

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

推奨処置

1. 電話機およびゲートウェイを調べて、最新のソフトウェア ロードを使用していることを確認します。
2. 最新のソフトウェア ロード、新しいパッチ、または問題に関連のあるリリース ノートがないかどうかを `www.cisco.com` で確認します。
3. シスコのCisco Unified Real-Time Monitoring ToolのSyslogビューアで、リセットされている電話機のインスタンスがないかどうかを確認します。電話機のリセットは情報イベントに相当します。

4. 電話機がリセットされた時間の前後で何らかのエラーが発生していないかどうかを調べます。
5. SDI トレースを開始し、リセットされている電話機に共通する特徴を識別して、問題を切り分けます。たとえば、これらの電話機がすべて同じサブネット、同じVLANなどに配置されていないかどうかを確認します。トレースを調べて、次の点を確認します。

   リセットはコール中に発生しているのか、断続的に発生しているのか。

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

ドロップされたコール

症状

ドロップされたコールが早期に終了します。

考えられる原因

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

推奨処置

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

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

含まれています。CDR の詳細については、『*CDR Analysis and Reporting Administration Guide*』を参照してください。

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

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

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

関連トピック

電話機のリセット （82 ページ）

電話機が登録されない

症状

5000 を超える数の電話機を登録できません。

考えられる原因

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

推奨処置

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

ゲートウェイの問題

ここでは、ゲートウェイの問題について説明します。

関連トピック

ゲートウェイのリオーダー トーン （85 ページ）
ゲートウェイの登録障害 （85 ページ）

ゲートウェイのリオーダー トーン

症状

リオーダー トーンが発生します。

考えられる原因

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

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

推奨処置

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

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

ゲートウェイの登録障害

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

症状

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

考えられる原因

登録は、さまざまな理由で失敗する可能性があります。

推奨処置

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

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

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

2. ゲートウェイが自身の IP アドレスを受信していることを確認します。スタンドアロン ゲートウェイは、DHCP または BOOTP を使用して自身の IP アドレスを受信する必要があります。Catalyst ゲートウェイは、DHCP や BOOTP を使用して、または NMP による手動設定で、自身の IP アドレスを受信することがあります。

3. DHCP サーバにアクセスできる場合、スタンドアロン ゲートウェイを確認する最善の方法は、デバイスに未処理の IP アドレス リースがないかどうかを確認することです。ゲートウェイがサーバ上に表示される場合、この方法はよい目安になりますが、決定的ではありません。DHCP サーバでリースを削除します。

4. ゲートウェイをリセットします。

5. 2 ～ 3 分以内にゲートウェイがリースとともにサーバに再表示される場合、このエリアではすべてが正常に動作します。再表示されない場合は、ゲートウェイが DHCP サーバに接続できない（ルータの設定に誤りがあり、DHCP ブロードキャストが転送されていない、サーバが稼働していないなど）、または肯定応答を取得できない（IP アドレス プールが枯渇しているなど）状態です。

6. このような確認を行っても答えが得られない場合は、スニファ トレースを使用して問題を特定します。

7. Catalyst 6000 ゲートウェイの場合、NMP がゲートウェイと確実に通信できることを確認する必要があります。これを確認するには、NMP から内部 IP アドレスに **ping** します。

   IP アドレスには次の形式が使用されます。

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

8. ping が機能している場合、**show port** コマンドを使用すると IP アドレス情報が表示されます。IP アドレス情報および TFTP IP アドレスが正しいことを確認します。

9. ゲートウェイが有効な DHCP 情報の取得に失敗している場合は、tracy ユーティリティ（Cisco TAC で提供）を使用して問題を特定します。

10. TAC からこのユーティリティを取得したあと、Cat6000 コマンドライン インターフェイス（CLI）から次のコマンドを発行します。

    tracy_start *mod port*

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

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

```
| | | | | | | | | | | | | | | | | | | | | | | | | | |:。| | | | | | | |:。C
 i s c o S y s t e m s CAT6K Analog Gateway (ELVIS) APP Version: A0020300,
 DSP Version: A0030300, Built Jun 1 2000 16:33:01 ELVIS>> 00:00:00.020
(XA) MAC Addr: 00-10-7B-00-13-DE 00:00:00.050 NMPTask:got message from XA
 Task 00:00:00.050 (NMP) Open TCP Connection ip:7f010101 00:00:00.050
NMPTask:Send Module Slot Info 00:00:00.060 NMPTask:get DIAGCMD 00:00:00.160
 (DSP) Test Begin -> Mask<0x00FFFFFF> 00:00:01.260 (DSP) Test Complete ->
 Results<0x00FFFFFF/0x00FFFFFF> 00:00:01.260 NMPTask:get VLANCONFIG
00:00:02.870 (CFG) Starting DHCP 00:00:02.870 (CFG) Booting DHCP for
dynamic configuration. 00:00:06.570 (CFG) DHCP Request or Discovery Sent,
 DHCPState = INIT_REBOOT 00:00:06.570 (CFG) DHCP Server Response Processed,
 DHCPState = INIT_REBOOT 00:00:06.780 (CFG) IP Configuration Change!
Restarting now... 00:00:10.480 (CFG) DHCP Request or Discovery Sent,
DHCPState = INIT 00:00:14:480 (CFG) DHCP Timeout Waiting on Server,
DHCPState = INIT 00:00:22:480 (CFG) DHCP Timeout Waiting on Server,
DHCPState = INIT 00:00:38:480 (CFG) DHCP Timeout Waiting on Server,
DHCPState = INIT
```

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

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

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

12. DHCP サーバが Catalyst 6000 ゲートウェイと同じ VLAN に配置されていない場合、DHCP 要求を DHCP サーバに転送するように適切な IP ヘルパー アドレスが設定されているこ

とを確認します。ゲートウェイは、VLAN番号が変更されたあと、ゲートウェイがリセットされるまで、INIT 状態のままになる可能性があります。

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

    tracy_close *mod port*

    tracy_start *mod port*

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

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

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

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

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

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

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

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

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

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

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

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

20. TFTP アドレスが正しい場合、ゲートウェイが TFTP サーバから自身の設定ファイルを取得していることを確認します。tracy 出力に次の情報が表示された場合は、TFTP サービスが正しく動作していないか、または Unified Communications Manager でゲートウェイが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
Server00:09:18.620 (CFG) TFTP Error: Timeout Awaiting Server Response
for.cnf File!
```

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

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

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

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

```
2000 Apr 14 19:24:08 %SYS-4-MODHPRESET:Host process (860) 7/1 got reset
asynchronously2000 Apr 14 19:26:05 %SYS-4-MODHPRESET:Host process (860)
7/1 got reset asynchronously 2000 Apr 14 19:28:02 %SYS-4-MODHPRESET:Host
 process (860) 7/1 got reset asynchronously The following example shows
what the tracy output would look like if the gateway is not in the Cisco
 CallManager database: 00:00:01.670 (CFG) Booting DHCP for dynamic
configuration. 00:00:05.370 (CFG) DHCP Request or Discovery Sent, DHCPState
 = INIT_REBOOT 00:00:05.370 (CFG) DHCP Server Response Processed, DHCPState
 = BOUND 00:00:05.370 (CFG) Requesting DNS Resolution of CiscoCM1
00:00:05.370 (CFG) DNS Error on Resolving TFTP Server Name. 00:00:05.370
 (CFG) TFTP Server IP Set by DHCP Option 150 = 10.123.9.2 00:00:05.370
(CFG) Requesting SAA00107B0013DE.cnf File From TFTP Server 00:00:05.370
(CFG) TFTP Error: .cnf File Not Found! 00:00:05.370 (CFG) Requesting
SAADefault.cnf File From TFTP Server 00:00:05.380 (CFG) .cnf File Received
 and Parsed Successfully. 00:00:05.380 (CFG) Updating Configuration ROM...
 00:00:05.610 GMSG: GWEvent = CFG_DONE --> GWState = SrchActive
00:00:05.610 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState =
AttemptingSocket 00:00:05.610 GMSG: Attempting TCP socket with CM
10.123.9.2 00:00:05.610 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState =
```

```
BackupUnified CM 00:00:05.610 GMSG: GWEvent = SOCKET_ACK --> GWState =
RegActive 00:00:05.610 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState =
SentRegister 00:00:05.680 GMSG: CCM#0 CPEvent = CLOSED --> CPState =
NoTCPSocket 00:00:05.680 GMSG: GWEvent = DISCONNECT --> GWState = Rollover
 00:00:20.600 GMSG: GWEvent = TIMEOUT --> GWState = SrchActive 00:00:20.600
 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState = AttemptingSocket
00:00:20.600 GMSG: Attempting TCP socket with CM 10.123.9.2 00:00:20.600
 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState = Backup CCM
```

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

```
00:00:07.390 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState =
SentRegister00:00:08.010 GMSG: TFTP Request for application load A0021300
 00:00:08.010 GMSG: CCM#0 CPEvent = LOADID --> CPState = AppLoadRequest
00:00:08.010 GMSG: ***TFTP Error: File Not Found*** 00:00:08.010 GMSG:
CCM#0 CPEvent = LOAD_UPDATE --> CPState = LoadResponse
```

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

```
ELVIS>> 00:00:00.020 (XA) MAC Addr : 00-10-7B-00-13-DE00:00:00.050
NMPTask:got message from XA Task 00:00:00.050 (NMP) Open TCP Connection
ip:7f010101 00:00:00.050 NMPTask:Send Module Slot Info 00:00:00.060
NMPTask:get DIAGCMD 00:00:00.160 (DSP) Test Begin -> Mask<0x00FFFFFF>
00:00:01.260 (DSP) Test Complete -> Results<0x00FFFFFF/0x00FFFFFF>
00:00:01.260 NMPTask:get VLANCONFIG 00:00:02.030 (CFG) Starting DHCP
00:00:02.030 (CFG) Booting DHCP for dynamic configuration. 00:00:05.730
(CFG) DHCP Request or Discovery Sent, DHCPState = INIT_REBOOT 00:00:05.730
 (CFG) DHCP Server Response Processed, DHCPState = BOUND 00:00:05.730
(CFG) Requesting DNS Resolution of CiscoCM1 00:00:05.730 (CFG) DNS Error
 on Resolving TFTP Server Name. 00:00:05.730 (CFG) TFTP Server IP Set by
 DHCP Option 150 = 10.123.9.2 00:00:05.730 (CFG) Requesting
SAA00107B0013DE.cnf File From TFTP Server 00:00:05.730 (CFG) .cnf File
Received and Parsed Successfully. 00:00:05.730 GMSG: GWEvent = CFG_DONE
--> GWState = SrchActive 00:00:05.730 GMSG: CCM#0 CPEvent = CONNECT_REQ
--> CPState = AttemptingSocket 00:00:05.730 GMSG: Attempting TCP socket
with CM 10.123.9.2 00:00:05.730 GMSG: CCM#0 CPEvent = SOCKET_ACK -->
CPState = Backup CCM 00:00:05.730 GMSG: GWEvent = SOCKET_ACK --> GWState
 = RegActive 00:00:05.730 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState
 = SentRegister 00:00:06.320 GMSG: CCM#0 CPEvent = LOADID --> CPState =
LoadResponse 00:01:36.300 GMSG: CCM#0 CPEvent = TIMEOUT --> CPState =
BadUnified CM 00:01:36.300 GMSG: GWEvent = DISCONNECT --> GWState =
Rollover 00:01:46.870 GMSG: CCM#0 CPEvent = CLOSED --> CPState =
NoTCPSocket 00:01:51.300 GMSG: GWEvent = TIMEOUT --> GWState = SrchActive
 00:01:51.300 GMSG: CCM#0 CPEvent = CONNECT_REQ --> CPState =
AttemptingSocket 00:01:51.300 GMSG: Attempting TCP socket with CM
10.123.9.2 00:01:51.300 GMSG: CCM#0 CPEvent = SOCKET_ACK --> CPState =
Backup CCM 00:01:51.300 GMSG: GWEvent = SOCKET_ACK --> GWState = RegActive
 00:01:51.300 GMSG: CCM#0 CPEvent = REGISTER_REQ --> CPState = SentRegister
 00:01:51.890 GMSG: Unified CM#0 CPEvent = LOADID --> CPState =
LoadResponse
```

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

ゲートキーパーの問題

ゲートキーパーのトラブルシューティングを開始する前に、ネットワーク内に IP 接続が存在することを確認します。ここでは、IP 接続が存在するという前提で、ゲートキーパー コールのトラブルシューティングに進みます。

関連トピック

アドミッション拒否 （91 ページ）
登録拒否 （92 ページ）

アドミッション拒否

症状

Unified Communications Manager がゲートキーパーに登録されていても電話コールを送信できず、システムからアドミッション拒否（ARJ）が発行されます。

考えられる原因

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

推奨処置

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

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

考えられる原因

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

推奨処置

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

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

症状

Unified Communications Manager システムでチャネル利用不可という原因 IE の Release Complete を受信したときに、システムから Restart が送信され、このチャネルがアイドル状態に戻されます。

考えられる原因

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

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

Unified Communications Manager サーバではチャネルがロックされているため、Unified Communications Manager は、このチャネルに対するすべてのコール要求を解放します。

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

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

この状態は、大量のコールが発生するサイトで頻繁に発生します。

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

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

推奨処置

E1 ポートをリセットします。

検証

B チャネルがアイドル状態に戻ります。

不正なデバイス登録ステータスが表示される

症状

Unified Communications Manager Administration のデバイス ウィンドウに、不正なデバイス登録ステータスが表示されます。

考えられる原因

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

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

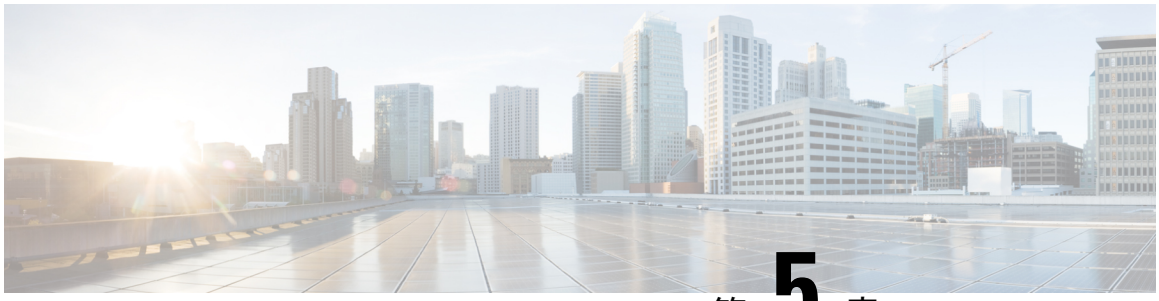
ネットワーク接続の問題またはDNS名前解決の問題が存在しているため、Unified Communications Manager Administration で Cisco RIS Data Collector サービスとの通信を確立できない。

推奨処置

1. Cisco Unified Serviceability を使用して、Cisco RIS Data Collector サービスが実行していることを確認します。サービスが実行している場合は、サービスを再起動します。サービス ステータスの確認およびサービスの再起動に関する詳細については、『Cisco Unified Serviceability Administration Guide』を参照してください。
2. 次の点を確認します。
   - DNS サーバが適切に設定され、使用可能になっている。
   - ホスト ファイルに、Unified Communications Manager サーバに対する適切なマッピングが含まれている。

- クラスタ内の Unified Communications Manager サーバに DNS 解決の問題がない。
- ローカル サーバ名をホストファイルに追加して、ipconfig /flushdns、ipconfig /registerdns、iisrest を実行している。

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



第 5 章

ダイヤル プランとルーティングの問題

ここでは、ダイヤル プラン、ルート パーティション、およびコーリング サーチ スペースで発生する可能性のある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リング サーチ スペース

ルート パーティションは、Unified Communications Manager 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、パーティションおよびコーリング サーチ スペースの設定方法、各パーティションとそれに関連付けられたコーリング サーチ スペースにあるどのデバイスがあるかを把握しておく必要があります。コールの発信に使用できる番号はコーリング サーチ スペースによって決定されます。デバイスまたはルート リストに許可されるコールはパーティションによって決定されます。

詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』のルート プランの章を参照してください。

次のトレースは、デバイスのコーリング サーチ スペースにあるダイヤル番号の例を示しています。SDI トレースの詳細な説明については、このマニュアルに記載されているケース スタディを参照してください。

```
08:38:54.968 CCM Communications Manager|StationInit - InboundStim -
OffHookMessageID tcpHandle=0x6b8802808:38:54.968 CCM CallManager|StationD -
stationOutputDisplayText tcpHandle=0x6b88028, Display= 5000 08:38:54.968 CCM
CallManager|StationD - stationOutputSetLamp stim: 9=Line instance=1
lampMode=LampOn tcpHandle=0x6b88028 08:38:54.968 CCM CallManager|StationD -
stationOutputCallState tcpHandle=0x6b88028 08:38:54.968 CCM CallManager|StationD
 - stationOutputDisplayPromptStatus tcpHandle=0x6b88028 08:38:54.968 CCM
CallManager|StationD - stationOutputSelectSoftKeys tcpHandle=0x6b88028
08:38:54.968 CCM CallManager|StationD - stationOutputActivateCallPlane
tcpHandle=0x6b88028 08:38:54.968 CCM 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、コールを発信しているデバイスがパーティション サーチ スペース（PSS：コーリング サーチ スペースとも呼ばれます）によってリストされています。

次のトレースでは、このデバイスがコールを許可されているパーティションがRTP_NC_Hardwood;RTP_NC_Woodland;Local_RTP で示されています。

```
08:38:54.968 CCM CallManager|Digit analysis:
potentialMatches=PotentialMatchesExist08:38:54.968 CCM CallManager|StationD -
 stationOutputStartTone: 33=InsideDialTone tcpHandle=0x6b88028 08:38:55.671
CCM CallManager|StationInit - InboundStim - KeypadButtonMessageID kpButton: 5
 tcpHandle=0x6b88028 08:38:55.671 CCM CallManager|StationD -
stationOutputStopTone tcpHandle=0x6b88028 08:38:55.671 CCM CallManager|StationD
 - stationOutputSelectSoftKeys tcpHandle=0x6b88028 08:38:55.671 CCM
CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="5") 08:38:55.671 CCM
CallManager|Digit analysis: potentialMatches=PotentialMatchesExist 08:38:56.015
 CCM CallManager|StationInit - InboundStim - KeypadButtonMessageID kpButton:
0 tcpHandle=0x6b88028 08:38:56.015 CCM CallManager|Digit analysis:
match(fqcn="5000", cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP",
 dd="50") 08:38:56.015 CCM CallManager|Digit analysis:
potentialMatches=PotentialMatchesExist 08:38:56.187 CCM CallManager|StationInit
 - InboundStim - KeypadButtonMessageID kpButton: 0 tcpHandle=0x6b88028
08:38:56.187 CCM CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="500") 08:38:56.187 CCM
CallManager|Digit analysis: potentialMatches=PotentialMatchesExist 08:38:56.515
 CCM CallManager|StationInit - InboundStim - KeypadButtonMessageID kpButton:
3 tcpHandle=0x6b88028 08:38:56.515 CCM CallManager|Digit analysis:
match(fqcn="5000", cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP",
 dd="5003") 08:38:56.515 CCM CallManager|Digit analysis: analysis results
08:38:56.515 CCM CallManager||PretransformCallingPartyNumber=5000
```

PotentialMatchesExist は、完全一致が見つかり、それに従ってコールがルーティングされるまでにダイヤルされた番号の番号分析結果になることに注意してください。

次のトレースは、Unified Communications Manager で電話番号 1001 をダイヤルしようとしたときに、該当するデバイスのコーリング サーチ スペースにその番号がなかった場合の動作を示しています。ここでも、番号分析ルーチンが、最初の番号がダイヤルされるまで可能性のある一致を保持していること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、デバイスのコーリング サーチ スペースであるRTP_NC_Hardwood;RTP_NC_Woodland;Local_RTP にないパーティションに存在します。このため、電話機ではリオーダー トーン（ビジー信号）を受信しました。

```
08:38:58.734 CCM CallManager|StationInit - InboundStim - OffHookMessageID
tcpHandle=0x6b8802808:38:58.734 CCM CallManager|StationD -
stationOutputDisplayText tcpHandle=0x6b88028, Display= 5000 08:38:58.734 CCM
CallManager|StationD - stationOutputSetLamp stim: 9=Line instance=1
lampMode=LampOn tcpHandle=0x6b88028 08:38:58.734 CCM CallManager|StationD -
stationOutputCallState tcpHandle=0x6b88028 08:38:58.734 CCM CallManager|StationD
 - stationOutputDisplayPromptStatus tcpHandle=0x6b88028 08:38:58.734 CCM
CallManager|StationD - stationOutputSelectSoftKeys tcpHandle=0x6b88028
08:38:58.734 CCM CallManager|StationD - stationOutputActivateCallPlane
tcpHandle=0x6b88028 08:38:58.734 CCM CallManager|Digit analysis:
```

```
match(fqcn="5000", cn="5000", pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP",
 dd="") 08:38:58.734 CCM CallManager|Digit analysis:
potentialMatches=PotentialMatchesExist 08:38:58.734 CCM CallManager|StationD
- stationOutputStartTone: 33=InsideDialTone tcpHandle=0x6b88028 08:38:59.703
CCM CallManager|StationInit - InboundStim - KeypadButtonMessageID kpButton: 1
 tcpHandle=0x6b88028 08:38:59.703 CCM CallManager|StationD -
stationOutputStopTone tcpHandle=0x6b88028 08:38:59.703 CCM CallManager|StationD
 - stationOutputSelectSoftKeys tcpHandle=0x6b88028 08:38:59.703 CCM
CallManager|Digit analysis: match(fqcn="5000", cn="5000",
pss="RTP_NC_Hardwood:RTP_NC_Woodland:Local RTP", dd="1") 08:38:59.703 CCM
CallManager|Digit analysis: potentialMatches=NoPotentialMatchesExist 08:38:59.703
 CCM 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すべての電話番号に関連付けることによって機能します。電話番号に発信できるのは、発信側デバイスに含まれているパーティションが、コールの発信先として発信側デバイスに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 サーチ スペース）にある場合だけです。これにより、ルーティングを強力に制御することが可能です。

コールの発信中に、番号分析では、ダイヤルされたアドレスをパーティション サーチ スペースで指定されているパーティション内でだけ解決しようとします。各パーティション名は、グローバルなダイヤル可能アドレスの個別のサブセットで構成されています。番号分析では、ダイヤルされた一連の番号に最もよく一致するパターンを、リストされた各パーティションから抽出します。次に、一致したパターンの中からベストマッチを選択します。ダイヤルされた一連の番号に一致するパターンが 2 つある場合は、パーティション サーチ スペースの最初にリスト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を選択します。

グループ ピックアップの設定

症状

パーティションが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機能しません。

考えられる原因

コーリング サーチ スペース（CSS）が、グループ内の各電話番号（DN）に対して適切に設定されていない可能性があります。

例

次の手順では、パーティションを使用した正しいグループ ピックアップ設定の例を示します。

1. Marketing/5656 という名前のピックアップ グループを設定します。*Marketing* はパーティション、5656 はピックアップ番号です。
2. DN 6000 と DN 7000 それぞれの設定で、これらの DN を *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 ピックアップに失敗する場合は、各ドメイン名（この例では DN 6000 と DN 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各 CSS に含まれていない場合は、設定が間違っており、ピックアップに失敗した可能性があります。

ダイヤル プランの問題

ここでは、ダイヤル プランの問題について説明します。

関連トピック

番号のダイヤル時の問題 （98 ページ）
安全なダイヤル プラン （100 ページ）

番号のダイヤル時の問題

症状

番号のダイヤル時に問題が発生します。

考えられる原因

ダイヤルプランは、番号と番号のグループのリストで構成され、特定の連続する数字が収集されたときにどのデバイス（電話機やゲートウェイなど）にコールを送信するかを Unified Communications Manager に通知するものです。このセットアップはルータの静的ルーティングテーブルに相当すると考えてください。

ダイヤルプランの潜在的な問題をトラブルシューティングする前に、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慎重に考慮され、適切に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、『*System Configuration Guide for Cisco Unified Communications Manager*』のルート プラン設定の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電話番号（DN）を特定します。
2. この DN のコーリング サーチ スペースを特定します。

ヒント　コールの発信に使用できる番号はコーリング サーチ スペースによって決定されます。

3. 必要に応じて、コーリング サーチ スペースによってこの DN に関連付けられているデバイスを特定します。正しいデバイスを特定していることを確認してください。複数のライン アピアランスがサポートされているため、複数のデバイスに同じ DN が設定されている可能性があります。デバイス コーリング サーチ スペースを追跡します。

コールの発信元が Cisco Unified IP Phone の場合は、特定の回線（DN）と回線が関連付けられているデバイスにコーリング サーチ スペースがあることに注意してください。コーリング サーチ スペースはコール発信時に結合されます。たとえば、回線インスタンス 1000 にコーリング サーチ スペース AccessLevelX があり、内線 1000 が設定されている Cisco Unified IP Phone にコーリング サーチ スペース AccessLevelY がある場合、ライン アピアランスからコールを発信すると、Unified Communications Manager では、コーリング サーチ スペース AccessLevelX と AccessLevelY に含まれるパーティション内で検索が行われます。

4. コーリング サーチ スペースに関連付けられているパーティションを特定します。

ヒント　デバイスまたはルート リストに許可されるコールはパーティションによって決定されます。

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、または送信されないかを特定します。
6. ダイヤルされている番号を特定します。ユーザが 2 次ダイヤル トーンを受信しているかどうか、およびいつ受信したかを追跡します。また、すべての番号が入力されたあとで受信している信号（リオーダー、ファースト ビジー）についても追跡します。受信する前にユーザがプログレス トーンを受信しているかどうかを確認します。発信者が番号間タイマーの時間が経過するまで待機する場合があるため、発信者が最後の番号を入力したあと少なくとも 10 秒間待機してください。
7. Unified Communications Manager Administration でルート プラン レポートを生成し、そのレポートを使用して問題のコールのコーリング サーチ スペースに含まれるパーティションのすべてのルート パターンを検査します。
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. コールの送信先ルート パターンを検出できる場合は、パターンが指すルート リストまたはゲートウェイを追跡します。
10. ルート リストの場合は、リストに含まれているルート グループとルート グループに含まれているゲートウェイを確認します。
11. 該当するデバイスが Unified Communications Manager に登録されていることを確認します。
12. ゲートウェイに Unified Communications Manager へのアクセス権限がない場合は、show tech コマンドを使用してこの情報を取得し、確認します。
13. @ 記号に注意します。このマクロは、多数の異なる機能を含めるように拡張できます。これは、多くの場合、フィルタリング オプションと組み合わせて使用されます。
14. デバイスがパーティションに含まれていない場合は、Null 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見なします。この場合、すべてのユーザがそのデバイスにコールできます。通常、Null パーティションは最後に検索されます。

15. 9.@パターンに一致する外線番号をダイヤルし、コールが成功するまで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.@ パターンの場合、7 桁の番号がダイヤルされると Cisco Unified IP Phone はコールを発信するまで 10 秒間待機します。LOCAL-AREA-CODE DOES-NOT- EXIST と END-OF-DIALING DOES-NOT-EXIST を表示するルート フィルタをパターンに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リング プランを作成するように Unified Communications Manager を設定するには、ルート パターンの @ マクロのセクションに基づくより一般的なフィルタリング（北米番号計画など）に加えて、パーティションとコーリング サーチ スペースを使用します。パーティションとコーリング サーチ 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。コーリング サーチ スペースまたはパーティション概念のサブセットであるフィルタリングによって、セキュリティ プランをさらに詳細に設定できます。

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推奨できません。十分な情報を取得できず、問題を悪化させる可能性が高くなります。

リモートゲートウェイを使用した自動代替ルーティング（AAR）の制限

症状

AAR には、AAR の使用時に広帯域の状況でリモート ゲートウェイを介してルーティングされたコールが失敗し、それらのコールをローカル ゲートウェイを介してルーティングできないという制限があります。この機能は、トール バイパスに Tail-End Hop Off（TEHO）を使用するユーザにとって重要です。

推奨処置

次の例は、AAR 使用時に広帯域の状況でリモート ゲートウェイを介してルーティングする必要があるコールの回避策を示しています。

回避策の例

対象の TEHO に特定のパーティションを使用します。

次の例では、本社（HQ）のエリア コードは 408、支社（BR1）のエリア コードは 919 です。

次のように設定します。

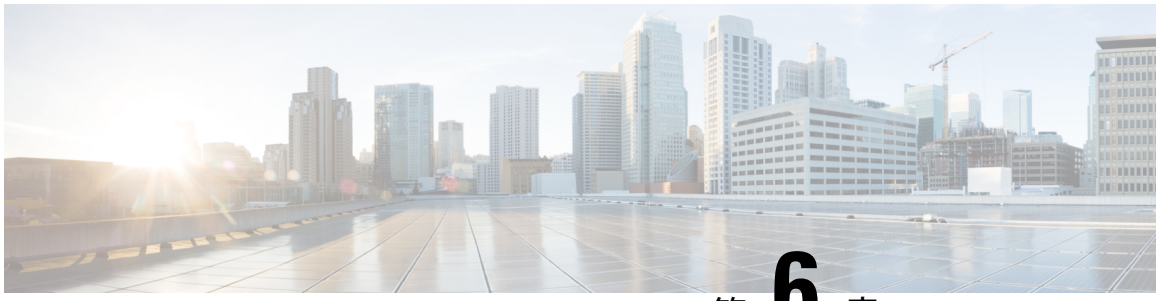
1. TehoBr1forHQPt パーティションを作成し、通常の PSTN アクセスで使用するより高い優先順位で HQ デバイスのコーリング サーチ スペース（CSS）に割り当てます。

2. TehoBr1forHQRL ルート リストを作成し、このルート リストに BR1 ゲートウェイを 1 番めのオプション、HQ ゲートウェイを 2 番めのオプションとして追加します。
3. 着信側の変更をルート リスト内で適用します。この場合、ドットの前の着信側の変更を BR1 ルート グループに適用し、ドットの前およびプレフィックス 1919 の着信側の変更を HQ ルート グループに適用します。
4. ゲートウェイでは着信側の変更を実行しないことを確認します。
5. TehoBr1forHQPt パーティションにルート パターンを作成します。
6. 着信側の変更がルート パターンに適用されないことを確認します。

結果

アウトオブバンドの状況では、Unified CM が TEHO の 1 番めのルート グループ（BR1 ルート グループ）を割り当てようとしたあと、システムが 91919 ストリングを削除して、長距離ダイヤルに最適な 1919 ストリングと置き換える時点で、Unified CM が 2 番めのルート グループを再試行します。ストリングはローカル ゲートウェイで使用するように設定されているため、再ルーティングの回数は少なくなります。

PSTN 番号の電話番号マスクがシステムでは不明なため、AAR は外部電話番号マスク ベースで動作しますが、外部 PSTN 番号用に処理できません。この回避策により AAR 機能が提供し、ネットワークの復元性が向上します。



第 6 章

Cisco Unified Communications Manager のサービスの問題

ここでは、Unified Communications Manager 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。

使用可能な会議ブリッジがない

症状

「使用可能な会議ブリッジがありません（No Conference Bridge Available）」というメッセージが表示されます。

考えられる原因

ソフトウェアまたはハードウェアの問題を示している可能性があります。

推奨処置

1. Unified Communications Manager に登録された、使用可能なソフトウェアまたはハードウェアの会議ブリッジ リソースがあるかどうかを確認します。
2. Unified Communications Manager の Cisco Unified リアルタイム監視ツールを使用して、Unicast Available Conferences の数を確認します。

   Cisco IP Voice Media Streaming アプリケーションは、会議ブリッジ機能を実行します。次のトレースに示すように、Cisco IP Voice Media Streaming の 1 つのソフトウェア インストレーションで、16 の Unicast Available Conferences（3 人/会議）がサポートされます。

（注） サポートされるデバイスの数は、Unified Communications Manager のリリースによって異なります。次の場所で、適切なバージョンの Unified Communications Manager のドキュメントを参照してください。

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

```
10:59:29.951 CCM CallManager|UnicastBridgeControl -
wait_capabilities_StationCapRes - Device= CFB_kirribilli - Registered -
ConfBridges= 16, Streams= 48, tcpHandle=4f12738 10:59:29.951 CCM
CallManager|UnicastBridgeManager - UnicastBridgeRegistrationReq - Device
Registration Complete for Name= Xoð ô%ð - DeviceType= 50, ResourcesAvailable=
 16, deviceTblIndex= 0
```

次のトレースに示すように、1 つの E1 ポート（WS-X6608-E1 カードには 8 個の E1 ポートがあります）によって、5 つの Unicast Available Conferences（最大会議サイズ = 6）が提供されます。

```
11:14:05.390 CCM CallManager|UnicastBridgeControl -
wait_capabilities_StationCapRes - Device= CFB00107B000FB0 - Registered -
ConfBridges= 5, Streams= 16, tcpHandle=4f19d64 11:14:05.480 CCM
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 and 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 Unified Communications Manager に会議ブリッジとして登録されたことを示しています。

```
greece-sup (enable) sh port 4/1Port 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 会議で設定されている最大ユーザ数を確認し、この数を超過したために問題が発生したかどうかを判別します。
4. [ロケーションの設定（Location Configuration）] ウィンドウの [オーディオ帯域幅（Audio Bandwidth）] フィールドの設定を確認します。コール帯域幅がこの設定済みの制限を超過している場合、会議は失敗します。この問題を解決するには、[無制限帯域幅（Unlimited Bandwidth）] オプション ボタンを選択します。[ロケーションの設定（Location Configuration）] ウィンドウの詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

ハードウェアトランスコーダが予期したとおりに機能しない

ハードウェア トランスコーダを Cisco Catalyst 6000 8 Port Voice T1/E1 and Services Module にインストールしましたが、予期したとおりに機能しません（共通のコーデックを持たない2人のユーザ間で通話できません）。

考えられる原因

Unified Communications Manager に登録された、使用可能なトランスコーダ リソース（ハードウェアである必要があります）がない可能性があります。

推奨処置

Unified Communications Manager の Cisco Unified リアルタイム監視ツールを使用し、Cisco MTP Device オブジェクトの ResourceAvailable カウンタを表示して、使用可能なリソース数を確認します。

次のトレースに示すように、1 つの E1 ポート（WS-X6608-E1 カードには 8 個の E1 ポートがあります）によって、16 コールのトランスコーダ/MTP リソースが提供されます。

（注） サポートされるデバイスの数は、Unified Communications Manager のリリースによって異なります。次の場所で、適切なバージョンの Unified Communications Manager のドキュメントを参照してください。

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

```
11:51:09.939 CCM CallManager|MediaTerminationPointControl - Capabilities Received
 - Device= MTP00107B000FB1 - Registered - Supports 16 calls
```

Cisco Catalyst 6000 8 Port Voice T1/E1 and 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 Unified Communications Manager に MTP/トランスコーダとして登録されたことを示しています。

```
greece-sup (enable) sh port 4/2Port 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） 同じE1ポートを会議ブリッジとトランスコーダ/MTPの両方に対して設定することはできません。

同じコーデックをサポートしない、低ビット レート コード（G.729やG.723など）を使用している 2 つのデバイス間で通話するには、トランスコーダ リソースが必要です。

Unified Communications Manager で、Region1 と Region2 の間のコーデックが G.729 に設定されているとします。次のシナリオが適用されます。

- 電話機 A の発信者がコールを開始した場合、Unified Communications Manager は、それが G.729 をサポートする Cisco Unified IP Phone モデル 7960 であることを認識します。番号が収集された後、Unified Communications Manager は、コールの宛先が Region2 にいるユーザ D であることを判別します。宛先デバイスも G.729 をサポートしているため、コールがセットアップされ、音声は電話機 A と電話機 D の間を直接流れます。
- 電話機 B の発信者が電話機 D へのコールを開始した場合、Cisco Unified Communications Manager は、今回は発信側電話機が G.723 または G.711 しかサポートしていないことを認識します。Unified Communications Manager は、トランスコーディング リソースを割り当てて、電話機 B とトランスコーダの間では音声が G.711 として流れ、トランスコーダと電話機 D の間では G.729 として流れるようにする必要があります。使用できるトランスコーダがない場合、電話機 D は鳴りますが、コールに応答するとすぐにコールが切断されます。
- 電話機 B のユーザが電話機 F にコールした場合、リージョン間で使用するコーデックとして G.729 が設定されていても、2 つの電話機は実際には 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がそれをサポートしており、使用する帯域幅が G.729 よりも少ないためです。

確立されたコールで補足サービスを使用できない

症状

コールが確立されましたが、補足サービスを使用できません。

考えられる原因

コールが確立されたが H323v2 をサポートしない H.323 デバイスで補足サービスを使用できない場合、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となることがあります。

推奨処置

1. Unified Communications Manager に登録された、使用可能なソフトウェアまたはハードウェア MTP リソースがあるかどうかを判別します。

2. Unified Communications Manager の Cisco Unified リアルタイム監視ツールのパフォーマンスモニタリングを使用して、使用可能な MTP デバイスの数を確認します。

   次のトレースに示すように、MTP を使用して H.323v2 をサポートしない H.323 デバイスで補足サービスをサポートすると、1 つの MTP ソフトウェア アプリケーションで 24 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、Unified Communications Manager のリリースによって異なります。次の場所で、適切なバージョンの Unified Communications Manager のドキュメントを参照してください。

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

```
10:12:19.161 CCM CallManager|MediaTerminationPointControl - Capabilities
Received - Device= MTP_kirribilli. - Registered - Supports 24 calls
```

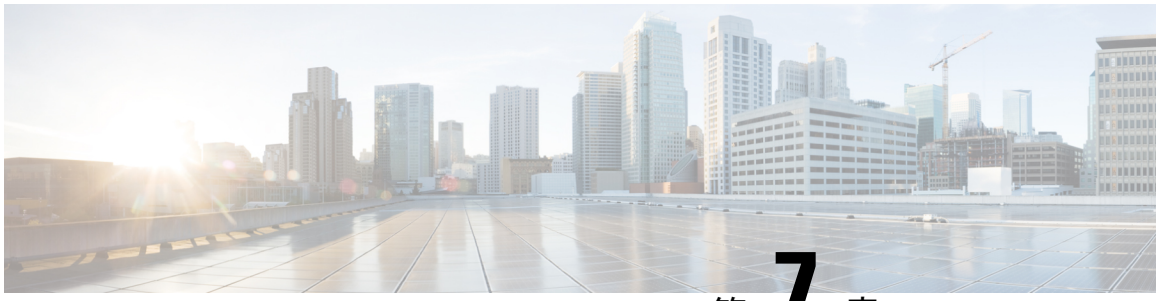
次のトレースに示すように、1 つの E1 ポート（WS-X6608-E1 カードには 8 個の E1 ポートがあります）によって、16 コールの MTP リソースが提供されます。

```
11:51:09.939 CCM CallManager|MediaTerminationPointControl - Capabilities
Received - Device= MTP00107B000FB1 - Registered - Supports 16 calls
```

Cisco Catalyst 6000 8 Port Voice T1/E1 and 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 Unified Communications Manager に MTP/トランスコーダとして登録されたことを示しています。

```
greece-sup (enable) sh port 4/2Port 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. Unified Communications Manager Administration の [ゲートウェイの設定（Gateway Configuration）] ウィンドウで、[メディアターミネーションポイントが必須（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. Unified Communications Manager によって必要な数の MTP デバイスが割り当てられていることを確認します。



第 7 章

ボイス メッセージングの問題

ここでは、一般的なボイス メッセージングの問題の解決方法について説明します。

Cisco Unity ボイス メッセージングに関する広範なトラブルシューティング情報については、次の URL にある『*Cisco Unity Troubleshooting Guide*』を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_troubleshooting_guides_list.html

Cisco Unity システム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/en/US/products/sw/voicesw/ps2237/tsd_products_support_series_home.html

ボイス メッセージングが 30 秒後に停止する

症状

Cisco Unity システムが Unified Communications Manager とともに実行されている場合、発信者がボイスメール メッセージを残すことができるのは 30 秒だけです。

考えられる原因

この問題は、発信者が音声メッセージを残しているときに発生し、コールはメッセージの開始から 30 秒で終了します。これは、有効な内線/番号をダイヤルし、30 秒を超える音声メッセージを残そうとすることで簡単に再現されます。

推奨処置

1. この問題を解決するには、メディア ゲートウェイ コントロール プロトコル（MGCP）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にない場合は、Cisco Unity サーバの Skinny トレースおよび Cisco Communications Manager トレースをイネーブルにします。

Cisco Unity 診断トレースの設定については、次の URL で該当する『*Cisco Unity Troubleshooting Guide*』の「「Diagnostic Trace Utilities and Logs」」を参照してください。

http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_troubleshooting_guides_list.html3.

Cisco Unity システムがロールオーバーされない：ビジー トーンが聞こえる

症状

Cisco Unity システムが最初の回線を通過せず、2 番めのポートにロールオーバーされません。

例

```
Call 5000 from 1001Get 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

Cisco Messaging Interface（CMI）サービスが Cisco Unity と同じ番号（5000）で設定されており、代行受信を登録しているため、コールは CMI に到達しています。

推奨処置

CMI サービス パラメータを確認し、voicemaildn パラメータが設定されていないことを確認します。

ボイス メッセージング システムに転送されるコールが Cisco Unity システムへの直接コールとして扱われる

症状

1 つの Cisco Unified IP Phone から別の Cisco Unified IP Phone へのコールがボイス メッセージング システムに転送されると、コールを発信する電話機から Cisco Unity システムへの直接コールとして扱われます。ただし、これは番号がダイヤルされた場合にだけ発生し、[リダイヤル（Redial）] ソフトキーが押された場合は正常に機能します（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、転送されたコールで originalCalledPartyName が「「Voicemail」」の場合、コールは直接コールとしてマークされます。これは、Unified Communications Manager を使用しているフェールオーバー Cisco Unity システムのために行われました。

推奨処置

1. Unified Communications Manager サーバで、Cisco Voice Mail ポートの [表示（Display）] フィールドの名前を「「VoiceMail」」以外に変更します。
2. Cisco Unity サーバで、HKLM\Software\ActiveVoice\AvSkinny\voiceMail display Name= VoiceMail 以外の名前という新しい 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

システム管理者（SA）ページにアクセスしようとしたときに、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というメッセージが表示されます。

考えられる原因

ユーザに対してアクセス権が設定されていません。

推奨処置

1. SA ページにアクセスできる適切な権限を取得するには、GrantUnityAccess ユーティリティを実行する必要があります。このツールがある場所は、**C:\commserver\grantunityaccess.exe** です。

（注） GrantUnityAccess ユーティリティの詳細については、次の URL で該当する『*Cisco Unity System Administration Guide*』の「「Accessing the Cisco Unity Administrator」」の章の「「Granting Administrative Rights to Other Cisco Unity」」を参照してください。
http://www.cisco.com/en/US/products/sw/voicesw/ps2237/prod_troubleshooting_guides_list.html

（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。

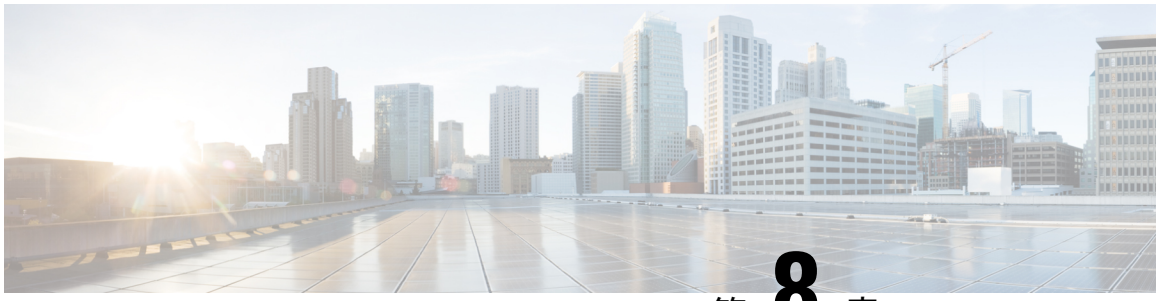
http://www.cisco.com/en/US/docs/voice_ip_comm/unity/3x/administration/guide/312/SAG_0255.html#wp1060485

2. オプションを指定しないでこのユーティリティを実行した場合、指示が表示されます。このツールの通常の使用では、SA へのアクセス権を付与するアカウントのドメイン/エイリアスを指定し、次にそれらの権限のコピー元アカウントに関する情報を指定します。

   たとえば、管理権限を付与するユーザのエイリアスが TempAdministrator であり、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.

   インストーラアカウントは常に管理権限を保持する特別なアカウントですが、ディレクトリ自体には作成されません。SQL データベースだけのローカルなアカウントです。



第 8 章

トラブルシューティングの機能とサービス

この章では、Unified Communications Manager の機能とサービスに関する一般的な問題の解決に役立つ情報を提供します。

割り込みのトラブルシューティング

ここでは、割り込み機能に関する最も一般的な問題の解決方法について説明します。

症状

[割込み（Barge）] ソフトキーを押すと、IP Phone に「使用可能な会議ブリッジがありません（No Conference Bridge Available）」というメッセージが表示されます。

考えられる原因

相手の電話機の [電話の設定（Phone Configuration）] で [ビルトイン ブリッジ（Built In Bridge）] が適切に設定されていません。

修正処置

問題を解決するには、次の手順を実行します。

手順

1. Unified Communications Manager Administration から、**[デバイス（Device）] > [電話（Phone）]** に移動し、[電話の検索（Find the phone）] をクリックして、問題がある電話機の電話機設定を見つけます。
2. [ビルトイン ブリッジ（Built In Bridge）] パラメータを [オン（On）] に設定します。
3. [更新（Update）] をクリックします。
4. 電話機をリセットします。

コールバックのトラブルシューティング

ここでは、コールバックが期待どおりに動作しない場合の症状、考えられる原因、推奨処置、およびエラー メッセージについて説明します。

関連トピック

コールバックのエラー メッセージ （116 ページ）
コールバック ログ ファイルの場所の特定 （117 ページ）
コールバック使用時の問題 （114 ページ）

コールバック使用時の問題

ここでは、問題、考えられる原因、推奨処置、および該当する場合はエラー メッセージについて説明します。

電話機が鳴る前にユーザが [コールバック（Callback）] ソフトキーを押す。

症状

コール時に、電話機がまだ鳴っていないのに電話機に [コールバック（Callback）] ソフトキーが表示されることがあります。

考えられる原因

ユーザが [折返し（Callback）] ソフトキーを押すタイミングが適切でない可能性があります。

修正処置

ユーザは呼び出し音またはビジー信号を聞いたあとで [折返し（Callback）] ソフトキーを押す必要があります。間違ったタイミングでソフトキーを押すと、電話機にエラーメッセージが表示されることがあります。

[コールバック（Callback）] ソフトキーを押したあと、コールバックが発生する前に、ユーザが電話機を取り外すかリセットする。

症状 1

[コールバック（Callback）] ソフトキーを押したあと、コールバックがアクティブになる前に、発信側の電話機がリセットされます。

考えられる原因

ユーザが電話機をリセットしました。

修正処置 1

リセット後、発信側の電話機にはコールバックのアクティブ化ウィンドウは表示されないため、発信者は、アクティブなコールバック サービスを表示するには[コールバック（Callback）] ソフトキーを押す必要があります。電話機でコールバック通知が発生します。

症状 2

コールバックがアクティブになりましたが、着信側が対応可能になる前に発信側の電話機がリセットされます。

考えられる原因

ユーザが電話機をリセットしました。

修正処置 2

修正処置は必要ありません。着信側が対応可能になる前にリセットが発生する場合は、予期したとおりにコールバックが発生します。

症状 3

コールバックがアクティブになったあとに発信側の電話機がリセットされましたが、リセットが完了する前に着信側が対応可能になります。

考えられる原因

ユーザが電話機をリセットしました。

修正処置 3

コールバック通知は自動的には発生しないため、アクティブなコールバック サービスを表示するには、発信者が [コールバック（Callback）] ソフトキーを押す必要があります。

発信者が対応可能通知に気付かずに電話機をリセットする。置換/保持画面に対応可能通知が発生したことが明示的に示されない。

症状

クラスタ内コールバックまたはクラスタ間コールバックのシナリオで、発信者が対応不可のユーザ（ユーザ B とする）に対してコールバックを開始しました。ユーザ B が対応可能になると、発信側の電話機に対応可能通知画面が表示されます。発信者が何らかの理由で対応可能通知に気付かず、電話機がリセットされました。

たとえば、発信者が別のユーザ（ユーザ C とする）に連絡し、ユーザ C が通話中だったため [コールバック（Callback）] ソフトキーを押します。発信側の電話機に置換/保持画面が表示されますが、ユーザ B の対応可能通知がすでに発生したことが画面に示されません。

考えられる原因

ユーザが電話機をリセットしました。

修正処置

電話機のリセット後、アクティブなコール中でないときに電話機のコールバック通知を確認します。[コールバック（Callback）] ソフトキーを押します。

コールバックのエラー メッセージ

ここでは、電話機に表示される可能性のあるエラー メッセージについて説明します。

エラー メッセージ コールバックがアクティブになっていません。[終了] を押してこの画面を終了してください。（Call Back is not active. Press Exit to quit this screen.）

説明 ユーザはアイドル状態のときに [コールバック（CallBack）] ソフトキーを押しています。

推奨処置 推奨処置はエラー メッセージに示されています。

エラー メッセージ コールバックはすでに xxxx でアクティブになっています。Press OK to activate on yyyy. [終了] を押してこの画面を終了してください。（CallBack is already active on xxxx. Press OK to activate on yyyy. Press Exit to quit this screen.）

説明 ユーザがコールバックをアクティブにしようとしましたが、すでにアクティブになっています。

推奨処置 推奨処置はエラー メッセージに示されています。

エラー メッセージ xxxx でコールバックをアクティブにできません（CallBack cannot be activated for xxxx.）

説明 ユーザがコールバックをアクティブにしようとしましたが、該当する内線がデータベース内に見つかりません。

推奨処置 再試行が必要です。または、管理者が Unified Communications Manager Administration にディレクトリ番号を追加する必要があります。

エラー メッセージ サービスがアクティブになっていません（Service is not active.）

説明 Callback Enabled Flag サービス パラメータを **False** に設定しているため、機能がディセーブルになったままです。

推奨処置 コールバック機能について、Cisco CallManager サービス パラメータ「Callback Enabled Flag」を **True** に設定します。

コールバック ログ ファイルの場所の特定

コールバック機能のトレースは、Cisco Communications Manager、CTIManager SDL、および SDI のレコードとして存在します。トレースへのアクセス方法については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

コール制御ディスカバリのトラブルシューティング

次のアラームでは、コール制御ディスカバリ機能がサポートされています。Cisco Unified Serviceability のアラーム定義にアクセスするには、**[アラーム（Alarm）] > [定義（Definitions）]** を選択します。アラームでは、CallManager アラーム カタログ（**[CallManager アラーム カタログ（CallManager Alarm Catalog）] > [CallManager]** を選択）がサポートされています。

- SAFUnknownService
  - 情報アラーム
  - Unified Communications Manager で、SAF フォワーダが発行した発行取り消しまたは撤回メッセージ内のサービス ID が認識されません。
- SAFPublishRevoke
  - 情報アラーム
  - このアラームに指定されているサービス ID またはサブサービス ID に対する発行アクションを取り消すために、CLI コマンドを SAF フォワーダ ルータ上で発行しました。
- DuplicateLearnedPattern
  - エラー アラーム
  - コール制御ディスカバリ要求サービスで、同じホステッド DN を複数のリモートコール制御エンティティから受け取りました。このアラームを発行するかどうかは、Issue Alarm for Duplicate Learned Patterns パラメータで制御されます。

- RTMT で学習パターン レポートを開き、このアラームで指定されている重複パターンを見つけます。学習パターンが固有であることを確認します。重複パターンが存在しないように変更する必要があるリモートコール制御エンティティを判別します。

- CCDIPReachableTimeOut
  - エラー アラーム
  - CCD 要求サービスは、IP を通じて学習したパターンに到達できなくなったことを検出しました。この SAF フォワーダからのすべての学習パターンは（IP 経由では）到達不能とマークされ、学習パターンへのすべてのコールは PSTN 経由でルーティングされます。コールは PSTN フェールオーバーがタイムアウトになるまでの指定の時間、PSTN 経由でルーティングされます。
  - IP 接続を確認し、ネットワークの TCP または IP の問題を解決します。

- CCDPSTNFailOverDurationTimeOut
  - エラー アラーム
  - 学習したパターンが IP 経由で到達不可能な場合、Unified Communications Manager は PSTN を通じてコールをルーティングします。このアラームが発生した場合は、PSTN フェールオーバーの時間が経過したため、学習パターンへのコールをルーティングできません。すべての学習パターンが Unified Communications Manager から消去されます。
  - ネットワークのトラブルシューティングを行い、IP 接続を復旧します。IP 接続が復旧すると、Unified Communications Manager によって自動的にパターンが再学習され、学習パターンへのコールは自動的に IP 経由で処理されます。

- CCDLearnedPatternLimitReached
  - 警告アラーム
  - このアラームは、CCD 要求サービスで学習パターンの数が許可される最大数に達したことを示します。
  - このアラームでは、CCD Maximum Numbers of Learned Patterns パラメータに設定されている値と、システムで許可されている学習パターンの最大数（20,000）が表示されます。指定した学習可能パターンの最大数が展開環境にとって適切であるかどうかを検討します。値が小さすぎる場合は、このアラームの SystemLimitCCDLearnedPatterns に表示されている数値と比較します。最大数がシステム制限（学習パターン 20,000 個）よりも低い場合は、CCD Maximum Numbers of Learned Patterns パラメータの値を大きくします。

- LostConnectionToSAFForwarder
  - エラー アラーム
  - TCP 接続障害により、SAF フォワーダと Unified Communications Manager の間の接続が失われました。TCP 接続が復旧すると、Unified Communications Manager は SAF フォ

ワーダに自動的に接続しようとします。IP接続がCCDLearnedPatternIPReachableDuration機能パラメータの指定時間を過ぎても到達不能な場合、学習パターンへのコールはIPの代わりにPSTN経由でルーティングされます。学習パターンへのPSTN経由のコールは、PSTNフェールオーバーがタイムアウトになるまでの指定の時間、保持されます。

- 電源障害、ケーブル接続のゆるみ、スイッチ設定の誤りなど、TCP接続エラーについて考えられる原因を調べます。

- SAFForwarderError
  - Unified Communications Managerで SAFフォワーダからエラーを受信しました。
  - このアラームが発生した原因について、原因コード、特定の情報の説明、該当する場合は対処方法を参照します。

    たとえば、原因コード472は、外部クライアント（この場合はUnified Communications Manager）がサービス バージョン番号を正しくインクリメントしなかったことを示します。原因コード474は、外部クライアント（この場合はUnified Communications Manager）がSAFフォワーダに登録する前に、発行要求をTCP接続経由でフォワーダに送信したことを示します。原因コード400は、外部クライアント（この場合はUnified Communications Manager）がSAFメッセージを正しく作成しなかったことを示します。

コール パークのトラブルシューティング

次の表に、コール パークの一般的な問題を復元するためのトラブルシューティング ヒントを示します。

表 7: コール パークのトラブルシューティングのヒント

問題の説明	推奨処置
コールをパークできない。[パーク（Park）]ソフトキーまたは機能ボタンを押してもコールがパークされません。	クラスタ内の各Unified Communications Managerに固有のコール パーク番号が割り当てられていることを確認します。『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。 コール パーク番号に割り当てられているパーティションと電話機の電話番号に割り当てられているパーティションが一致しません。『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

問題の説明	推奨処置
コール パーク番号の表示時間が短すぎる。	コール パーク表示タイマーに、より長い時間を設定します。コール パークの設定パラメータについては、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

Cisco Extension Mobility のトラブルシューティング

Cisco Extension Mobility には、管理者用のトラブルシューティング ツールが用意されています。これらのツールには、パフォーマンス カウンタ（perfmon とも呼ばれる）や Cisco Unified Serviceability に組み込まれているアラームなどがあります。パフォーマンス カウンタ（perfmon）の詳細については、『*Cisco Unified Real-Time Monitoring Tool Administration Guide*』を参照してください。アラームの詳細については、『*Cisco Unified Serviceability Administration Guide*』を参照してください。

ここでは、Cisco Communications Manager Extension Mobility に関する問題のトラブルシューティングに役立つ次の情報について説明します。

関連トピック

Cisco Extension Mobility のエラー メッセージのトラブルシューティング （121 ページ）
Cisco Extension Mobility の一般的な問題のトラブルシューティング （120 ページ）

Cisco Extension Mobility の一般的な問題のトラブルシューティング

Cisco Extension Mobility で問題が発生した場合は、次のトラブルシューティングのヒントから始めてください。

- Cisco Extension Mobility トレース ディレクトリを設定し、次の手順を実行してデバッグ トレースをイネーブルにします。
  - Cisco Unified Serviceability から **[トレース（Trace）] > [トレース設定（Trace Configuration）]** を選択します。
  - [サーバ（Servers）] ドロップダウン リスト ボックスからサーバを選択します。
  - [設定されているサービス（Configured Services）] のドロップダウン メニューから、[Cisco Extension Mobility] を選択します。
- Cisco Extension Mobility サービスの URL を正しく入力したことを確認します。URL では、小文字と大文字が区別されます。
- 設定手順をすべて適切に実行したことを確認します。
- Cisco Extension Mobility ユーザの認証で問題が発生する場合は、ユーザ ページに移動して PIN を確認します。

上記の手順で問題が解決しない場合は、次の表にあるトラブルシューティングの解決方法を使用してください。

表 *8 : Cisco Unified Communications Manager Extension Mobility* のトラブルシューティング

問題の説明	推奨処置
ユーザがログアウトし、電話機がデフォルト デバイス プロファイルに戻ったあと、電話サービスが使用できなくなる。	**1.** エンタープライズ パラメータを調べ、Synchronization Between Auto Device Profile and Phone Configuration が **True** に設定されていることを確認します。 **2.** 電話機を Cisco Extension Mobility サービスに登録します。
ログイン後、電話サービスが使用できない。	この問題は、電話機にユーザ プロファイルがロードされたとき、関連付けられたサービスがプロファイルになかったために発生します。 次の操作を行ってください。 **1.** Cisco Extension Mobility サービスが含まれるようにユーザ プロファイルを変更します。 **2.** Cisco Extension Mobility が含まれるように、ユーザがログインする電話機の設定を変更します。電話機が更新されたあと、ユーザは電話サービスにアクセスできるようになります。
ログインまたはログアウト後に、電話機の再起動ではなくリセットが発生する。	ロケールの変更が原因でリセットが発生することがあります。 ログイン ユーザまたはプロファイルに関連付けられているユーザ ロケールがロケールまたはデバイスと異なる場合、ログインが正常に完了すると、電話機は再起動を実行し、次にリセットを実行します。これは、電話機設定ファイルが再作成されるために発生します。

Cisco Extension Mobility のエラー メッセージのトラブルシューティング

Cisco Extension Mobility の使用中に電話機に表示されるエラー コードとエラー メッセージのトラブルシューティングを行うには、次の表の情報を使用してください。

表 *9*：電話機に表示されるエラー メッセージのトラブルシューティング

エラー コード	電話機のメッセージ	推奨処置
201	[201]- 認証エラー（Authentication error）	ユーザ ID と PIN を正しく入力したことをユーザが確認します。また、ユーザ ID と PIN が正しいことをシステム管理者に確認する必要があります。
22	[22]- デバイスのログインが無効です（Dev.logon disabled）	[電話の設定（Phone Configuration）] ウィンドウの [Extension Mobility の有効化（Enable Extension Mobility）]「」チェックボックスをオンにしていることを確認します。『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。
205	[205]- ユーザ プロファイルなし（User Profile Absent）	デバイスプロファイルをユーザに関連付けていることを確認します。『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。
208	[208]- EMService 接続エラー（EMService Conn. error）	**[Cisco Unified Serviceability]** > **[ツール（Tools）]** > **[コントロール センターの機能サービス（Control Center—Feature Services）]** を選択し、Cisco Extension Mobility サービスが実行されていることを確認します。
25	[25]-ユーザは既にログインしています（User logged in elsewhe..）	ユーザが別の電話機にログインしているかどうかを確認します。複数のログインを許可する必要がある場合は、Multiple Login Behavior サービス パラメータが Multiple Logins Allowed に設定されていることを確認します。
	ホストを検出できません（Host not found）	**[Cisco Unified Serviceability]** > **[ツール（Tools）]** > **[コントロール センターのネットワーク サービス（Control Center—Network Services）]** を選択し、Cisco Tomcat サービスが実行されていることを確認します。

エラー コード	電話機のメッセージ	推奨処置
	HTTP エラー [503]（Http Error [503]）	[サービス（Services）]ボタンを押したときにこのエラーが表示された場合は、**[Cisco Unified Serviceability]** > **[ツール（Tools）]** > **[コントロール センターのネットワーク サービス（Control Center—Network Services）]** を選択し、Cisco Communications Manager の Cisco IP Phone Services サービスが実行されていることを確認します。 Extension Mobility サービスを選択したときにこのエラーが表示された場合は、**[Cisco Unified Serviceability]** > **[ツール（Tools）]** > **[コントロール センターのネットワーク サービス（Control Center—Network Services）]** を選択し、Cisco Extension Mobility アプリケーション サービスが実行されていることを確認します。
202	[202]- ユーザ ID または PIN が空です（Blank userid or pin）	有効なユーザ ID と PIN を入力します。
26	[26]- ビジー。再実行してください。（Busy, please try again）	同時ログイン/ログアウト要求の数が Maximum Concurrent requests サービス パラメータよりも大きいかどうかを確認します。大きい場合は同時要求の数を小さくします。 同時ログイン/ログアウト要求の数を確認するには、Cisco Unified Communications Manager の Cisco Unified リアルタイム監視ツールを使用して、Extension Mobility オブジェクトの Requests In Progress カウンタを表示します。

エラー コード	電話機のメッセージ	推奨処置
6	[6]- データベース エラー（Database Error）	大量の要求が存在するどうかを確認します。 大量の要求が存在する場合、Extension Mobility カウンタの Requests In Progress カウンタに高い値が指定されています。同時要求の数が多すぎるため要求が拒否される場合は、Requests Throttled カウンタにも高い値が指定されています。 詳細なデータベース ログを収集します。
207	[207]- デバイス名が空白です（Device Name Empty）	Cisco Extension Mobility に設定されている URL が正しいことを確認します。

Cisco Unified Communications Manager Assistant のトラブルシューティング

ここでは、Cisco Unified Communications Manager Assistant 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。

次の表に、Unified CM Assistant とクライアント デスクトップのトラブルシューティング ツールについて説明します。

表 *10 : Cisco Unified Communications Manager Assistant* とクライアント デスクトップのためのトラブルシューティング ツール

ツールの説明	参照先
Cisco Unified CM Assistant サーバのトレース ファイル	ログ ファイルは、Cisco IP Manager Assistant サービスを実行するサーバに存在します。 これらのファイルは次のいずれかの方法でサーバからダウンロードできます。 • CLI コマンド **file get activelog tomcat/logs/ipma/log4j** を使用する。 • Unified CM の Cisco Unified Real-Time Monitoring Tool（RTMT）のトレース収集機能を使用する。詳細については、『Cisco Unified Real-Time Monitoring Tool Administration Guide』を参照してください。 デバッグ トレースをイネーブルにするには、**[Cisco Unified Serviceability]** > **[トレース（Trace）]** > **[設定（Configuration）]** を選択します。
Cisco IPMA クライアントのトレース ファイル	クライアントのデスクトップ上で、Unified CM Assistant のアシスタント コンソールと同じ場所にある `$INSTALL_DIR\logs\ACLog*.txt`。 デバッグ トレースをイネーブルにするには、アシスタントコンソールの設定ダイアログボックスに移動します。詳細設定のパネルで、[トレースを有効にする（Enable Trace）] チェックボックスをオンにします。 （注） この操作でイネーブルになるのはデバッグ トレースだけです。エラー トレースは常にオンになっています。
Cisco IPMA クライアントのインストール トレース ファイル	クライアントのデスクトップ上で、Unified CM Assistant のアシスタント コンソールと同じ場所にある `$INSTALL_DIR\InstallLog.txt`。

ツールの説明	参照先
Cisco IPMA クライアントの AutoUpdater トレース ファイル	クライアントのデスクトップ上で、Unified CM Assistant のアシスタント コンソールと同じ場所にある `$INSTALL_DIR\UpdatedLog.txt`。
インストール ディレクトリ	デフォルトでは、`C:\Program Files\Cisco\Unified Communications Manager Assistant Console\`

関連トピック

IPMAConsoleInstall.jsp で「HTTP ステータス 503：アプリケーションは現在使用できません（HTTP Status 503-This Application is Not Currently Available）」エラーが表示される （127 ページ）
IPMAConsoleInstall.jsp で「ページが見つかりません（No Page Found）」エラーが表示される （127 ページ）
例外：java.lang.ClassNotFoundException: InstallerApplet.class（Exception: java.lang.ClassNotFoundException: InstallerApplet.class） （128 ページ）
MS 仮想マシンの自動インストールのダウンロードは提供されなくなりました（Automatic Installation of MS Virtual Machine Is No Longer Provided for Download） （128 ページ）
ユーザ認証に失敗する （129 ページ）
アシスタント コンソールに「システム エラーが発生しました。システム管理者にお問い合わせください（System Error - Contact System Administrator）」エラーが表示される （130 ページ）
アシスタント コンソールに「Cisco IP Manager Assistant サービスに到達できません（Cisco IP Manager Assistant Service Unreachable）」エラーが表示される （131 ページ）
フィルタリングをオン/オフにするとコールがルーティングされない （132 ページ）
Cisco IP Manager Assistant サービスが初期化できない （133 ページ）
発呼側にリオーダー トーンが聞こえる （134 ページ）
マネージャがログアウトしてもサービスが動作している （134 ページ）
マネージャがアシスタント プロキシ回線で鳴っているコールを代行受信できない （135 ページ）
Cisco IP Manager Assistant サービスがダウンしているときにマネージャ電話機にコールできない （136 ページ）

IPMAConsoleInstall.jsp で「HTTP ステータス 503：アプリケーションは現在使用できません（HTTP Status 503-This Application is Not Currently Available）」エラーが表示される

症状

http://<サーバ名>:8443/ma/Install/IPMAConsoleInstall.jsp で次のエラー メッセージが表示されます。

HTTP ステータス 503：アプリケーションは現在使用できません（HTTP Status 503 - This Application is Not Currently Available）

考えられる原因

Cisco IP Manager Assistant サービスがアクティブになっていないか、または実行されていません。

修正処置

Cisco IP Manager Assistant サービスがアクティブになっていることを確認します。確認するには、**[Cisco Unified Serviceability] > [ツール（Tools）] > [サービスの開始（Service Activation）]** を選択し、サービスのアクティベーション ステータスを調べます。

Cisco IP Manager Assistant サービスがアクティブになっていない場合は、**[Cisco Unified Serviceability] > [ツール（Tools）] > [コントロール センターの機能サービス（Control Center—Feature Services）]** を選択し、Cisco Unified Communications Manager Assistant を再起動します。

IPMAConsoleInstall.jspで「ページが見つかりません（NoPageFound）」エラーが表示される

症状

http://<サーバ名>:8443/ma/Install/IPMAConsoleInstall.jsp で次のエラー メッセージが表示されます。

ページが見つかりません（No Page Found）

考えられる原因 1

ネットワークに問題があります。

修正処置 1

クライアントがサーバに接続していることを確認します。URL で指定されているサーバ名に対して ping を実行し、到達可能であることを確認します。

考えられる原因 2

URL のつづりが間違っています。

修正処置 2

URL では大文字と小文字が区別されるため、URL が指示と正確に一致していることを確認します。

関連トピック

Cisco Unified Communications Manager のシステムの問題 （37 ページ）

例外：java.lang.ClassNotFoundException:InstallerApplet.class（Exception: java.lang.ClassNotFoundException: InstallerApplet.class）

症状

Web からアシスタント コンソールをインストールできません。次のメッセージが表示されます。

例外：java.lang.ClassNotFoundException: InstallerApplet.class（Exception: java.lang.ClassNotFoundException: InstallerApplet.class）

考えられる原因

Cisco Unified Communications Manager Assistant Console の標準インストールで Microsoft JVM の代わりに Sun Java プラグイン仮想マシンを使用するとエラーの原因となります。

修正処置

Sun Java プラグインをサポートしている JSP ページの URL（`https://<サーバ名>:8443/ma/Install/IPMAConsoleInstallJar.jsp`）を、管理者がユーザに通知します。

MS 仮想マシンの自動インストールのダウンロードは提供されなくなりました（Automatic Installation of MS Virtual Machine Is No Longer Provided for Download）

症状

Microsoft Windows XP を実行しているコンピュータに Web からアシスタント コンソールをインストールしようとすると失敗します。プログラムのすべてのコンポーネントが使用できないというメッセージが表示されます。ユーザが [今すぐダウンロード（Download Now）] を選択すると、次のメッセージが表示されます。

MS 仮想マシンの自動インストールのダウンロードは提供されなくなりました（Automatic installation of MS Virtual Machine is no longer available for download）

考えられる原因

Microsoft Windows XP の IE バージョン 6 では Microsoft JVM はサポートされていません。

（注） システムに XP Service Pack 1 と Microsoft JVM がインストールされている場合、このエラーは発生しません。

修正処置

次のいずれかの修正処置を実行します。

- Netscape ブラウザ（バージョン 7.x）をインストールし、Netscape を使用してアシスタント コンソールをインストールします。
- 次の URL から IE 用の Sun Java 仮想マシン プラグインをインストールします。

  `http://java.sun.com/getjava/download.html`

  Sun Java プラグインのインストールが完了したら、ブラウザで次の URL を指定します。

  `https://<servername>:8443/ma/Install/IPMAInstallJar.jsp`
- アシスタント コンソールをインストールする前に、Windows XP Service Pack 1 と Microsoft Microsoft Java 仮想マシン（JVM）をインストールします。

ユーザ認証に失敗する

症状

アシスタント コンソールからログイン ウィンドウでサイン インするときにユーザ認証に失敗します。

考えられる原因

次の原因が考えられます。

- データベースでユーザが正しく管理されていない。
- アシスタントまたはマネージャとしてユーザが正しく管理されていない。

修正処置

ユーザ ID とパスワードが、Unified Communications Manager Administration を通じて Unified Communications Manager のユーザとして管理されていることを確認します。

ユーザには Unified Communications Manager Assistant のユーザ情報を関連付けて、アシスタントまたはマネージャとして管理する必要があります。ユーザ情報にアクセスするには、**Unified Communications Manager Administration** > **[ユーザ管理（User Management）]** > **[エンドユーザ（End User）]** を選択します。

アシスタント コンソールに「システム エラーが発生しました。システム管理者にお問い合わせください（System Error - Contact System Administrator）」エラーが表示される

症状

アシスタント コンソールの起動後、次のメッセージが表示されます。

システム エラーが発生しました。システム管理者にお問い合わせください（System Error - Contact System Administrator）

考えられる原因 1

Unified Communications Manager が 4.x リリースから 5.x リリースにアップグレードされている可能性があります。アシスタント コンソールは4.x リリースから 5.x リリースに自動的にはアップグレードされません。

修正処置 1

[スタート] > [プログラム] > [Cisco Unified Communications Manager Assistant] > [Assistant Console のアンインストール（Uninstall Assistant Console）] を選択してコンソールをアンインストールし、URL `https://<サーバ名>:8443/ma/Install/IPMAConsoleInstall.jsp` からコンソールを再インストールします。

考えられる原因 2

ユーザがデータベースに正しく設定されていません。

修正処置 2

ユーザ ID とパスワードが、Unified Communications Manager Administration を通じて Unified Communications Manager のユーザとして管理されていることを確認します。

ユーザには Unified Communications Manager Assistant のユーザ情報を関連付けて、アシスタントまたはマネージャとして管理する必要があります。ユーザ情報にアクセスするには、**Unified Communications Manager Assistant** > **[ユーザ管理（User Management）]** > **[エンド ユーザ（End User）]** を選択します。詳細については、『Cisco Unified Communications Manager 機能設定ガイド』を参照してください。

考えられる原因 3

アシスタントからマネージャを削除したときに、Unified Communications Manager Administration でアシスタントに空白行が残されました。

修正処置 3

[アシスタントの設定（Assistant Configuration）] ウィンドウでプロキシ行を再割り当てします。詳細については、『Cisco Unified Communications Manager 機能設定ガイド』を参照してください。

アシスタント コンソールに「Cisco IP Manager Assistant サービスに到達できません（Cisco IP Manager Assistant Service Unreachable）」エラーが表示される

症状

アシスタント コンソールの起動後、次のメッセージが表示されます。

Cisco IPMA サービスに到達できません（Cisco IPMA Service Unreachable）

考えられる原因 1

Cisco IP Manager Assistant サービスが停止している可能性があります。

修正処置 1

[Cisco Unified Serviceability] > **[ツール（Tools）]** > **[コントロールセンター-機能サービス（Control Center—Feature Services）]** を選択して、Unified Communications Manager Assistant を再起動します。

考えられる原因 2

プライマリおよびセカンダリの Unified Communications Manager Assistant サーバのサーバ アドレスがDNS名で設定されていますが、それらのDNS名がDNSサーバで設定されていません。

修正処置 2

次の手順を実行して DNS 名を置き換えます。

手順

1. **Unified Communications Manager Administration** > **[システム（System）]** > **[サーバ（Server）]** を選択します。
2. サーバの DNS 名を対応する IP アドレスに置き換えます。

3. **[Cisco Unified Serviceability]** > **[ツール（Tools）]** > **[コントロールセンター-機能サービス（Control Center—Feature Services）]** を選択して、Unified Communications Manager Assistant を再起動します。

考えられる原因 3

Cisco CTI Manager サービスが停止している可能性があります。

修正処置 3

[Cisco Unified Serviceability] > **[ツール（Tools）]** > **[コントロール センターの機能サービス（Control Center - Feature Services）]** を選択して、Cisco CTI Manager および Cisco IP Manager Assistant サービスを再起動します。

考えられる原因 4

Unified Communications Manager Assistant サービスがセキュア モードで CTI 接続をオープンするように設定されていますが、セキュリティ設定が適切でない可能性があります。

この場合、アラーム ビューアまたは Unified Communications Manager Assistant サービス ログに次のメッセージが表示されます。

IPMA サービスが初期化できません。プロバイダーを取得できませんでした（IPMA Service cannot initialize - Could not get Provider）

修正処置 4

Cisco IP Manager Assistant サービスのサービス パラメータで、セキュリティ設定を確認します。詳細については、『Cisco Unified Communications Manager 機能設定ガイド』を参照してください。

[Cisco Unified Serviceability] > **[ツール（Tools）]** > **[コントロールセンター-機能サービス（Control Center—Feature Services）]** を選択して、Unified Communications Manager Assistant を再起動します。

フィルタリングをオン/オフにするとコールがルーティングされない

症状

コールが適切にルーティングされません。

考えられる原因 1

Cisco CTI Manager サービスが停止している可能性があります。

修正処置 1

[Cisco Unified Serviceability] > [ツール（Tools）] > [コントロールセンターの機能サービス（Control Center - Feature Services）] を選択して、Cisco CTI Manager および Cisco IP Manager Assistant サービスを再起動します。

考えられる原因 2

Unified Communications Manager Assistant ルート ポイントが適切に設定されていません。

修正処置 2

Unified Communications Manager Assistant CTI ルート ポイントのディレクトリ番号と、Unified Communications Manager Assistant に設定されているすべてのマネージャのプライマリ ディレクトリ番号に一致するワイルド カードを使用します。

考えられる原因 3

マネージャの電話機のステータス ウィンドウに「フィルタ使用不可（Filtering Down）」というメッセージが表示されます。これは、Unified Communications Manager Assistant CTI ルート ポイントが削除されているか、機能していない可能性があることを示します。

修正処置 3

次の手順を実行して、CTI ルート ポイントを設定し、Cisco IP Manager Assistant サービスを再起動します。

手順

1. Unified Communications Manager Administration から、**[デバイス（Device）] > [CTIルートポイント（CTI Route Point）]** を選択します。
2. 該当するルート ポイントを見つけるか、または新しいルート ポイントを追加します。設定の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。
3. **[Cisco Unified Serviceability] > [ツール（Tools）] > [コントロール センターの機能サービス（Control Center—Feature Services）]** を選択して、Cisco IP Manager Assistant サービスを再起動します。

Cisco IP Manager Assistant サービスが初期化できない

症状

Cisco IP Manager Assistant サービスで CTI Manager への接続をオープンできず、次のメッセージが表示されます。

IPMA サービスが初期化できません。プロバイダーを取得できませんでした（IPMA Service cannot initialize - Could not get Provider）

考えられる原因

Cisco IP Manager Assistant サービスで CTIManager への接続をオープンできません。アラームビューアまたは Unified CM Assistant サービス ログでメッセージを確認できます。

修正処置

[Cisco Unified Serviceability] > **[ツール（Tools）]** > **[コントロール センターの機能サービス（Control Center - Feature Services）]** を選択して、Cisco CTI Manager および Cisco IP Manager Assistant サービスを再起動します。

発呼側にリオーダー トーンが聞こえる

症状

発呼側がリオーダー トーンまたは「「ダイヤルした電話番号を完了できません（This call cannot be completed as dialed）」」というメッセージを受信します。

考えられる原因

発呼回線のコーリング サーチ スペースを正しく設定していない可能性があります。

修正処置

回線のコーリングサーチスペースを確認します。設定の詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

また、Cisco Dialed Number Analyzer サービスを使用して、コーリング サーチ スペース内の不備を確認することもできます。詳細については、『*Cisco Unified Communications Manager Dialed Number Analyzer Guide*』を参照してください。

マネージャがログアウトしてもサービスが動作している

症状

マネージャが Unified Communications Manager Assistant からログアウトしても、サービスは継続して実行されています。マネージャの IP Phone のディスプレイの表示が消えます。フィルタリングがオンになっていますがコールはルーティングされません。マネージャがログアウトしたことを確認するには、Cisco Unified Real-Time Monitoring Tool を使用してアプリケーション ログを表示します。Cisco IP Manager Assistant サービスがログアウトされたことを示す、Cisco Java アプリケーションからの警告がないかどうかを調べます。

考えられる原因

マネージャがソフトキーを 1 秒間に 5 回以上押しました（最大許容回数は 4 回）。

修正処置

Unified Communications Managerの管理者が、マネージャの設定を更新する必要があります。次の手順を実行して問題を修正します。

手順

1. Unified Communications Manager Administration から、**[ユーザ管理（User Management）] > [エンドユーザ（End User）]** を選択します。

   [ユーザの検索と一覧表示（Find and List Users）] ウィンドウが表示されます。
2. 検索フィールドにマネージャ名を入力し、[検索（Find）] ボタンをクリックします。
3. 検索結果のリストから更新するマネージャを選択します。

   [エンド ユーザの設定（End User Configuration）] ウィンドウが表示されます。
4. [関連リンク（Related Links）] ドロップダウン リスト ボックスから [Cisco IPMA マネージャ（Cisco IPMA Manager）] を選択し、[移動（Go）] をクリックします。
5. マネージャの設定に必要な変更を行い、[更新（Update）] をクリックします。

マネージャがアシスタントプロキシ回線で鳴っているコールを代行受信できない

症状

マネージャがアシスタント プロキシ回線で呼び出しているコールを代行受信できません。

考えられる原因

プロキシ回線のコーリング サーチ スペースが適切に設定されていません。

修正処置

アシスタント電話機のプロキシ回線のコーリング サーチ スペースを確認します。次の手順を実行して問題を修正します。

手順

1. Unified Communications Manager Administration から、[デバイス（Device）] > [電話（Phone）] を選択します。

   [電話の検索と一覧表示（Find and List Phones）] 検索ウィンドウが表示されます。
2. アシスタント電話機をクリックします。

   [電話の設定（Phone Configuration）] ウィンドウが表示されます。

3. 電話機と電話番号（回線）のコーリング サーチ スペース設定を確認し、必要に応じて更新します。

Cisco IP Manager Assistant サービスがダウンしているときにマネージャ電話機にコールできない

症状

Cisco IP Manager Assistant サービスがダウンしているときに、コールがマネージャに適切にルーティングされません。

考えられる原因

Unified Communications Manager Assistant CTI ルート ポイントで無応答時転送が有効になっていません。

修正措置

次の手順を実行して、Unified Communications Manager Assistant ルート ポイントを適切に設定します。

手順

1. Unified Communications Manager Administration から、**[デバイス（Device）] > [CTIルートポイント（CTI Route Point）]** を選択します。

   [CTI ルートポイントの検索と一覧表示（Find and List CTI Route Points）] 検索ウィンドウが表示されます。

2. [検索（Find）] ボタンをクリックします。

   設定済み CTI ルート ポイントのリストが表示されます。

3. 更新する Unified Communications Manager Assistant CTI ルート ポイントを選択します。

4. [CTI ルートポイントの設定（CTI Route Point Configuration）] ウィンドウの [電話番号（Directory Numbers）] ボックスで、更新する回線をクリックします。

   [電話番号の設定（Directory Number Configuration）] ウィンドウが表示されます。

5. [コール転送とコール ピックアップの設定（Call Forward and Call Pickup Settings）] セクションで、[無応答時転送（Forward No Answer Internal、内部）] チェックボックスまたは [無応答時転送（Forward No Answer External、外部）] チェックボックスをオンにし、[カバレッジ/接続先（Coverage/Destination）] フィールドに CTI ルート ポイントの DN を入力します（たとえば、ルート ポイント DN 1xxx の場合、CFNA に 1xxx を入力します）。

6. [コーリング サーチ スペース（Calling Search Space）] ドロップダウン リスト ボックスから CSS-M-E（または、該当するコーリング サーチ スペース）を選択します。

7. [更新（Update）] ボタンをクリックします。

Cisco Unified Mobility のトラブルシューティング

ここでは、Cisco Unified Mobility に関する問題のトラブルシューティングに役立つ情報について説明します。

関連トピック

Cisco Unified Mobility ユーザが携帯電話を切ったあと、デスクトップ電話機でコールを再開できない （137 ページ）
Dial-via-Office-Related SIP のエラー コード （138 ページ）

Cisco Unified Mobility ユーザが携帯電話を切ったあと、デスクトップ電話機でコールを再開できない

症状

リモート接続先（携帯電話）がスマートフォンではなく、この携帯電話へのコールが Unified Communications Manager を通じて固定されている場合、ユーザは、携帯電話を切ったらデスクトップ電話機に [再開（Resume）] ソフトキーが表示され、コールを再開できることを期待します。ユーザは、デスクトップ電話機でこのコールを再開できません。

考えられる原因

携帯電話が切れたときに、発呼側がビジー、リオーダー、または切断トーンを受信する場合、携帯電話のプロバイダーによってメディアが切断されなかった可能性があります。プロバイダーから切断信号が届かないため、Unified Communications Manager ではこの状況を認識できません。この状況に該当するかどうかを確認するには、発呼側で45秒間待機します。これでサービス プロバイダーがタイムアウトになると、切断信号が送信され、Unified Communications Manager でコールを再開するための [再開（Resume）] ソフトキーを表示できるようになります。

推奨処置

次の操作を実行します。

- 次のコマンドをゲートウェイに追加します。

  voice call disc-pi-off

- Cisco CallManager サービスの場合は、Active Call サービス パラメータの Retain Media on Disconnect with PI を False に設定します。

Dial-via-Office-Related SIP のエラー コード

症状

Cisco Unified Mobility Dial-via-Office（DVO）コールが成功しません。

考えられる原因

Unified Communications Manager では、Dial-via-Office コールが成功しなかった場合に、特定の SIP エラー コードが提供されます。次の表に、成功しなかった Dial-via-Office コールに対する SIP エラー コードを示します。

コール シナリオ	SIP エラー コード
ターゲット番号をルーティングできない。	404 Not Found
ターゲットがビジー状態である。	486 Busy Here
ターゲットが応答する前に、Cisco Unified Mobile Communicator が電話を切った。	487 Request Terminated
Cisco Unified Mobile Communicator が SIP CANCEL を送信した。	487 Request Terminated
Cisco Unified Mobile Communicator が登録に成功せずにコールを発信しようとしている。	503 Service Unavailable
すでに 2 つの未処理のコールが会社の電話回線にあるときに、Cisco Unified Mobile Communicator がコールを発信しようとしている。	486 Busy Here
未処理で保留中の DVO-F コール（PSTN コールの待機中）があるときに、Cisco Unified Mobile Communicator が DVO-F コールを発信しようとしている。	487 Request Terminated（最初のコール）

その他の資料

Cisco Unified Mobile Communicator を Unified Communications Manager と連携して動作するように設定する方法の詳細については、次のドキュメントを参照してください。

- http://www.cisco.com/en/US/products/ps7270/prod_installation_guides_list.html にある『*Installing and Configuring Cisco Unified Mobility Advantage*』の「「Configuring Unified Communications Manager for Use With Cisco Unified Mobility Advantage」」の章
- http://www.cisco.com/en/US/products/ps7270/products_installation_and_configuration_guides_list.html にある『*Configuring Features in Cisco Unified Mobility Advantage: Dial Via Office*』

Cisco Web Dialer のトラブルシューティング

ここでは、Cisco Web Dialer に関連する最も一般的な問題のエラー メッセージについて説明します。

関連トピック

認証エラー （139 ページ）
Cisco CTIManager がダウンしている （140 ページ）
転送先に到達できない （142 ページ）
ディレクトリ サービスがダウンしている （140 ページ）
デバイス/回線を開くことができない （141 ページ）
サービスが一時的に使用できない （139 ページ）
セッションの期限切れ、再ログイン （140 ページ）
ユーザがログインしているデバイスがない （141 ページ）

認証エラー

症状

Cisco Web Dialer で次のメッセージが表示されます。

認証に失敗しました。もう一度入力してください（Authentication failed, please try again）

考えられる原因

ユーザが入力したユーザ ID またはパスワードが正しくありません。

修正処置

ユーザ ID とパスワードを確認します。**Unified Communications Manager** のユーザ ID とパスワードを使用してログインする必要があります。

サービスが一時的に使用できない

症状

Cisco Web Dialer で次のメッセージが表示されます。

サービスは一時的に使用できない状態です。あとでもう一度実行してください（Service temporarily unavailable, please try again later）

考えられる原因

同時 CTI セッションの制御制限 3 に達したため、Cisco CallManager サービスが過負荷になりました。

修正処置

しばらくしてから接続を再試行します。

ディレクトリ サービスがダウンしている

症状

Cisco Web Dialer で次のメッセージが表示されます。

サービスは一時的に使用できない状態です。あとでもう一度実行してください: ディレクトリ サービスがダウンしています（Service temporarily unavailable, please try again later: Directory service down）

考えられる原因

Cisco Communications Manager のディレクトリ サービスがダウンしている可能性があります。

修正処置

しばらくしてから接続を再試行します。

Cisco CTIManager がダウンしている

症状

Cisco Web Dialer で次のメッセージが表示されます。

サービスは一時的に使用できない状態です。あとでもう一度実行してください：Cisco CTIManager がダウンしています（Service temporarily unavailable, please try again later: Cisco CTIManager down）

考えられる原因

Cisco Web Dialer に設定されている Cisco CTIManager サービスがダウンしました。

修正処置

しばらくしてから接続を再試行します。

セッションの期限切れ、再ログイン

症状

Cisco Web Dialer で次のメッセージが表示されます。

セッションの期限が切れました。もう一度ログインしてください（Session Expired, Please Login Again）

考えられる原因

次のいずれかの場合に、Cisco Web Dialer セッションの期限が切れます。

- Web Dialer サーブレットの設定後
- Cisco Tomcat サービスの再起動時

修正処置

Unified Communications Manager のユーザ ID とパスワードを使用してログインします。

ユーザがログインしているデバイスがない

症状

Cisco Web Dialer で次のメッセージが表示されます。

ユーザがログインしているデバイスがありません（User Not Logged in on Any Device）

考えられる原因

ユーザが Cisco Web Dialer の初期設定ウィンドウで Cisco Extension Mobility の使用を選択していますが、いずれの IP Phone にもログインしていません。

修正処置

- 電話機にログインしてから Cisco Web Dialer を使用します。
- [Extension Mobility を使用する（Use Extension Mobility）] オプションを選択する代わりに、ダイアログボックスの Cisco Web Dialer 初期設定リストからデバイスを選択します。

デバイス/回線を開くことができない

症状

ユーザがコールを発信しようとすると、Cisco Web Dialer で次のメッセージが表示されます。

ユーザがログインしているデバイスがありません（User Not Logged in on Any Device）

考えられる原因

- ユーザが選択した Cisco Unified IP Phone が Unified Communications Manager に登録されていません。たとえば、アプリケーションを起動する前に、Cisco IP SoftPhone を優先デバイスとして選択しています。
- 新しい電話機があるユーザが、すでに稼働していない古い電話機を選択しています。

修正処置

Unified Communications Manager に登録され、稼働している電話機を選択します。

転送先に到達できない

症状

Cisco Web Dialer で [終了（End Call）] ウィンドウに次のメッセージが表示されます。

転送先に到達できません（Destination Not Reachable）

考えられる原因

- ユーザが間違った番号をダイヤルしました。
- 適切なダイヤル ルールが適用されていません。たとえば、ユーザが 95550100 ではなく 5550100 をダイヤルしました。

修正処置

ダイヤル ルールを確認します。

ダイレクト コール パークのトラブルシューティング

次の表に、ダイレクト コール パークの一般的な問題を復元するためのトラブルシューティング ヒントを示します。

表 *11*：ダイレクト コール パークのトラブルシューティングのヒント

問題の説明	推奨処置
コールをパークできない。[転送（Transfer）] ソフトキー（使用可能な場合は [転送（Transfer）] ボタン）を押し、ダイレクト コール パークをダイヤルしてもコールがパークされません。	コール パーク番号に割り当てられているパーティションと電話機の電話番号に割り当てられているパーティションが一致していることを確認します。『Cisco Unified Communications Manager 機能設定ガイド』を参照してください。 デバイスにパーティションとコーリング サーチ スペースが正しく設定されていることを確認します。『*System Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

問題の説明	推奨処置
コールをパークできない。[転送（Transfer）] ソフトキー（使用可能な場合は [転送（Transfer）] ボタン）を押し、ダイレクト コール パーク番号をダイヤルしたあと、ユーザにビジー トーンが聞こえ、IP Phone に「パーク スロットが利用できません（Park Slot Unavailable）」というメッセージが表示されます。	ダイヤルしたダイレクト コール パーク番号が、パークされたコールでまだ使用されていないことを確認するか、または別のダイレクト コール パーク番号にコールをパークします。
コールをパークできない。[転送（Transfer）] ソフトキー（使用可能な場合は [転送（Transfer）] ボタン）を押し、ダイレクト コール パーク番号をダイヤルしたあと、ユーザにリオーダー トーンまたはアナウンスが聞こえます。	ダイヤルした番号がダイレクト コール パーク番号として設定されていることを確認します。『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。
パーク保留中のコールの復帰が早すぎる。	コール パーク復帰タイマーの設定時間を長くしてください。『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。
コールをパークできない。復帰タイマーが時間切れになったあと、ユーザにリオーダー トーンが聞こえる。	ユーザが、[転送（Transfer）] ソフトキー（使用可能な場合は [転送（Transfer）] ボタン）を押してからダイレクト コール パーク番号をダイヤルし、ダイレクト コール パーク番号をダイヤルしたあとにもう一度 [転送（Transfer）] ソフトキー（使用可能な場合は[転送（Transfer）]ボタン）を押すか、またはオンフックにしていることを確認します。ダイレクト コール パークは転送機能であるため、ダイレクトコールパーク番号を単独でダイヤルできません。『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。 （注） Transfer On-hook Enabled サービス パラメータを True に設定している場合は、[転送（Transfer）] ソフトキー（使用可能な場合は[転送（Transfer）] ボタン）を 2 回押す代わりに、オンフックにするだけで転送が完了します。『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。
パークされたコールを取得できない。パークされたコールを取得するためにダイレクト コール パーク番号をダイヤルしたあと、ユーザにビジー トーンが聞こえ、IP Phone に「パークスロットが利用できません（Park Slot Unavailable）」というメッセージが表示されます。	ユーザが取得用プレフィックスに続けてダイレクト コール パーク番号をダイヤルしているかどうかを確認します。『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

問題の説明	推奨処置
パークされたコールが、コールをパークした番号に復帰しない。	ダイレクト コール パーク番号の設定を調べ、別の電話番号ではなく、コールをパークした番号に復帰するように設定されていることを確認します。『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。
ダイレクト コール パーク番号または範囲を削除しようとすると、番号または範囲が使用中であるため削除できないというメッセージが表示される。	デバイスが監視するように設定されている（[BLF] ボタンを使用）ダイレクトコールパーク番号は削除できません。どのデバイスが番号を使用しているかを特定するには、[ダイレクトコールパークの設定（Directed Call Park Configuration）] ウィンドウの [依存関係レコード（Dependency Records）] リンクをクリックします。
ダイレクト コール パーク番号の範囲を設定したあと、範囲内の番号にコールをパークできない。	ダイレクト コール パーク番号の範囲を入力する構文を確認します。構文に誤りがあると、実際には範囲を設定していない場合でも、範囲を設定するように見えることがあります。『*Feature Configuration Guide for Cisco Unified Communications Manager*』を参照してください。

外部コール制御のトラブルシューティング

ここでは、一般的な外部コール制御の問題を処理する方法について説明します。

Unified Communications Manager が補助ルート サーバに接続できない。

- Unified Communications Manager Administration の [外部コール制御プロファイル（External Call Control Profile）] ウィンドウに設定されている URI が正しくありません。（**[コールルーティング（Call Routing）] > [外部コール制御（External Call Control）]**）。
  - 補助ルート サーバの URI を確認します。URI で次の構文を使用していることを確認してください。

    ```
    https://<hostname or IPv4 address of route server>:<port that
    is configured on route server>/path from route server
    configuration
    ```

  - 補助ルート サーバで https を使用している場合は、必須の証明書をインポートまたはエクスポートしていることを確認します。詳細については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「「External Call Control」」の章を参照してください。
  - 補助ルート サーバで https を使用している場合は、Unified Communications Manager Administration の [外部コール制御プロファイル（External Call Control Profile）] ウィンドウで [プライマリWebサービス（Primary Web Service）] フィールドと [セカンダリ

Webサービス（Secondary Web Service）] フィールドの URI に入力したホスト名が、補助ルート サーバ証明書のホスト名と一致することを確認します。

- Unified Communications Manager と補助ルート サーバ間のネットワーク接続が切断されました。Connection Loss および PDP Out Of Service カウンタは増分するカウンタであるため、一度は補助ルート サーバへの正常な接続が作成されたことを示します。したがって、ネットワーク内のイベントが原因で問題が発生したか、または補助ルート サーバ上でイベントが発生しました。
  - 補助ルート サーバが実行されており、ネットワーク接続が正常であることを確認します。
- 補助ルート サーバの応答が遅いため、補助ルート サーバに対する Unified Communications Manager ルーティング クエリーがタイムアウトになります。サービス要求の処理で補助ルート サーバが過負荷になっているか、ネットワークが不安定になっている可能性があります。
  - 外部コール制御プロファイルのルーティング要求タイマーまたは External Call Control Routing Request Timer サービス パラメータの値を大きくします。
  - External Call Control Maximum Connection Count To PDP サービス パラメータの値を大きくします。
  - 外部コール制御プロファイルにセカンダリ Web サービス（冗長補助ルート サーバ）を追加し、プロファイルでロード バランシングをイネーブルにします。
- Unified Communications Manager で補助ルート サーバからのルーティング指示を解析できなかったときに、Unified Communications Manager ルーティング要求が失敗しました。
  - XACML または CIXML の書式が正しいことを確認します。XACML 要求と応答の両方が Cisco CallManager SDI トレースに表示されます。各ルーティング要求のルーティング応答コードはトレースに含まれています。値 0 は、要求が受信され正しく解析されたことを示します。

最大ディバージョン ホップまたは同じトランスレーション パターンへの最大ディバージョン ホップを超えたため、コールが失敗した。

- 発信側はリオーダー トーンを受信します。
- Cisco CallManager SDI トレースを確認します。たとえば、External Call Control Diversion Maximum Hop Count サービス パラメータが 12 の場合、Cisco CallManager SDI トレースでは次のように表示されます。

```
PER_RoutingCallInfo::isCallDiversionMaximumHopCountExceeded:
callDiversionHopCount(12) >= CallDiversionMaximumHopCountLimit(12)
```

- たとえば、Maximum External Call Control Diversion Hops to Pattern or DN サービス パラメータが 12 の場合、Cisco CallManager SDI トレースでは次のように表示されます。

```
PER_RoutingCallInfo::isCallDiversionMaximumHopToSamePatternCountExceeded:
CallDiversionHopToSamePatternCount(12) >=
CallDiversionMaximumHopToSamePatternCountLimit(12)
```

- サービス パラメータの設定を確認し、必要に応じて変更します。
- コール転送について、補助ルート サーバのオブリゲーション設定を確認します。たとえば、A が B にコールすると、B のルートは A を C に転送することを指示し、C のルートは A を D に転送することを指示します。D は E に対して CFA を有効化し、E のルートは A を F に転送することを指示します。

Unified Communications Manager で補助ルート サーバからのコール ルーティング指示、必須パラメータ、または XACML を解析できない。

- RTMT でエラー アラーム ErrorParsingDirectiveFromPDP が表示されます。このアラームには次のいずれかの原因が該当します。
  - 補助ルート サーバからのルーティング処理の解析時にエラーが発生しました。
  - 補助ルート サーバからのルーティング処理が正確ではありません。
  - 補助ルート サーバからのルーティング処理が適用されません。

  ヒント 上記の項目について、補助ルート サーバのルート ルールおよび設定を確認してください。Unified Communications Manager は、失敗時の処理に基づいてコールをルーティングします。

- 補助ルート サーバで、オブリゲーション内に宛先がない状態でコールを転送します。

  ヒント 補助ルート サーバのオブリゲーション設定を確認してください。コール ルーティング指示が転送（divert）の場合は、オブリゲーションに宛先が必要です。

- コールが拒否されました。補助ルート サーバでコールが拒否されるが、CIXML 応答には拒否以外のオブリゲーションが含まれています。

  ヒント 補助ルート サーバで、オブリゲーションに拒否（reject）のコール ルーティング指示があるかどうかを確認してください。上記の項目は、ルーティングが拒否されるが、オブリゲーションは拒否ではない場合に適用されます。

Unified Communications Manager で、補助ルート サーバからのコール ルーティング応答に含まれる 1 つ以上のオプションの属性の解析に失敗した。

- RTMT で警告アラーム ErrorParsingResponseFromPDP が表示されます。このアラームには、エラーが 1 つかまたは複数かによって、次の原因のいずれか、または原因の組み合わせが含まれています。
  - 要求処理エラー：エラーの補助ルート サーバ トレースを確認します。
  - XACML 構文エラー：補助ルート サーバのルート設定を確認します。
  - CIXML のオプション属性の欠落：補助ルート サーバのオブリゲーション設定を確認します。
  - CIXML 構文エラー：補助ルート サーバのオブリゲーション設定を確認します。
  - 無効なアナウンス ID：補助ルート サーバのオブリゲーション設定を確認します。

Unified Communications Manager 機能の相互作用または Unified Communications Manager の設定のために、補助ルート サーバから返されたコール ルーティング指示を Unified Communications Manager で処理できない。

- Unified Communications Manager でコール ルーティング指示を処理できません。Unified Communications Manager でコールを宛先に転送できません。発信側はリオーダー トーンを受信します。発信側にアナウンスが聞こえません。Unified Communications Manager で FailedToFulfillDirectiveFromPDP アラームが生成されます。
- RTMT で警告アラーム FailedToFulfillDirectiveFromPDP が表示されます。このアラームには次のいずれかの原因が該当します。
  - アナウンスの挿入に失敗しました。Cisco Unified Serviceability で Cisco IP Voice Media Streaming アプリケーション サービスが実行されていることを確認します。実行されている場合は、Cisco IP Voice Media Streaming アプリケーション サービスの Annunciator サービス パラメータが True に設定されていることを確認します。また、コーデックのミスマッチが存在する可能性があります。アナンシエータでは、G.711、G.729、および Cisco Wideband コーデックがサポートされていますが、発信側デバイスでサポートされていない可能性があります。
  - 早期メディア機能がないため、アナウンスを再生できません。発信側デバイスで早期メディア機能がサポートされていません。早期メディア機能がサポートされているデバイスには、SIP トランクや H323 トランクがあります。
  - エラー コード付きのリダイレクト コール エラー。外部コール制御プロファイルに設定されている [ディバージョン再ルーティング用コーリング サーチ スペース（Diversion Rerouting Calling Search Space）] を調べ、リダイレクトされる宛先またはデバイスのパーティションが含まれているかどうかを確認します。
  - エラー コード付きの拡張コール エラー。宛先が通話中または未登録か、またはトランスレーション パターンが、デバイスに関連付けられているものとは異なるものである可能性があります。

Unified Communications Manager Administration で、アップロードしたカスタム アナウンスの処理エラーが報告される。

- カスタム アナウンスの .wav ファイルの形式が適切であることを確認します。適切な形式は、Windows PCM、16 ビット、1 秒当たりのサンプル数が 16000、32000、48000、または 48100、モノまたはステレオです。
- RTMT で、エラー分析用に Cisco Audio Translator トレースを収集します。

アナウンスが再生されない。

Cisco IP Voice Media Streaming App サービスで次のアラームが発行されます。

- kANNAudioUndefinedAnnID：アナウンスで未定義のカスタム アナウンス ID またはロケール ID が使用されています。アラームには数字の ID が含まれています。
- kANNAudioFileMissing：カスタムまたは Cisco 提供のアナウンスの .wav ファイルが見つかりません。アラームには、ファイル名、アナウンス ID、ユーザ ロケール、およびネットワーク ロケールが含まれています。
- ANN デバイスが Unified Communications Manager に登録されていることを確認します。
- メディア リソース グループを使用中の場合は、ANN デバイスがメディア リソース グループ内にあることを確認します。
- アナウンス ID が正しいことを確認します。
- English、United States ロケールを使用していない場合は、ロケールがインストールされていることを確認します。

ホットラインのトラブルシューティング

次の表に、ホットライン コールが正しくダイヤルされない場合のトラブルシューティング情報を示します。

表 *12 :* ホットライン コールが正しくダイヤルされない場合のトラブルシューティング

問題	ソリューション
ダイヤル トーン	PLAR 設定を確認します。
リオーダー トーンまたは VCA（クラスタ内コール）	• PLAR 設定を確認します。 • 両端の電話機がホットライン電話機として設定されていることを確認します。

問題	ソリューション
リオーダートーンまたはVCA（クラスタ内または TDM コール）	• PLAR 設定を確認します。 • 両端の電話機がホットライン電話機として設定されていることを確認します。 • トランクでルートクラスシグナリングがイネーブルになっていることを確認します。 • CAS ゲートウェイのルートクラストランスレーションの設定を確認します。

次の表に、発信者 ID に基づくコール スクリーニングが機能しない場合のトラブルシューティング情報を示します。

表 *13* : 発信者 *ID* に基づくコール スクリーニングの問題のトラブルシューティング

問題	ソリューション
コールが許可されない	• 発信者 ID を確認します。 • パターンをスクリーン CSS に追加します。
コールが許可される	パターンをスクリーン CSS から削除します。

即時転送のトラブルシューティング

ここでは、即時転送機能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。

関連トピック

ビジー （150 ページ）
キーがアクティブでない （149 ページ）
一時エラー発生 （150 ページ）

キーがアクティブでない

症状

ユーザが [即転送（iDivert）] を押すと、このメッセージが電話機に表示されます。

考えられる原因

[即転送（iDivert）] を押したユーザの音声メッセージング プロファイルに音声メッセージング パイロットがありません。

修正処置

ユーザの音声メッセージング プロファイルに音声メッセージング パイロットを設定します。

一時エラー発生

症状

ユーザが [即転送（iDivert）] を押すと、このメッセージが電話機に表示されます。

考えられる原因

音声メッセージング システムが機能していないか、またはネットワークに問題があります。

修正処置

音声メッセージング システムのトラブルシューティングを行います。トラブルシューティングか、 音声メッセージングのドキュメンテーションを参照してください。

ビジー

症状

ユーザが [即転送（iDivert）] を押すと、このメッセージが電話機に表示されます。

考えられる原因

メッセージは音声メッセージング システムが取り込み中であることを示しています。

修正処置

音声メッセージング ポートを追加設定するか、再実行してください。

インターコムのトラブルシューティング

ここでは、インターコ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。

関連トピック

インターコム回線でのダイヤル アウト時にビジー トーンが聞こえる （151 ページ）
スピーカー、ハンドセット、またはヘッドセットを使用してオフフックにしてもインターコム コールが接続状態にならない （151 ページ）
SCCP のトラブルシューティング （151 ページ）
SIP のトラブルシューティング （152 ページ）
Cisco Extension Mobility ユーザがログインしてもインターコム回線が表示されない （153 ページ）

インターコム回線でのダイヤル アウト時にビジー トーンが聞こえる

症状

ユーザがインターコム回線でダイヤル アウトするときに、電話機でビジー トーンが再生されます。

考えられる原因

DN が発信番号と同じインターコム パーティションにありません。

推奨処置

1. DN が発信番号と同じインターコム パーティションにあることを確認します。
2. 同じインターコム パーティションにある場合は、ダイヤルアウトした DN が別の電話機に設定されていることと、その電話機が同じ Unified Communications Manager クラスタに登録されていることを確認します。

スピーカー、ハンドセット、またはヘッドセットを使用してオフフックにしてもインターコム コールが接続状態にならない

症状

ヘッドセット、ハンドセット、またはスピーカーを使用時に、インターコム コールを応答モードにすることができません。

考えられる原因

これは仕様上の問題です。インターコム コールを接続状態にするには、対応する回線ボタンを押す方法しかありません。

推奨処置

スピーカー、ハンドセット、またはヘッドセットを使用してコールを終了できます。

SCCP のトラブルシューティング

ここでは、SCCP を実行している電話機に関するトラブルシューティングのヒントを示します。

関連トピック

インターコム回線がボタンテンプレートにあるのに電話機に表示されない（152 ページ）
電話機が SRST にフォールバックしてもインターコム回線が表示されない（152 ページ）

インターコム回線がボタン テンプレートにあるのに電話機に表示されない

症状

インターコム回線が電話機に表示されません。

考えられる原因

電話機のバージョンが8.3(1)よりも前か、ボタンテンプレートが電話機に割り当てられていない可能性があります。

手順

1. 電話機のバージョンを調べ、8.3(1) 以降であることを確認します。
2. ボタン テンプレートが電話機に割り当てられているかどうかを確認します。
3. Unified Communications Manager と電話機間のスニファ トレースをキャプチャします。ボタンテンプレートの応答時に、インターコム回線が電話機に送信されるかどうかを確認します（ボタン定義 = Ox17）。

電話機が SRST にフォールバックしてもインターコム回線が表示されない

症状

Unified Communications Manager リリース 6.0(x) 以降で設定された電話機に 2 つのインターコム回線があります。Unified Communications Manager が停止し、SRST にフォールバックします。しかし、インターコム回線が表示されません。

考えられる原因

SRST の SCCP バージョンで SCCP バージョン 12 がサポートされていません。

推奨処置

1. SRST の SCCP バージョンを確認します。SRST で SCCP バージョン 12 がサポートされている場合は、インターコム回線がサポートされます。
2. SRST で SCCP バージョン 12 がサポートされている場合は、スニファ トレースをキャプチャし、電話機から送信されたボタンテンプレートにインターコム回線が含まれていることを確認します。

SIP のトラブルシューティング

ここでは、SIP を実行している電話機に関する問題を特定するのに役立つ情報を示します。

関連トピック

SIP を実行している電話機の設定 （153 ページ）

SIP を実行している電話機のデバッグ （153 ページ）

SIP を実行している電話機のデバッグ

デバッグ コマンド **Debug sip-messages sip-task gsmfsmIsm sip-adapter** を使用します。

SIP を実行している電話機の設定

show config：電話機に対してこのコマンドを実行すると、インターコム回線が標準回線（featureid-->23）として設定されているかどうかが表示されます。

Cisco Extension Mobility ユーザがログインしてもインターコム回線が表示されない

症状

Cisco Extension Mobility ユーザが電話機にログインしてもユーザのインターコム回線が表示されません。

考えられる原因

[デフォルトのアクティブ デバイス（Default Activated Device）] が正しく設定されていません。

推奨処置

1. [デフォルトのアクティブ デバイス（Default Activated Device）] がインターコムの電話番号に対して設定されていることを確認します。
2. [デフォルトのアクティブ デバイス（Default Activated Device）] が、ログインに使用したデバイスと一致することを確認します。

詳細情報の入手先

- 『Cisco Unified Communications Manager 機能設定ガイド』の「「インターコム」」の章

IPv6 のトラブルシューティング

ここでは、IPv6 に関連する問題の修正処置について説明します。

関連トピック

デバイス間のコールが失敗する （155 ページ）
SIP トランク経由のコールが失敗する （154 ページ）
保留音が電話機で再生されない （155 ページ）
電話機が Cisco Unified Communications Manager に登録されない （154 ページ）

電話機が Cisco Unified Communications Manager に登録されない

症状

[IPアドレッシングモード（IP Addressing Mode）] が [IPv6のみ（IPv6 Only）] の Cisco Unified IP Phone が Cisco Unified Communications Manager に登録されません。

修正措置

- CLI を使用して、Unified Communications Manager サーバで IPv6 が有効になっていることを確認します。
- [エンタープライズ パラメータ設定（Enterprise Parameters Configuration）] ウィンドウで、Enable IPV6 エンタープライズ パラメータが True に設定されていることを確認します。
- [サーバの設定（Server Configuration）] ウィンドウで、[IPv6名（Ipv6 Name）] フィールドに Unified Communications Manager サーバのホスト名または IPv6 アドレスが設定されていることを確認します。ホスト名を設定した場合は、ホスト名を IPv6 アドレスに解決するように DNS を設定したことを確認します。
- Unified Communications Manager サーバに、非リンクローカル IPv6 アドレスが 1 つだけ設定されていることを確認します。
- 電話機がステートレス自動設定により IPv6 アドレスを取得する場合は、[電話の設定（Phone setting）] の [電話の自動設定を許可（Allow Auto-Configuration）] を [オン（On）] に設定したことを確認します。
- Cisco CallManager サービスと Cisco TFTP サービスが実行されていることを確認します。

SIP トランク経由のコールが失敗する

症状

[IP アドレッシング モード（IP Addressing Mode）] が [IPv6 のみ（IPv6 Only）] に設定された SIP トランク経由の着信コールが失敗します。

修正処置

- CLI を使用して、Unified Communications Manager サーバで IPv6 が有効になっていることを確認します。
- [エンタープライズ パラメータ設定（Enterprise Parameters Configuration）] ウィンドウで、Enable IPV6 エンタープライズ パラメータが True に設定されていることを確認します。
- INVITE に IPv4 シグナリングが含まれていないことを確認します。

症状

[IP アドレッシング モード（IP Addressing Mode）] が [IPv6 のみ（IPv6 Only）] に設定された SIP トランク経由の発信コールが失敗します。

修正処置

- CLI を使用して、Unified Communications Manager サーバのオペレーティング システムで IPv6 が有効になっていることを確認します。
- [エンタープライズ パラメータ設定（Enterprise Parameters Configuration）] ウィンドウで、Enable IPV6 エンタープライズ パラメータが True に設定されていることを確認します。
- [トランクの設定（Trunk Configuration）] ウィンドウで、SIP トランクの IPv6 宛先アドレスを設定したことを確認します。

デバイス間のコールが失敗する

症状

2 つのデバイス間のコールが失敗します。

修正処置

- [デバイス設定（Device Configuration）] ウィンドウで、デバイスの IP アドレッシング モードを確認します。
- 一方のデバイスで [IPアドレッシングモード（IP Addressing Mode）] が [IPv4のみ（IPv4 Only）] に設定されていて、もう一方で [IPアドレッシングモード（IP Addressing Mode）] が [IPv6のみ（IPv6 Only）] に設定されている場合は、IP v 4 と IPv6 の両方のスタックをサポートする MTP が設定されていることを確認します。

保留音が電話機で再生されない

症状

電話機のユーザに保留音が聞こえません。

修正処置

- 保留音が再生されるデバイスの IP アドレッシング モードを確認します。デバイスの IP アドレッシング モードが [IPv6のみ（IPv6 Only）] で、保留音がユニキャスト保留音に設定されている場合は、IPv4 と IPv6 の両方のスタックをサポートする MTP が設定されていることを確認してください。
- マルチキャスト保留音を設定している場合は、IPアドレッシングモードが [IPv6のみ（IPv6 Only）] に設定された電話機では保留音を再生できません。

論理パーティションのトラブルシューティング

ここでは、論理パーティションに関連する問題の修正処置について説明します。

関連トピック

論理パーティションが期待どおりに機能しない （156 ページ）
論理パーティション ポリシーを調整する必要がある （157 ページ）

論理パーティションが期待どおりに機能しない

症状

論理パーティションが期待どおりに機能しません。

修正処置

次の処置を実行して問題を解決します。

- Enable Logical Partitioning エンタープライズ パラメータが **True** に設定されていることを確認します。
- デバイスが、デバイスまたはデバイス プール レベルで有効な位置情報に関連付けられていることを確認します。
- デバイスが、デバイスまたはデバイス プール レベルで、いくつかの位置情報フィールドを選択して構成される有効な位置情報フィルタに関連付けられていることを確認します。
- Logical Partitioning Default Policy エンタープライズ パラメータが **DENY** の場合は、ゲートウェイの GeolocationPolicy と VoIP サイトの GeolocationPolicy 間に ALLOW 論理パーティション ポリシーが設定されていることを確認します。
- 論理パーティション GeolocationPolicy レコードの大文字と小文字の表記が正確であり、位置情報レコードに設定されている表記と一致することを確認します。
  - **例**：位置情報 US:NC:RTP:BLD1 および US:TX:RCDN:bld1 があるとします。

    GeolocationPolicy レコードが論理パーティション ポリシー レコードから設定される場合は、Border:US:NC:RTP:bld1 から Interior:US:NC:RTP:bld1 へというポリシーを設定できます。

    この場合、[論理パーティション ポリシーの設定（Location Partitioning Policy Configuration）] ウィンドウの [LOC] フィールドのドロップダウン リスト ボックスから誤った値が選択され、BLD1 と bld1 の両方が表示されます。

    そのため、管理者は、位置情報エントリと GeolocationPolicy で使用されている値の大文字と小文字が一致するようにエントリを選択する必要があります。
- 論理パーティション ポリシー チェックは VoIP-to-VoIP デバイス コールまたは VoIP 参加者だけの機能では実行されません。

- Unified Communications Manager Administration では、Interior:geolocpolicyX と Interior:geolocpolicyY 間のポリシーを設定できますが、このような設定は論理パーティション チェックでは使用されません。

論理パーティション ポリシーを調整する必要がある

症状

論理パーティション ポリシーのフィールドが正しく設定されていません。

修正処置

位置情報フィールドの階層は重要であるため、すべてのフィールドの階層順序が正しいこと、すべてのフィールドが存在することを確認します。階層順序とは、Country エントリは A1 エントリよりも前にあり、A1 エントリは A2 エントリよりも前にあることを意味します。

すべてのフィールドが論理パーティションポリシーに存在し、正しい階層順序で指定される必要があります。

次の例を参照してください。

一致する論理パーティションの例

次の位置情報では、Border:IN:KA と Interior:IN:KA 間のポリシーを検索します。

次のポリシーは順序どおりに一致します。この場合、***IN*** は Country フィールドのエントリ、KA は A1 フィールドのエントリを示します。

GeolocationPolicyA	**GeolocationPolicyB**	**ポリシー**
Border:IN:KA	Interior:IN:KA	Allow/Deny
Border:IN:KA	Interior:IN	Allow/Deny
Border:IN:KA	Interior	Allow/Deny
Border:IN	Interior:IN:KA	Allow/Deny
Border:IN	Interior:IN	Allow/Deny
Border:IN	Interior	Allow/Deny
Border	Interior:IN:KA	Allow/Deny
Border	Interior:IN	Allow/Deny
Border	Interior	Allow/Deny

一致しない論理パーティション ポリシーの例

位置情報のフィールドが論理パーティションポリシーにない場合は、必要な一致が発生しません。次の論理パーティション ポリシーでは、Country フィールドのエントリである ***IN*** が欠落しています。

Border:KA
Interior:KA
Border:BLR
Interior:BLR
Border:KA:BLR
Interior:KA:BLR

（注） Country=IN が欠落しています。

DNS キャッシュが有効な SIP のトラブルシューティング

ロギング

症状

ログのデバッグ レベルを設定します。

推奨処置

ネットワーク ネームサービスのデバッグ レベルを 3 に設定します（デフォルトは 0）。

- レベル 0：ログなし
- レベル 1：エラー、一部のキャッシュの削除
- レベル 2：キャッシュの入力
- レベル 3 以上：キャッシュ ヒットとみなされるエントリ、プルーニング キャッシュ

ログ ファイル

ログファイル：**activelog syslog/nscd.log**

次に示すサンプル ログ ファイルの内容の例を参考にしてください。

Wed Dec 17 18:26:01 2014 - 21908: Have not found "clock.cisco.com" in hosts cache!

Wed Dec 17 18:26:01 2014 - 21908: add new entry "clock.cisco.com" of type GETHOSTBYNAME for hosts to cache (first)

Wed Dec 17 18:26:01 2014 - 21908: handle_request: request received (Version = 2) from PID 22151

パケット キャプチャ

utils network capture port 53

例：

admin: utils network capture port 53

オプション付きのコマンドの実行：

```
size=128                count=1000              interface=eth0
 src=                    dest=                   port=53
 ip=  17:54:55.397539 IP b7k-vma150.cisco.com.45921 > dns-sj.cisco.com.domain: 38531+
A? b7k-vma154.cisco.com.(38)
17:54:55.398952 IP b7k-vma150.cisco.com.44296 > dns-sj.cisco.com.domain: 63056+ PTR?
183.168.70.171.in-addr.arpa.(45)
17:54:55.430709 IP dns-sj.cisco.com.domain > b7k-vma150.cisco.com.45921: 38531* 1/3/6 A
 10.94.12.154.(240)
17:54:55.431802 IP b7k-vma150.cisco.com.47404 > dns-sj.cisco.com.domain: 40244+ PTR?
154.12.94.10.in-addr.arpa.(43)
17:54:55.432016 IP dns-sj.cisco.com.domain > b7k-vma150.cisco.com.44296: 63056* 1/3/6
PTR dns-sj.cisco.com.(261)
17:54:55.465242 IP dns-sj.cisco.com.domain > b7k-vma150.cisco.com.47404: 40244* 1/3/6
PTR b7k-vma154.cisco.com.(263)
```

A/AAAA レコード キャッシングが機能しない

症状

A/AAAA レコード キャッシングが機能していません。SIP コールでホスト名の解決が必要になると、毎回 A/AAAA レコード クエリが送信されます。

修正処置

ネーム サービス キャッシュ サービスのステータスを確認します。ステータスは、次のように「STARTED」であることが必要です。

```
admin:utils service list
Requesting service status, please wait…
System SSH [STARTED]
Cluster Manager [STARTED]
Password Reset [STOPPED] Service Activated
Name Service Cache [STARTED]…
```

ネーム サービス キャッシュのステータスが [STARTED] でない場合は、次の CLI コマンドを使用してアクティブ化します。

admin:utils service activate Name Service Cache

admin:utils service start Name Service Cache

ネーム サービス キャッシュ サービスのステータスがすでに [STARTED] である場合は、次の CLI コマンドを使用して再起動します。

admin:utils service restart Name Service Cache

デバッグ レベルを 3 以上に設定します。有効なホスト名に ping を実行します。nscd.log を確認し、A/AAAA レコードがキャッシュに追加されるか、またはシステムが既存のキャッシュ エントリを使用していることを確認します。

イベントが、システム ログ（/var/log/active/syslog/messages）に表示されます。

Dec 17 10:41:31 localhost user 6 ilog_impl: Received request for platform-event (platform-system-startup)

Dec 17 10:41:31 localhost user 6 ilog_impl: emitting platform-event (platform-system-startup)

Dec 17 10:41:31 localhost user 6 ilog_impl: emitted platform-event (platform-system-startup)

（注） 「ping」のキャッシングが機能する場合、そのキャッシングが Unified Communications Manager のサービス（Cisco CallManager Service など）で機能することを確認します。検出 と nscd とのインタラクションを実行するアプリケーションで遅延が発生する場合があります。

ホスト名解決で誤った IP アドレスが返ってくる

症状

ホスト名解決で誤った IP アドレスが返ってきます。

考えられる原因

キャッシュが期限切れになっています。これは通常、DNS サーバの A/AAAA レコードの変更が原因です。

修正処置

- 次の CLI コマンドを使用して現在のキャッシュをフラッシュします。

admin:utils network name-service hosts cache invalidate

- 問題が解決しない場合は、次の CLI コマンドを使用して nscd を再開します。

admin:utils service restart Name Service Cache

- 問題が解決されない場合は、次の CLI コマンドを使用して nscd を無効化します。

admin: utils service stop Name Service Cache

- 問題が解決されない場合は、DNS サーバで A/AAAA レコードの設定を確認します。

ログが見つからない

症状

ログの /var/log/active/syslog/nscd.log が見つかりません。

修正処置

デバッグ レベルが 0 以下であることを確認します（デフォルトは 0）。デバッグ レベルを更新した後、次の CLI コマンドを使用して nscd を再開します。

admin:utils service restart Name Service Cache

CLI から nscd 属性を設定する

症状

CLI で nscd 属性を設定しましたが、新しい属性値が適用されません。

修正処置

属性の変更後に、次の CLI コマンドを使用して nscd を再起動します。

utils service restart Name Service Cache

TTL を設定する CLI コマンド

症状

nscd キャッシュ エントリの TTL を設定する CLI コマンドを使用したにもかかわらず、設定した値が A/AAAA レコード キャッシュに適用されません。

修正処置

DNS サーバの A/AAAA レコードに設定された TTL は、nscd の構成設定を上書きします。

nscd 用に設定された TTL は、TTL が DNS サーバの A/AAAA レコードに設定されていない場合にのみ有効です。

TTL の期限切れ前の A/AAAA レコード クエリ

症状

ネーム サービス キャッシュが有効にもかかわらず、TTL の期限切れ前に複数の A/AAAA レコード クエリが DNS サーバに送信されます。

修正処置

これらのクエリは、ほとんどの場合、既存のキャッシュ エントリをリロードする nscd にトリガされます。 nscd リロードの動作は、nscd 設定ファイルのリロード数に関連します。

キャッシュのクリア

症状

nscd を再起動すると、A/AAAA レコード キャッシュはクリアされますか?

修正処置

nscd を再起動しても、必ずキャッシュがクリア/フラッシュされるわけではありません。これは永続属性の設定によって異なります。

- 永続属性が [はい（Yes）] に設定されている場合、キャッシュは nscd の再起動時に変化しません。
- 永続属性が [いいえ（No）]（デフォルト）に設定されている場合、キャッシュは nscd の再起動時にクリア/フラッシュされます。

キャッシュをクリア/フラッシュするには、次の CLI コマンドを使用します。

admin:utils network name-service hosts cache invalidate

AAAA レコード キャッシュの内容

症状

A/AAAA レコード キャッシュの内容を確認できますか?

修正処置

いいえ。NSCD のアクティビティは（目的のデバッグ レベルを設定した）nscd.log でしか確認できません。A/AAAA レコードのキャッシング統計情報も、CLI コマンドを使用してクエリすることができます。

admin:show network name-service hosts cache-stats

SAML シングル サインオンのトラブルシューティング

ここでは、SAML シングル サインオンが予期したとおりに動作しない場合の症状と修正処置について説明します。

IdP へのリダイレクションが失敗する

症状

Unified Communications Manager でサポートされている Web ブラウザを使用してエンド ユーザが SAML 対応 Web アプリケーションにログインしようとしたときに、認証の詳細を入力するために設定された ID プロバイダー（IdP）にリダイレクトされません。

修正処置

次の条件が満たされていることを確認します。

- IdP は稼働しています。
- 正しい IdP メタデータ ファイルが Unified Communications Manager にアップロードされている。
- サーバと IdP が信頼と同じ範囲にあるかどうかを確認する。

IdP 認証が失敗する

症状

エンド ユーザが IdP によって認証されません。

修正処置

次の条件が満たされていることを確認します。

- LDAP ディレクトリが IdP にマッピングされている。
- ユーザが LDAP ディレクトリに追加されている。
- LDAP アカウントがアクティブである。
- ユーザ ID とパスワードが正しい。

Unified Communications Manager へのリダイレクションが失敗する

症状

IdP で認証された後でも、ユーザが SAML SSO 対応 Web アプリケーションにリダイレクトされません。

修正処置

次の条件が満たされていることを確認します。

- すべての Unified Communications Manager ノードのクロックと IdP が同期されます。クロックの同期については、『*System Configuration Guide for Cisco Unified Communications Manager*』の「NTP 設定」の項を参照してください。
- 必須属性の uid が IdP で設定されている。
- 正しい Cisco Unified Communication サーバのメタデータ ファイルが IdP にアップロードされている。
- ユーザに必要な権限がある。

テストの実行が失敗する

症状

テストの実行に失敗します。

修正処置

IdP へのリダイレクションが失敗する （163 ページ）、IdP 認証が失敗する （163 ページ）、およびUnified Communications Manager へのリダイレクションが失敗する （163 ページ）で説明されている修正処置を参照してください。

[SAML シングル サインオン（SAML Single Sign-On）] ページがクラスタの誤ったステータスを示す

症状

SAML SSOがクラスタでイネーブルになっている。パブリッシャがダウンしているときにSAML SSO をサブスクライバでディセーブル化し、さらにパブリッシャがアップになった後にパブリッシャで SAML SSO をディセーブル化すると、クラスタ全体の SAML SSO のステータスは「SAML SSO はイネーブル（SAML SSO enabled）」と誤表示されます。

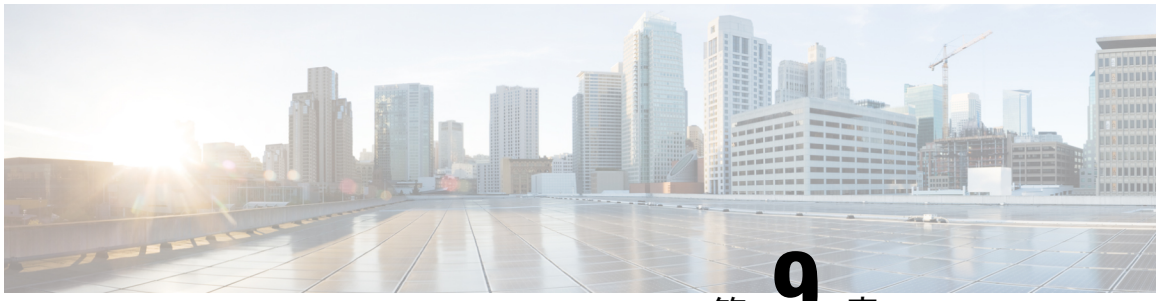
修正処置

Cisco Unified Reporting で、「Unified CM Cluster Overview」レポートを表示します。「Unified CM SAML SSO Status Summary」セクションを参照してください。このセクションでは、サーバの SAML SSO ステータスのデータベース値が、サブスクライバで同期されていないことが示されます。サーバのレポートには、SAML SSO がイネーブル化されていると示されるため、システムはクラスタ全体で SAML SSO がイネーブルであると見なします。この設定を解決するには、サブスクライバ ノードを再起動します。

Cisco Unified Reporting のレポート表示の詳細については、『*Cisco Unified Reporting Administration Guide*』を参照してください。

一般的なヒント

- SAML トレース レベルは必ずデバッグに設定してください。CLI の詳細については、『*Command Line Interface Reference Guide for Cisco Unified Communications Solutions Release 10.0(1)*』を参照してください。
- Unified RTMT の TLC を使用するか、**CLI** コマンドの **file get activelog** を実行して、「Cisco SSO」サービス ログ（パス：/tomcat/logs/ssosp/log4j/* and /platform/logs/ssoApp*）を収集します。



第 9 章

SNMP のトラブルシューティング

この章では、SNMP のトラブルシューティングで使用する情報について説明します。

トラブルシューティングのヒント

トラブルシューティングのヒントについては、この項を参照してください。

- 『*Cisco Unified Serviceability Administration Guide*』の「SNMP Services」にリストされているすべての機能およびネットワーク サービスが実行されていることを確認します。
- コミュニティ ストリングまたは SNMP ユーザがシステム上に適切に設定されていることを確認します。SNMP コミュニティ ストリングまたはユーザを設定するには、Cisco Unified Serviceability で **[SNMP]** > **[V1/V2]** > **[コミュニティ ストリング（Community String）]**、または **[SNMP]** > **[V3]** > **[ユーザ（User）]** を選択します。詳細については、『*Cisco Unified Communications Manager Administration Guide*』を参照してください。

システムから MIB をポーリングできない

この状態は、コミュニティ ストリングまたは SNMP ユーザがシステム上に設定されていないか、システム上に設定されているものと一致しないことを意味します。

（注） デフォルトでは、コミュニティ ストリングまたはユーザはシステム上に設定されていません。

SNMP の設定ウィンドウを使用して、コミュニティ ストリングまたは SNMP ユーザがシステム上に適切に設定されているかどうかを確認します。

システムから通知を受信できない

この状態は、通知の宛先がシステム上に正しく設定されていないことを意味します。

[通知先（Notification Destination）]（V1/V2c または V3）設定ウィンドウで、通知の宛先を正しく設定したことを確認します。

Unified Communications Manager ノードから SNMP トラップを受信できない

この状態は、Unified Communications Manager ノードからの SNMP トラップを確認できないことを意味します。

電話機の登録/登録解除/障害に関連する次の MIB オブジェクト ID（OID）を次の値に設定したことを確認します（どちらの値もデフォルトは 0 です）。

- ccmPhoneFailedAlarmInterval（1.3.6.1.4.1. 9.9.156.1.9.2）が 30 ～ 3600 に設定されていること。次の CLI コマンドを使用できます。**snmpset -c** <*community string*> **-v2c** <*transmitter ipaddress*> **1.3.6.1.4.1.9.9.156.1.9.2.0 i** <value>
- ccmPhoneStatusUpdateAlarmInterval（1.3.6.1.4.1.9.9.156.1.9.4）が 30 ～ 3600 に設定されていること。次の CLI コマンドを使用できます。**snmpset -c** <*community string*> **-v2c** <*transmitter ipaddress*> **1.3.6.1.4.1.9.9.156.1.9.4.0 i** <*value*>

『*Cisco Unified Serviceability Administration Guide*』の「SNMP Services」にリストされているすべての機能およびネットワーク サービスが実行されていることを確認します。

[通知先（Notification Destination）]（V1/V2c または V3）設定ウィンドウで、通知の宛先を正しく設定したことを確認します。

[コミュニティ ストリング（Community String）]（V1/V2c）または [ユーザ（User）]（V3）設定ウィンドウで、コミュニティ ストリング/ユーザ特権（通知の権限を含む）を正しく設定したことを確認します。

CISCO-CCM-MIB のヒント

ここでは、CISCO-CCM-MIB に関するヒントを示します。

関連トピック

よく寄せられる質問 （173 ページ）
一般的なヒント （169 ページ）
制限事項 （172 ページ）

一般的なヒント

- Cisco UCM SNMP Service のトレース設定を詳細に設定します（『*Cisco Unified Serviceability Administration Guide*』を参照）。
- コマンド **snmp walk -c** <*community*> **-v2c** <*ipaddress*> **1.3.6.1.4.1.9.9.156.1.1.2** を実行します
- Unified Communications Manager のバージョンの詳細を取得します
- 次の処理を実行してログと情報を収集します。
  - SNMP Master Agent（パス：`platform/snmp/snmpdm/*`）および Cisco UCM SNMP Service（パス：`cm/trace/ccmmib/sdi/*`）（RTMT の TLC を使用するか CLI コマンド **file get activelog** を使用）
  - CLI コマンド **show packages active snmp** を使用して、SNMP パッケージのバージョンを取得します。
  - CLI コマンド **show risdb query phone** を使用して、MMF Spy の出力を取得します。
- トレース ログと MMFSpy データを詳細な分析に送ります。

次の表に、CISCO-CCM-MIB SNMP トラップが送信されたことを確認する手順を示します。

表 *14 : CISCO-CCM-MIB SNMP* トラップのチェック方法

トラップ	確認手順
ccmPhoneStatusUpdate	**1.** CiscoSyslog->dogBasic MIB テーブルで MaxSeverity=Info を設定します。 **2.** ccmAlarmConfigInfo MIB テーブルで PhoneStatusUpdateAlarmInterv に 30 以上を設定します。 **3.** 電話機の登録先の Unified Communications Manager サーバを接続解除します。 **4.** 電話機が登録解除されます。 **5.** Unified Communications Manager サーバを再接続します。 **6.** 電話機が再登録されます。 **7.** ccmPhoneStatusUpdate トラップが生成されることを確認します。

トラップ	確認手順
ccmPhoneFailed	1. CiscoSyslog->clogBasic MIB テーブルで MaxSeverity=Info を設定します。 2. ccmAlarmConfigInfo MIB テーブルで PhoneFailedAlarmInterv に 30 以上を設定します。 3. 電話機が機能しないようにします。電話機を Cisco Unified Communications Manager Administrator から削除し、再登録します。 4. ccmPhoneFailed トラップが生成されることを確認します。
MediaResourceListExhausted	1. 標準の会議ブリッジリソース（CFB-2）のいずれかを含むメディア リソース グループ（MRG）を作成します。 2. 作成した MRG を含むメディア リソース グループリスト（MRGL）を作成します。 3. 電話機設定のウィンドウ（実際の電話機の）で、電話機のメディア リソース グループ リストとして MRGL を設定します。 4. IPVMS を停止します。これにより、会議ブリッジリソース（CFB-2）が動作を停止します。 5. メディア リストを使用する電話機で電話会議を行うと、電話機の画面に「「使用可能な会議ブリッジがありません（No Conference Bridge available）」」と表示されます。 6. MediaListExhausted アラーム/アラート/トラップが生成されることを確認します。

トラップ	確認手順
RouteListExhausted	1. ゲートウェイを 1 つ含むルート グループ（RG）を作成します。 2. 作成した RG を含むルート グループ リスト（RGL）を作成します。 3. 9XXXX のコールを RGL 経由でルーティングするルートパターン（9.XXXX）を作成します。 4. ゲートウェイの登録を解除します。 5. 電話機の 1 つで 9XXXX にダイヤルします。 6. RouteListExhausted アラーム/アラート/トラップが生成されることを確認します。
MaliciousCallFailed	1. ソフトキー テンプレートを作成します。テンプレートで、電話機のさまざまな状態に [迷惑呼（MaliciousCall）]「」ソフトキーを追加します。 2. 新しいソフトキー テンプレートを実際の電話機に割り当てて、電話機をリセットします。 3. 電話をかけ、コール中およびコール後に電話機の画面で [迷惑呼（MaliciousCall）]「」ソフトキーを選択します。 4. 「「MaliciousCallFailed」」アラーム/アラート/トラップが生成されることを確認します。

次のログおよび情報を収集して分析します。

- `/platform/snmp/snmpdm/*` に格納される SNMP Master Agent ログ。
- Cisco UCM SNMP Service（Real Time Monitoring Tool（RTMT）を使用するか、**file get activelog** <*path*> CLI コマンドを入力）。ログが格納されるパスは */cm/trace/ccmmib/sdi/** です。
- /usr/local/Snmpri/conf フォルダ内のすべてのファイル。（これは、ROOT/REMOTE ログインが可能な場合にだけ可能です）。
- 上記のフォルダの 'ls -l'リスト。（これは、ROOT/REMOTE ログインが可能な場合にだけ可能です）。
- perfmon のログ（**file get activelog /cm/log/ris/csv/** CLI コマンドを実行）。

- 問題を引き起こした一連の実行処理の詳細。
- ccmservice のログ（**file get activelog /tomcat/logs/ccmservice/log4j** CLI コマンドを実行）。
- SNMP パッケージのバージョン（**show packages active snmp** CLI コマンドを実行）。
- 電話機の MMF Spy 出力（**show risdb query phone** CLI コマンドを実行）。

制限事項

SNMP 要求に複数の OID が指定されている場合、および変数が CISCO-CCM-MIB の空のテーブルを指している場合、要求には時間がかかります。getbulk/getnext/getmany 要求の要求 PDU 内に複数の OID があり、CISCO-CCM-MIB で後続のテーブルが空の場合、SNMP v1 バージョンでは NO_SUCH_NAME、SNMP v2c または v3 バージョンでは GENERIC_ERROR が応答で指定されることがあります。

- 理由：このタイムアウトは、CCMAgent のパフォーマンスを向上させ、大量のクエリを受け取ったときに抑制するために追加されたコードが原因で発生します。これにより、Unified Communications Manager コール処理エンジンの優先度が保たれるようになっています。
- 回避策：
  - テーブルにアクセスする前に利用可能なスカラ変数（1.3.6.1.4.1.9.9.156.1.5）を使用してテーブル サイズを判別するか、目的のテーブルで get 操作を実行してから、空ではないテーブルを照会します。
  - 単一の要求内で照会される変数の数を減らします。たとえば、空のテーブルでは、管理アプリケーションのタイムアウトが 3 秒に設定されている場合、指定する OID は 1 つだけにすることを推奨します。空ではないテーブルについては、1 行のデータを取得するのに 1 秒かかります。
  - 応答タイムアウトの値を大きくします。
  - 再試行回数を減らします。
  - getbulk SNMP API を使用しないようにします。getbulk API では、MaxRepetitions で指定されているレコード数が取得されます。つまり、次のオブジェクトがテーブルまたは MIB の範囲外であっても、それらのオブジェクトが取得されます。そのため、CISCO-CCM-MIB に空のテーブルがある場合は、次の MIB に進みます。この場合、応答に時間がかかります。テーブルが空ではないことがわかっており、レコード数もわかっている場合は、getbulk API を使用します。この状況では、応答を 5 秒以内に取得するために、最大繰り返し回数を 5 に制限します。
  - SNMP 照会を構成し、現在の制限にあわせて調整します。
  - 多数の電話機が Unified Communications Manager に登録されている場合は、PhoneTable で多数の getbulk を実行しないようにします。このようなシナリオでは、更新が発生すると常に ccmPhoneStatusUpdateTable が更新されます。

よく寄せられる質問

CISCO-CCM-MIB について、Cisco Unified Communications Manager ノードから SNMP トラップが取得されないのはなぜですか。

CISCO-CCM-MIB の SNMP トラップを受信するには、次の MIB OID の値が適切な値に設定されていることを確認する必要があります。ccmPhoneFailedAlarmInterval（1.3.6.1.4.1.9.9.156.1.9.2）および ccmPhoneStatusUpdateAlarmInterv（1.3.6.1.4.1.9.9.156.1.9.4）は、30 ～ 3600 に設定します。デフォルトでは、ゼロ（0）に指定されています。

Linux コンピュータから次のコマンドを実行します。

- **snmpset -c** <*Community String*> **-v 2c** <*transmitter ip address*> **1.3.6.1.4.1.9.9.156.1.9.2.0 i** <*value*>
- **snmpset -c** <*Community String*> **-v 2c** <*transmitter ip address*> **1.3.6.1.4.1.9.9.156.1.9.4.0 i** <*value*>

次の問題は、電話機の登録/登録解除/障害に関連しています。

- 通知の宛先の設定：通知の宛先が設定されていることを確認する必要があります。これは、Cisco Unified Serviceability の Web ウィンドウから実行できます。**[SNMP]** > **[通知の宛先（Notification Destinations）]** というメニューがあります。

  通知の宛先を設定する前に、必要な SNMP サービスがアクティブであり、実行されていることを確認します（SNMP Master Agent および Cisco UCM SNMP Service）。また、コミュニティ ストリング/ユーザの特権を正しく設定してあることを確認します。通知の権限も含まれている必要があります。

  トラップがまだ生成されない場合は、対応するアラームが生成されるかどうかを確認します。これらのトラップはアラーム イベントに基づいて生成されるため、SNMP エージェントがこれらのアラーム イベントを取得していることを確認します。ローカル Syslog をイネーブルにします。Cisco UCM Serviceability ウィンドウの **[アラーム（Alarm）]** > **[設定（Configuration）]** で利用できるアラーム設定から、ローカル Syslog の宛先について Cisco UCM のアラーム設定を情報レベルに設定します。トラップを再現し、対応するアラームが CiscoSyslog ファイルにロギングされるかどうかを確認します。

- トラップとしての syslog メッセージの受信：特定の重大度を超える syslog メッセージをトラップとして受信するには、clogBasic テーブルで次の 2 つの MIB オブジェクトを設定します。

  - clogNotificationsEnabled（1.3.6.1.4.1.9.9.41.1.1.2）：syslog トラップ通知をイネーブルにするには、これを **true**（**1**）に設定します。デフォルト値は **false**（**2**）です。例：**snmpset -c** <*Community String*> **-v 2c** <*transmitter ip address*> **1.3.6.1.4.1.9.9.41.1.1.2.0 i** <*value*>

  - clogMaxSeverity（1.3.6.1.4.1.9.9.41.1.1.3）：トラップを受け取る最低の重大度レベルを設定します。デフォルト値は **warning**（**5**）です。通知がイネーブルの場合、設定した重大度以下のアラーム重大度の syslog メッセージはすべてトラップとして送信されます。例：**snmpset -c** <*Community String*> **-v 2c** <*transmitter ip address*> **1.3.6.1.4.1.9.9.41.1.1.3.0 i** <*value*>

Cisco Unified Communications Manager に対して定義されているさまざまなトラップは何ですか。

CISCO-CCM-MIB には、次の定義済みトラップのリストが含まれています。

- ccmCallManagerFailed：Cisco UCM プロセスが重要なサブシステムの 1 つで障害を検出することを示します。ハートビート/イベント モニタリング プロセスから検出することもできます。
- ccmPhoneFailed：ccmPhoneFailedAlarmInterval で指定された間隔によって ccmPhoneFailedTable 内の少なくとも 1 つのエントリが示されることを通知します。
- ccmPhoneStatusUpdate：ccmPhoneStatusUpdateTable 内に 1 つのエントリが存在する場合に ccmPhoneStatusUpdateInterv で指定された間隔で生成される通知です。
- ccmGatewayFailed：少なくとも 1 つのゲートウェイが Cisco UCM への登録および通信を試行して失敗したことを示します。
- ccmMediaResourceListExhausted：Cisco UCM が指定されたタイプのリソースを使い果たしたことを示します。
- ccmRouteListExhausted：指定されたルート リスト内で Cisco UCM が使用可能なルートを見つけることができなかったことを示します。
- ccmGatewayLayer2Change：Skinny ゲートウェイの登録済みインターフェイスの D チャネル/レイヤ 2 で状態が変更されることを示します。
- ccmMaliciousCall：ユーザがコールを悪質としてローカル Cisco UCM サーバに登録することを示します。
- ccmQualityReport：ユーザが Quality Report Tool を使用して品質の問題を報告することを示します。
- ccmTLSConnectionFailure：指定されたデバイスに対して Unified Communications Manager が TLS 接続を開けなかったことを示します。

トラップのアラームへのマッピングは、次のとおりです。

- ccmCallManagerFailed—CallManagerFailure
- ccmPhoneFailed—DeviceTransientConnection
- ccmPhoneStatusUpdate
- ccmGatewayFailed—DeviceTransientConnection
- ccmMaliciousCall—MaliciousCall
- ccmMediaResourceListExhausted—MediaResourceListExhausted
- ccmQualityReportRequest—QRTRequest
- ccmRouteListExhausted—RouteListExhausted
- ccmGatewayLayer2Change—DChannelOOS, DChannelISV

Cisco Unified Communications Manager からのさまざまな SNMP トラップをどのようにしてチェックできますか。

少数のトラップを起動する次の手順を実行します。

- ccmPhoneStatusUpdate トラップ
  - ccmAlarmConfigInfo MIB テーブルで ccmPhoneStatusUpdateAlarmInterv（1.3.6.1.4.1.9.9.156.1.9.4）を 30 以上に設定します。
  - 電話機が登録されている Unified Communications Manager サーバを接続解除します。電話機が登録解除されます。
  - Unified Communications Manager サーバを再接続します。電話機が再登録され、ccmPhoneStatusUpdate トラップが取得されます。
- ccmPhoneFailed トラップ
  - ccmAlarmConfigInfo MIB テーブルで ccmPhoneFailedAlarmInterval（1.3.6.1.4.1.9.9.156.1.9.2）を 30 以上に設定します。
  - 電話機が機能しないようにします。電話機を Unified Communications Manager から削除し、再登録します。電話機の障害のトラップの場合、次の 2 つの異なるシナリオを試行できます。

    tftp/Unified Communications Manager サーバ A をポイントするように電話機を設定します。別のスイッチ上の Unified Communications Manager サーバ B に電話機を接続します。電話機ステータスは不明のままです。次のメッセージが表示されます。

    ```
    2007-10-31:2007-10-31 14:53:40 Local7.Debug 172.19.240.221
    community=public, enterprise=1.3.6.1.4.1.9.9.156.2.0.2,
    enterprise_mib_name=ccmPhoneFailed, uptime=7988879,
    agent_ip=128.107.143.68, version=Ver2, ccmAlarmSeverity=error,
    ccmPhoneFailures=1.
    ```

    Cisco UCM で 7960 電話機を 7940 電話機として登録し、電話機障害トラップを生成する db 問題を発生させます。
- MediaResourceListExhausted トラップ
  - メディア リソース グループ（MRG）を作成し、標準の ConferenceBridge リソース（CFB-2）のいずれかが含まれるようにします。
  - メディア リソース グループ リスト（MRGL）を作成し、作成した MRG が含まれるようにします。
  - 実際の電話機の [電話の設定（Phone Configuration）] ウィンドウで、MRGL を電話機の [メディア リソース グループ リスト（Media Resource Group List）] として設定します。
  - IPVMS を停止します。これにより、ConferenceBridge リソース（CFB-2）は機能を停止します。

- メディア リストを使用して電話機で電話会議を行います。電話機の画面に「使用可能な会議ブリッジがありません（No Conference Bridge available）」が表示されます。
- MediaListExhausted アラーム/アラート/トラップが生成されるかどうかを確認します。

- RouteListExhausted トラップ
  - ルート グループ（RG）を作成し、ゲートウェイが 1 つ含まれるようにします。
  - ルート グループ リスト（RGL）を作成し、作成した RG が含まれるようにします。
  - 9XXXX コールを RGL によって再ルーティングするルート パターン（9.XXXX）を作成します。
  - ゲートウェイの登録を解除します。
  - 電話機の 1 つで 9XXXX にダイヤルします。
  - RouteListExhausted アラーム/アラート/トラップが生成されるかどうかを確認します。

- MaliciousCallFailed トラップ
  - ソフトキー テンプレートを作成します。テンプレートで、使用可能なすべての [迷惑呼（MaliciousCall）] ソフトキーを電話機ステータスに追加します。
  - この新しいソフトキーテンプレートを実際の電話機に割り当てます。電話機をリセットします。
  - 電話をかけ、コール中およびコール後に電話機の画面で MaliciousCall を選択します。
  - MaliciousCallFailed アラーム/アラート/トラップが生成されるかどうかを確認します。

- GatewayFailed トラップ
  - 方法 1：Web Admin を使用してデータベースからゲートウェイ設定を削除するか、ゲートウェイ MAC アドレスを無効な値に変更して更新します。ゲートウェイをリブートします。または、ゲートウェイが接続されている Cisco UCM サービスを再起動します。
  - 方法 2：ccmAlarmConfigInfo MIB テーブルで、GatewayAlarmEnable=true を設定します。Cisco Unified Serviceability で、SNMP の設定ウィンドウに移動し、SNMP コミュニティ ストリングおよびトラップの宛先が正しく設定されていることを確認します。ゲートウェイ障害イベントを作成すると、トラップ受信側にトラップが表示されます。ゲートウェイ障害およびフェールオーバーを発生させるには、Cisco UCM を再起動します。ゲートウェイが冗長 Cisco UCM サーバにフェールオーバーします。冗長 Cisco UCM サーバのデータベース内にゲートウェイを設定しないでください。

- ccmGatewayLayer2Change トラップ
  - ccmGatewayLayer2Change トラップは、Cisco UCM からの D-Channel Out Of Service（DChannelOOS）または D-Channel Inservice（DChannelISV）中に起動されます。テスト目的で、そのようなイベントが起動されるかどうかを確認します。

- ccmCallManagerFailed トラップ
  - Cisco UCM 障害アラームは、内部エラーの発生時に生成されます。これらのアラームには、CPU 不足、タイマーの問題などによる内部スレッド停止が含まれます。これは、Cisco UCM チームがこれらのいずれかを意図的に発生させないかぎり再現が難しいトラップです。

Cisco UCM Agent の高い CPU 消費が継続する場合、何を行う必要がありますか。

分析用のログを収集し、障害 CSCsm74316 を参照します。使用している Cisco UCM リリースに障害の修正が追加されているかどうかを確認します。

CTI Routepoint を Unified Communications Manager Administration から削除しても、ccmCTIDeviceTable MIB にそのエントリが存在します。なぜですか。

「「RIS Unused Cisco CallManager Device Store Period」」というサービス パラメータによって、未登録デバイスが RIS データベースおよび MIB 内に残される時間が定義されています。[Cisco UCM Administration] ウィンドウと SNMP MIB は同期していない場合があります。[Cisco UCM Administration] ウィンドウにはデータベースからの情報が表示され、SNMP では RIS データベースが使用されるためです。

ccmPhoneType を Cisco-CCM-MIB の ccmPhoneTable で照会したときに情報が返されません。なぜですか。

これは、ccmPhoneType が古いことを意味します。CcmProductTypeEntry に対する ccmPhoneProductTypeIndex から、同じ情報を取得できます。テーブルでは、インデックスはそのテーブルでリストされているインデックスと名前に対応します。

次のリストに、その他の古い OID の一部と、参照する必要がある代替 OID を示します。

- ccmGatewayType は古いため、ccmGateWayProductTypeIndex を参照する必要があります。
- ccmMediaDeviceType は古いため、ccmMediaDeviceProductTypeIndex を参照する必要があります。
- ccmCTIDeviceType は古いため、ccmCTIDeviceProductTypeIndex を参照する必要があります。

ccmPhoneProductTypeIndex に対する照会でゼロが返ります。なぜですか。

使用している Unified Communications Manager のリリースにこの機能があることを確認してください。

WALK が ccmPhoneTable に対して実行されていますが、ccmPhoneUserName によって値が返されません。ユーザ名は IP Phone にどのように関連付けられていますか。

エンド ユーザを作成し、登録済みの電話機に移動して、オーナーのユーザ ID を関連付けます。これを実行したあとに、SNMP Walk 内の OID によってユーザが表示されます。

SNMP を使用して各電話機のファームウェアのバージョンを取得するにはどうすればいいですか。

ccmPhoneTable 内の ccmPhoneLoadID オブジェクトによって、各電話機のファームウェア バージョンが示されます。新しいイメージダウンロードが失敗した場合にはこの値が異なることがあります。SNMP では、設定済みのファームウェア ID（ccmPhoneLoadID）と実際に実行されているファームウェア（ccmPhoneActiveLoad）の両方が示されるためです。

CCM MIB によって ccmVersion が 5.0.1 として返されますが、これは間違いです。

使用している Unified Communications Manager のリリースにこの機能があることを確認してください。ない場合はアップグレードしてください。

CCM MIB が正しくない ccmPhoneLoadID を返します。

ccmPhoneLoadID の値は RIS データベースから取得されます。このデータベースには、電話機の登録中に受信されたアラームに基づいて情報が入力されます。次の手順を実行し、詳細な分析のためのログを収集してください。

1. Cisco Unified Serviceability で、**[アラーム（Alarm）] > [設定（Configuration）]** を選択します。サーバを選択します。次に、[移動（Go）] をクリックします。サービス グループの [CM サービス（CM Services）] を選択します。次に、[移動（Go）] をクリックします。サービスの [Cisco CallManager] を選択します。次に、[移動（Go）] をクリックします。
2. [ローカル Syslog（Local Syslog）]、[SDI トレース（SDI Trace）]、および [SDL トレース（SDL Trace）] の [アラームの有効化（Enable Alarm）] をオンにします。それぞれの [アラーム イベント レベル（Alarm Event Level）] ドロップダウン リスト ボックスから [情報（Informational）] を選択します。
3. [トレース設定（Trace Configuration）] ウィンドウで、Cisco UCM サービスの [デバッグ トレース レベル（Debug Trace Level）] を [詳細（Detailed）] に設定します。
4. 正しくない LoadID が表示されている電話機をリセットします。
5. Syslog および Cisco UCM トレースを収集します。
6. 電話機の詳細を収集します。

Cisco Call Manager のステータス（START/STOP）はどのようにすればモニタできますか。

サービス監視には次のオプションがあります。

- SYSAPPL MIB
- HOST-RESOURCE-MIB
- CISCO-CCM-MIB（ccmStatus）
- SOAP インターフェイス
- Real-Time Monitoring Tool（RTMT）アラート

Cisco UCM サービス障害用に ccmCallManagerFailed トラップがあります。ただし、このトラップでは、通常のサービス停止および不明のクラッシュは対象になりません。

ポーリングされたデバイスのデバイス プール情報が正しくないように見えます。なぜですか。使用された OID は ccmPhoneDevicePoolIndex です。

CISCO-CCM-CAPABILITY MIB に記述されているように、ccmPhoneDevicePoolIndex はサポートされていないためゼロ（0）が返されます。Cisco UCM デバイス登録アラームには、現在はデバイス プール情報は含まれていません。

HOST-RESOURCES-MIB のヒント

HOST-RESOURCES-MIB は、システムで実行されているすべてのプロセスに関する情報を hrSWRunTable から取得します。HOST-RESOURCES-MIB は、システムで実行されているすべてのプロセスを監視する場合に使用します。インストールされているシスコのアプリケーションだけを監視するには、SYSAPPL-MIB を使用します。

関連トピック

ディスク容量および RTMT （179 ページ）
よく寄せられる質問 （180 ページ）
収集するログ （179 ページ）

収集するログ

トラブルシューティング目的で次のログおよび情報を収集します。

- hostagt ログ ファイル。**file get activelog /platform/snmp/hostagt/** コマンドを実行して収集します。
- syslog ファイル。**file get activelog /syslog/** コマンドを実行して収集します。
- Master SNMP Agent ログ ファイル。**file get activelog /platform/snmp/snmpdm/** コマンドを実行して収集します。
- 実行した一連の操作。

ディスク容量および RTMT

HOST-RESOURCES-MIB で表示される使用済みディスク容量と使用可能ディスク容量の値は、RTMT で表示されるディスク容量の値と一致しない場合があります。これは、ファイル システムの予約済みディスク ブロックにおける最小空き容量の割合が原因です。Unified Communications Manager リリース 7.1(x) 以降のシステムの minfree 値は 1% であるため、RTMT と HOST-RESOURCES-MIB で表示される使用済みディスク容量の値には 1% の相違があります。

- RTMT では、df の報告値を使用して使用済みディスク容量の値が表示されます。この値は、[（合計容量 - 使用可能容量）/ 合計容量] X 100 で計算されます。合計容量には最小空き容量も含まれます。
- HOST-RESOURCES-MIB での使用済みディスク容量の値は [hrStorageUsed / hrStorageSize] X 100 で計算されます。hrStorageSize には最小空き容量は含まれません。

よく寄せられる質問

HOST-RESOURCES-MIB をプロセスのモニタリングに使用できますか。

Host Resources MIB では、hrSwRunTable 内の、システムで実行されているプロセスに関する情報が取得されます。ただし、システムで実行されているすべてのプロセスが監視されます。インストールされているシスコのアプリケーションだけを監視する必要がある場合は、SYSAPPL-MIB の使用を推奨します。

Real-Time Monitor Tool によって表示されるメモリ使用率の値は HOST-RESOURCES-MIB にどのようにマッピングされますか。

次の表に、メモリ使用率の値を示します。

表 *15 :* メモリ使用率の値

メモリ使用率	RTMT カウンタ	HOST-RESOURCES-MIB
スワップ メモリの使用率	メモリ\使用されているスワップのキロバイト数	hrStorageUsed.2（説明は仮想メモリ）
物理メモリの使用率	メモリ\使用されているキロバイト数	hrStorageUsed.1（この説明は物理 RAM になっています）

メモリ使用率	RTMT カウンタ	HOST-RESOURCES-MIB
物理メモリとスワップ メモリの使用率の合計	メモリ\使用されている仮想メモリのキロバイト数	実際の値ではありません。基本的には、hrStorageUsed.2 と hrStorageUsed.1 を足し合わせる必要があります。 使用率の低いサーバではスワップ メモリを使用できないため、HR 仮想メモリによって 0 が返される場合があります。HR 仮想メモリが正しく返されていることを確認するには、値を RTMT の Memory\Used Swap KBytes と比較する必要があります。RTMT と HR では、「「仮想メモリ」」という用語の使用法が異なります。物理メモリの hrStorageUsed では、データは使用済み（バッファ＋キャッシュ）という観点で表示されます。 物理メモリの hrStorageUsed は、使用済みに関するデータ（バッファ＋キャッシュ）を示します。 HOST-RESOURCES-MIB によって示される共有メモリ情報は、::hrStorageDescr.10 = STRING: /dev/shm です。 HOST-RESOURCES-MIB によって報告される仮想メモリは、RTMT ではスワップ メモリと見なされるもので構成されます。 HOST RESOURCES MIB の場合、次の公式が使用されます。 • %Physical memory usage = (Physical RAM hrStorageUsed + /dev/shm hrStorageUsed) / (Physical RAM hrStorageSize) • %使用されている仮想メモリ = （物理 RAM の hrStorageUsed + /dev/shm hrStorageUsed + 仮想メモリの hrStorageUsed）/（物理 RAM の hrStorageSize + 仮想メモリの hrStorageSize）

RTMT で表示されるディスク容量の値と HOST-RESOURCES-MIB のディスク容量の値が異なるのはなぜですか。

一般的に、dfサイズは表示される使用済みおよび使用可能なディスク容量データと一致しません。これは、予約済みのファイル システム ディスク ブロックの minfree パーセンテージのために発生します。リリース 6.x および 7.0 の Cisco Unified Communications Manager の minfree 値は 1% です。RTMT および HOST-RESOURCES-MIB で表示される使用済みディスク容量の値には、1% の差異が発生します。

RTMT では、使用済みディスク容量の値は df 報告値から表示されます。[(合計容量 - 使用可能容量) / 合計容量] X 100 であり、合計容量には minfree も含まれます。HOST-RESOURCES-MIB の場合、これは [hrStorageUsed/hrStorageSize] X 100 で計算されます。hrStorageSize には minfree は含まれません。

hrStorageUsed の値は、ホスト エージェントではどのように表示されますか。

物理 RAM の hrStorageUsed ではデータは使用済み（バッファ + キャッシュ）という観点で表示されるように修正されました。ホストエージェントのバージョンが正しいかどうかを確認するには、**show packages active snmp** コマンドを使用して、システムにインストールされている snmp-rpm バージョンを収集します。

メモリ容量/使用率の値は HOST-RESOURCES-MIB の値とどのように比較されますか。

HOST-RESOURCES-MIB では、サイズおよび使用済みストレージは hrStorageUnits で表されます。そのストレージ タイプで、hrStorageUnits が 4096 バイトの場合、MIB 値で照会される hrStorageUsed または hrStorageSize の値には 4096 が掛けられます。たとえば、**show status** コマンドを使用することで、物理 RAM の合計メモリは 4090068K として表示されます。

物理 RAM ストレージ タイプの hrStorageUnits が 4096 バイトの場合、物理 RAM の hrStorageSize は 1022517 として表示されます。これは 4090078K [(1022517 X 4096)/1024 = 4090068K] です。

Windows で、HOST-RESOURCES-MIB の hrSWRunName に対する SNMP 照会で断続的に正しくないエントリが返されるのはなぜですか。

Microsoft 社の SNMP 拡張エージェント（hostmib.dll）では、HOST-RESOURCE-MIB がサポートされています。Microsoft のサポートがこの問題に役立つ場合があります。この問題が継続する場合は、次の手順を実行します。

1. tlist snmp.exe ファイルを使用して、hostmib.dll が出力内にリストされていることを確認します。
2. SNMP サービスの開始時に、SNMP からのエラー/警告メッセージがイベント ビューアにないことを確認します。
3. snmp サービス プロパティで、使用されるコミュニティ ストリングが読み取り権限で設定されていることを確認します。
4. MSSQL-MIB（MssqlSrvInfoTable）を使用して、SQL プロセスのステータスを確認します。

プロセスのモニタリング

HOST-RESOURCES-MIB は、システムで実行されているすべてのプロセスに関する情報を hrSWRunTable から取得します。システムで実行されているすべてのプロセスをモニタする場合は、この MIB を使用します。インストールされているシスコのアプリケーションだけを監視するには、SYSAPPL-MIB.Disk Space および RTMT を使用します。

HOST-RESOURCES-MIB で表示される使用済みディスク容量と使用可能ディスク容量の値は、RTMT で表示されるディスク容量の値と一致しない場合があります。これは、ファイル システムの予約済みディスク ブロックにおける最小空き容量の割合が原因です。Cisco Unified Communications Manager 6.x および 7.0 システムの minfree 値は 1% であるため、RTMT および HOST-RESOURCES-MIB で表示される使用済みディスク容量の値には 1% の相違があります。

- RTMT では、df の報告値を使用して使用済みディスク容量の値が表示されます。この値は、[（合計容量 - 使用可能容量）/ 合計容量] X 100 で計算されます。合計容量には最小空き容量も含まれます。
- HOST-RESOURCES-MIB での使用済みディスク容量の値は [hrStorageUsed / hrStorageSize] X 100 で計算されます。hrStorageSize には最小空き容量は含まれません。

CISCO-CDP-MIB のヒント

ここでは、次の項目について説明します。

関連トピック

よく寄せられる質問 （184 ページ）
一般的なヒント （183 ページ）

一般的なヒント

次のログおよび情報を収集して分析します。

- **set trace enable Detailed cdpmib** コマンドを使用して、cdpAgt () の詳細トレースを設定します。
- [Cisco Unified Serviceability] ウィンドウ（**[ツール（Tools）] > [コントロール センター（Control Center）] > [ネットワーク サービス（Network Services）]**）から Cisco CDP Agent サービスを再起動し、しばらく待機します。
- 次のトレース ファイルを収集します。
  - **file get activelog cm/trace/cdpmib/sdi** コマンドを使用して Cisco CDP Agent のトレースをイネーブルにし、**file get activelog cm/trace/cdp/sdi** コマンドを使用して Cisco CDP デーモンのトレースをイネーブルにします。
  - Real-Time Monitoring Tool（RTMT）の **[トレースおよびログ セントラル（Trace & Log Central）] > [ファイルの収集（Collect Files）] > [Cisco CallManager SNMP Service] >**

[Cisco CDP Agent および Cisco CDP（Cisco CDP Agent and Cisco CDP）] を使用して、Cisco CDP Agent およびデーモンのトレースをイネーブルにします。

- ログが収集されたあと、**set trace disable cdpmib** コマンドを使用してトレース設定をリセットします。

よく寄せられる質問

CDP インターフェイス テーブルおよび globalinfo テーブルが空白なのはなぜですか。

使用している Cisco UCM リリースにこの機能があることを確認します。ない場合は、アップグレードしてください。

インターフェイス テーブルに設定されている MessageInterval の値が、CDP MIB のグローバル テーブルにも設定されているのはなぜですか。

HoldTime 値が MessageInterval 値よりも大きいかどうかを確認します。小さい場合、インターフェイス テーブルとグローバル テーブルのどちらからも MessageInterval 値は設定されません。

SYSAPP-MIB のヒント

ここでは、SYSAPP-MIB のヒントについて説明します。

関連トピック

ログの収集 （184 ページ）
Cisco Unified Communications Manager 8.0 でのサーブレットの使用 （184 ページ）

ログの収集

次のログおよび情報を収集して分析します。コマンド **file get activelog** *<paths in the following bullets>* を実行します。

- SNMP Master Agent のパス：`/platform/snmp/snmpdm/*`
- システム アプリケーション エージェントのパス：`/platform/snmp/sappagt/*`

Cisco Unified Communications Manager 8.0 でのサーブレットの使用

SysAppl MIB には、インストールされて実行されているインベントリを一度に取得する方法が用意されています。SysAppl エージェントからは、アクティブまたは非アクティブなサービスのリストは提供されません。アプリケーションとサービスの実行中状態または実行中以外の状態だけ示すことができます。Web App サービス/サーブレットは、SysAppl MIB を使用して監視できません。8.0 システムには、次のサーブレットがあります。

- Cisco CallManager Admin
- Cisco CallManager Cisco IP Phone サービス
- Cisco CallManager Personal Directory
- Cisco CallManager のサービスアビリティ
- Cisco CallManager のサービスアビリティ RTMT
- Cisco Dialed Number Analyzer
- Cisco エクステンション モビリティ
- Cisco Extension Mobility アプリケーション
- Cisco RTMT Reporter Servlet
- Cisco Tomcat Stats Servlet
- Cisco Trace Collection Servlet
- Cisco AXL Web Service
- Cisco Unified Mobile Voice Access Service
- Cisco エクステンション モビリティ
- Cisco IP Manager Assistant
- Cisco WebDialer Web Service
- Cisco CAR Web Service
- Cisco Dialed Number Analyzer

システムの健全性のために重要なサービス ステータスを監視するには、次のアプローチを推奨します。

- GetServiceStatus という Cisco Unified Serviceability API を使用します。この API では、Web アプリケーション タイプと Web 以外のアプリケーション サービス両方のアクティベーション ステータスなど、完全なステータス情報が提供されます（詳細については、『*AXL Serviceability API Guide*』を参照してください）。
- **utils service list** コマンドを使用して、さまざまなサービスのステータスをチェックします。
- syslog メッセージを使用して、servM で生成されたメッセージをモニタします。次に例を示します。

```
Mar 18 16:40:52 ciscart26 local7 6 : 92: Mar 18 11:10:52.630 UTC :
%CCM_SERVICEMANAGER-SERVICEMANAGER-6-ServiceActivated: Service Activated.
Service Name:Cisco CallManager SNMP Service App ID:Cisco Service Manager
Cluster ID: Node ID:ciscart26
```

SNMP 開発者のヒント

SNMP 開発者のトラブルシューティングのヒントについて、この項を確認してください。

- CISCO-CCM-MIB のサポート リストについては、次のリンクで CISCO-CCM-CAPABILITY-MIB を参照してください。

  http://tools.cisco.com/Support/SNMP/do/BrowseMIB.do?local=en&step=2&mibName=CISCO-CCM-CAPABILITY

  CISCO-CCM-CAPABILITY

  「CISCO-CCM-CAPABILITY-MIB」で説明されているとおり、ccmPhoneDevicePoolIndex はサポートされていないため、0 を返します。Cisco UCM デバイス登録アラームには、現在はデバイス プール情報は含まれていません。

- Cisco UCM SNMP Service が実行中でない場合、MIB の次のテーブルだけが応答します。
  - ccmGroupTable
  - ccmRegionTable
  - ccmRegionPairTable
  - ccmDevicePoolTable
  - ccmProductTypeTable
  - ccmQualityReportAlarmConfigInfo
  - ccmGlobalInfo

  Cisco UCM SNMP Service を実行中にするには、Cisco Unified Serviceability でサービスをアクティブにして起動します。

- SYS-APPL MIB の SysApplInstallPkgTable を照会して、システムにインストールされている Unified Communications Manager アプリケーションのインベントリを取得します。SYS-APPL MIB の SysApplRunTable を照会して、システムで実行されている Unified Communications Manager アプリケーションのインベントリを取得します。システム アプリケーション エージェントでは、アクティブまたは非アクティブになっているサービスを表示したり、Web アプリケーションのサービスやサーブレットを監視したりすることはできません。このため、システムの正常性や Cisco Unified Communications Manager アプリケーションのサービス ステータスを監視するには、次の方法を使用します。
  - getservicestatus という Cisco Unified Serviceability API を使用して、Web アプリケーションと Web 以外のアプリケーションの両方について、アクティベーション ステータスなどの完全なステータス情報を提供します。詳細については、『AXL Serviceability API Guide』を参照してください。
  - CLI コマンド **utils service list** を使用して、サービス ステータスを確認します。
  - syslog を使用して、servM で生成されたメッセージをモニタします（次の例を参照）。

```
Mar 18 16:40:52 ciscart26 local7 6 : 92: Mar 18 11:10:52.630 UTC :
%CCM_SERVICEMANAGER-SERVICEMANAGER-6-ServiceActivated: Service Activated.
 Service Name:Cisco CallManager SNMP Service App ID:Cisco Service Manager
 Cluster ID: Node ID:ciscart26
```

（注） Unified Communications Manager が使用する Web アプリケーション サービスおよびサーブレットは次のとおりです。Cisco UCM Admin、Cisco UCM Cisco IP 電話サービス、Cisco UCM Personal Directory、Cisco Unified Serviceability、Cisco Unified RTMT、Cisco Extension Mobility、Cisco Extension Mobility アプリケーション、Cisco Unified RTMT Reporter Servlet、Cisco Tomcat Stats Servlet、Cisco Trace Collection Servlet、Cisco AXL Web Service、Cisco Unified Mobile Voice Access Service、Cisco Extension Mobility、Cisco IP Manager Assistant、Cisco WebDialer Web Service、Cisco CAR Web Service、および Cisco Dialed Number Analyzer。

要求タイムアウトの回避策

SNMP 要求で複数の OID を指定し、変数が空のテーブルを指している場合、タイムアウトの問題により、NO_SUCH_NAME（SNMPv1 の場合）または GENERIC ERROR（SNMPv2c または SNMPv3 の場合）が返されることがあります。Unified Communications Manager 処理エンジンを保護するためにスロットリングを強化すると、タイムアウトが発生することがあります。

（注） スカラ オブジェクトを使用すると、CCMH323DeviceTable および ccmSIPDeviceTable のエントリ数を取得できます。そのため、SNMP マネージャ（クライアント）は、エントリが存在しない場合に、これらのテーブルでの不要な **get/getnext** オペレーションをしなくて済みます。

SNMP 開発者は、この問題に対する次の回避策を使用できます。

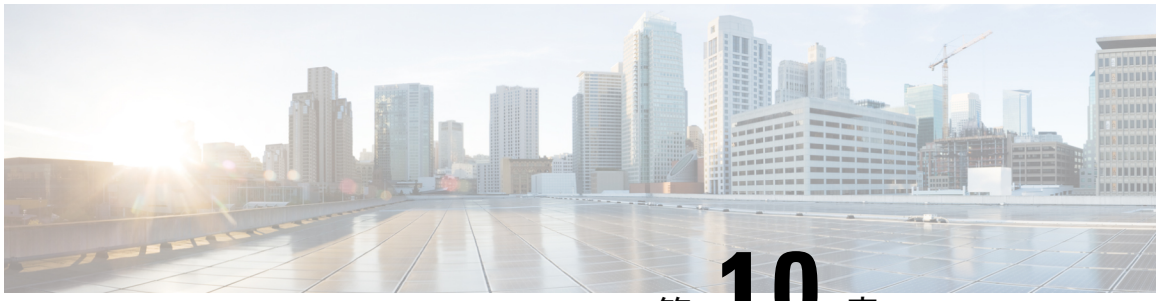
- 最初に、テーブルにアクセスする前に利用可能なスカラ変数（1.3.6.1.4.1.9.9.156.1.5）を使用してテーブル サイズを判別するか、目的のテーブルで **get** 操作を実行してから、空ではないテーブルを照会します。
- 1 回の要求で照会する変数の数を減らします。たとえば、空のテーブルに対して管理アプリケーションのタイムアウトが 3 秒に設定されている場合、OID を 1 つだけ指定します（空でないテーブルの場合、1 つのデータ行の取得に 1 秒かかります）。
- 応答タイムアウトの値を大きくします。
- 再試行回数を減らします。
- getbulk SNMP API を使用しないようにします。getbulk API では MaxRepetitions で指定されているレコード数が取得されるため、次のオブジェクトがテーブルまたは MIB の範囲外であっても、それらのオブジェクトが取得されます。空のテーブルの場合は、さらに遅延が大きくなります。テーブルが空でなく、レコード数が既知の場合は、getbulk API を使用します。このような場合には、MaxRepetitions を 5 秒に設定し、5 秒以内の応答を要求します。

- 既存の制限に適合させるには、SNMP 照会を作成します。
- 多数の電話機が Cisco UCM に登録されている場合は、複数の getbulk を実行して PhoneTable を定期的にウォークしないようにします。電話機の更新が存在する場合に更新を行う ccmPhoneStatusUpdateTable を使用すると、PhoneTable をウォークするかどうかを決定できます。

詳細情報の入手先

関連資料

- 『*Command Line Interface Reference Guide for Cisco Unified Solutions*』
- 『*Cisco Unified Serviceability Administration Guide*』の「「SNMP」」の章



第 10 章

TAC とのケースのオープン

この項では、TAC に問い合わせる場合に必要な情報の詳細、および TAC の担当者と情報を共有する方法について説明します。

シスコテクニカルサポートでは、有効なシスコ サービス契約を保有しているすべてのお客様、パートナー、リセラー、およびディストリビュータ向けに、24時間対応の高い評価を得ているテクニカル サポートを用意しています。Cisco Technical Support Web サイトでは、シスコ製品やシスコ テクノロジーに関する技術的な問題を解決するためのオンラインのドキュメントやツールをご利用いただけます。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

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 と S4 の問題とは、ネットワークの障害が軽微である場合、あるいは製品情報が必要な場合を意味します）。状況をご説明いただくと、TAC Service Request ツールが自動的に推奨する解決方法を提供します。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 に関して、またはインターネット アクセスがない場合は、電話で Cisco TAC にご連絡ください。（S1 または S2 の問題とは、運用中のネットワークがダウンした場合、あるいは重大な障害が発生した場合を意味します）。S1 および S2 の問題には Cisco TAC の技術者がただちに対応し、業務を円滑に実行できるよう支援します。

電話でサービス リクエストを開く場合は、次の番号にご連絡ください。

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

米国：1 800 553 2447

詳細な 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

- 必要な情報 （190 ページ）
- 必要な予備的情報 （190 ページ）

必要な情報

Cisco TAC に対してサービス リクエストをオープンする場合は、問題を特定し、その内容を把握しやすくするための予備的情報をご提供いただく必要があります。問題の内容によっては、追加の情報をご提供いただく必要があります。次に示す情報をエンジニアから要求されなくても遅滞なく収集してください。サービス リクエストをオープンし、エンジニアから要求されたあとに収集を開始すると、問題の解決が遅くなります。

関連トピック

Cisco Live! （193 ページ）
Cisco Secure Telnet （194 ページ）
全般情報 （191 ページ）
ネットワーク レイアウト （190 ページ）
オンライン ケース （192 ページ）
問題の説明 （191 ページ）
リモート アクセス （193 ページ）
必要な予備的情報 （190 ページ）

必要な予備的情報

すべての問題において、必ず次の情報を TAC に提供してください。この情報を収集および保存して TAC サービス リクエストをオープンするときに使用できるようにし、変更があった場合には定期的に更新します。

関連トピック

全般情報 （191 ページ）
ネットワーク レイアウト （190 ページ）
問題の説明 （191 ページ）

ネットワーク レイアウト

物理セットアップおよび論理セットアップの詳細な説明、および音声ネットワークに関連する次のすべてのネットワーク要素をお知らせください（存在する場合）。

- Unified Communications Manager

- バージョン（Unified Communications Manager Administration で [**詳細（Details**）] を選択）
- Unified Communications Manager の数
- セットアップ（スタンドアロン、クラスタ）
    - Unity
- バージョン（Unified Communications Manager Administration から）
- 統合のタイプ
    - 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 のバージョン
- show tech コマンド（IOS ゲートウェイ）
- Unified Communications Manager の負荷（Skinny ゲートウェイ）
    - スイッチ（Switch）
- OS のバージョン
- VLAN の設定
    - ダイヤル プラン：番号付け方式、コール ルーティング

Visio や JPG などで作成した詳細な図を提出すると理想的です。ホワイトボードを使用して、Cisco Live! セッションから図を提供することもできます。

問題の説明

問題が発生したときにユーザが実行した処理について、手順ごとの詳細を提供します。詳細情報には、次の内容を含める必要があります。

- 予想される動作
- 実際に観察された動作の詳細

全般情報

次の情報を準備する必要があります。

- 新しいインストールかどうか
- 以前のバージョンの Unified Communications Manager がインストールされている場合、最初からこの問題が発生していたかどうか（最初から発生していない場合は、最近システムに対して行った変更）
- この問題は再現可能かどうか
  - 再現可能である場合は、通常の環境で発生するか、または特別な環境で発生するか
  - 再現不可能である場合は、問題発生のタイミングが特別であったかどうか
  - 発生の頻度
- 影響のあるデバイス
  - ランダムなデバイスではなく、特定のデバイスが影響を受ける場合、影響を受けるデバイスの共通点は何か
  - 問題に関連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）
- コール パス上のデバイス（存在する場合）

オンライン ケース

Cisco.com から TAC Case Open ツールのオンライン サービスを使用すると、他のすべてのサービス リクエスト オープン方法よりも優先的に処理されます。ただし、高優先度のサービス リクエスト（P1 および P2）は例外です。

サービス リクエストをオープンする場合は、問題についての正確な説明を提供してください。問題の説明を提供すると、すぐに解決策として使用できる可能性がある URL リンクが返されます。

リンクを参照しても問題の解決策が見つからない場合は、プロセスを続行して、サービス リクエストを TAC エンジニアに送信してください。

Serviceability Connector

Serviceability Connector の概要

この製品を活用することで、シスコのテクニカル サポート スタッフがより迅速にインフラストラクチャの問題を診断できます。診断ログと情報を検出、取得して SR ケースに保存するタスク、および診断シグネチャに対する分析をトリガーするタスクを自動化することで、TAC がオンプレミスの機器に関する問題をより効率的に特定して解決できるようにします。

この機能は、お客様の社内に導入された *Serviceability Connector* を使用します。*Serviceability Connector* は、ネットワーク内の専用 Expressway（「コネクタ ホスト」）に常駐するソフト

ウェアです。このソフトウェアは、Cisco Webex に接続してデータ収集の要求を受信し、オンプレミス機器の API を使用して要求されたデータを収集します。要求されたデータは、シスコの SR ファイル ストアに安全にアップロードされ、SR ケースに添付されます。

Serviceability サービスを使用する利点

- TACエンジニアが問題の診断を実行するときに関連ログを要求できるようにし、追加のログを要求したり手動で収集して提供したりすることで生じる遅延を避けることによって、ログの収集をス迅速化します。これにより、問題解決に要する時間を数日短縮できる可能性があります。
- TAC の Collaboration Solution Analyser とその診断シグネチャのデータベースと併せて、ログが自動的に分析され、既知の問題が特定され、既知の修正または回避策が推奨されます。

Serviceability Connector の TAC サポート

Serviceability Connector の詳細については、https://www.cisco.com/go/serviceability を参照するか、TAC の担当者に問い合わせてください。

Cisco Live!

安全で暗号化された Java アプレットである Cisco Live! を利用すると、コラボレーティブ Web ブラウジング、URL 共有、ホワイトボード、Telnet、クリップボード ツールを使用することによって、Cisco TAC のエンジニアとより効率的に協同して作業できます。

Cisco Live! には次の URL からアクセスできます。

```
http://c3.cisco.com/
```

リモート アクセス

リモート アクセスを使用すると、必要なすべての装置に対して Terminal Services セッション（リモート ポート 3389）、HTTP セッション（リモート ポート 80）、および Telnet セッション（リモート ポート 23）を確立できます。

注意 ダイヤルインを設定する場合は、システムに対する脆弱性となるため、**login:cisco** または **password:cisco** は使用しないでください。

TAC エンジニアが次のいずれかの方法を使用してデバイスにリモート アクセスすることを許可すると、多くの問題を非常に迅速に解決できます。

- パブリック IP アドレスが設定された装置

- ダイヤルイン アクセス：（プリファレンスの高い順に）アナログ モデム、統合デジタル通信網（ISDN）モデム、バーチャル プライベート ネットワーク（VPN）
- ネットワーク アドレス変換（NAT）：プライベート IP アドレスが設定された装置へのアクセスを可能にする IOS およびプライベート インターネット エクスチェンジ（PIX）。

エンジニアの介入時にファイアウォールによってIOSトラフィックとPIXトラフィックが遮断されないこと、およびサーバ上で Terminal Services などの必要なすべてのサービスが開始されていることを確認してください。

（注） TACでは、すべてのアクセス情報は厳重に管理されます。また、お客様の同意なしにシステムを変更することはありません。

Cisco Secure Telnet

シスコ サービス エンジニア（CSE）は、Cisco Secure Telnet を使用して、サイト上の Unified Communications Managerサーバに対して透過的にファイアウォールアクセスを実行できます。

Cisco Secure Telnet は、シスコのファイアウォール内部で Telnet クライアントをイネーブル化することによって、ファイアウォールで稼働する Telnetデーモンに接続します。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、Unified Communications Manager 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、許可があった場合にだけお客様のネットワークにアクセスします。サイトに、このプロセスの開始を支援するネットワーク管理者を配置する必要があります。

ファイアウォールによる保護

ほとんどすべての内部ネットワークでは、外部から内部のホストシステムへのアクセスを制限するためにファイアウォールアプリケーションが使用されています。これらのアプリケーションでは、ネットワークとパブリック インターネットとの間のIP接続を制限することによって、ネットワークが保護されます。

ファイアウォールでは、許可するように明示的に再設定しないかぎり、外部から開始される TCP/IP 接続が自動的にブロックされます。

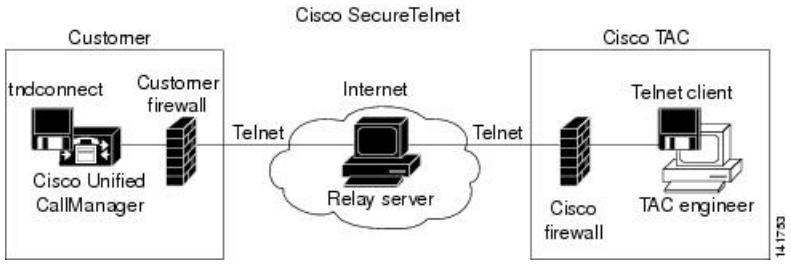
通常、企業ネットワークではパブリック インターネットとの通信が許可されますが、ファイアウォール内部から外部ホストに向けて開始される接続だけが許可されます。

Cisco Secure Telnet の設計

Cisco Secure Telnet では、ファイアウォールの内側から簡単に Telnet 接続を開始できるという技術を活用しています。外部のプロキシ マシンを使用して、ファイアウォールの内側からの TCP/IP 通信が Cisco TAC にある別のファイアウォールの内側のホストへとリレーされます。

このリレーサーバを使用することによって、両方のファイアウォールの完全性が維持され、また保護されたリモート システム間の安全な通信がサポートされます。

図 *1 : Cisco Secure Telnet* システム



Cisco Secure Telnet の構造

外部のリレー サーバによって、お客様のネットワークとシスコとの間に Telnet トンネルが構築され、接続が確立されます。これにより、Unified Communications Manager サーバの IP アドレスおよびパスワード識別子を CSE に送信できます。

（注） パスワードは、管理者と CSE が相互に同意した文字列です。

管理者は、Telnet トンネルを開始することによって、プロセスを開始します。これにより、ファイアウォールの内部からパブリック 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。次に、Telnet トンネルによって、ローカルの Telnet サーバへの別の接続が確立され、エンティティ間の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 上で動作するシステム、または UNIX オペレーティング システムに準拠して動作します。

ローカル サイトの Cisco Communications Manager がパスワードを受け入れると、Cisco TAC で実行されている Telnet クライアントは、ローカル ファイアウォールの内側で動作する Telnet デーモンに接続します。この結果確立される透過的接続によって、マシンがローカルで使用されている場合と同様にアクセスできるようになります。

安定的な Telnet 接続が確立されると、CSE は、Unified Communications Manager サーバに対してメンテナンス タスク、診断タスク、およびトラブルシューティング タスクを実行するためのあらゆるリモート有用性機能を導入できます。

CSE が送信するコマンドおよび Unified Communications Manager サーバから発行される応答を確認することはできますが、コマンドや応答が常に完全な形式で表示されるとは限りません。

リモート アカウントの設定

シスコ サポートがトラブルシューティングのためにご使用のシステムに一時的にアクセスできるよう、Unified Communications Manager でリモート アカウントを設定します。

手順

ステップ 1 [Cisco Unified オペレーティング システムの管理（Cisco Unified Operating System Administration）] で、**[サービス（Services）] > [リモート サポート（Remote Support）]** を選択します。

ステップ 2 [アカウント名（Account Name）] フィールドに、リモート アカウントの名前を入力します。

ステップ 3 [アカウントの有効期限（Account Duration）] フィールドに、アカウントの有効期限を日数で入力します。

ステップ 4 **[保存（Save）]** をクリックします。
システムは、暗号化パス フレーズを生成します。

ステップ 5 シスコのサポート担当者に連絡して、リモート サポート アカウント名とパス フレーズを提供します。

第 11 章

ケース スタディ：Cisco Unified IP Phone コールのトラブルシューティング

この付録では、Cisco Unified IP Phone のトラブルシューティングに関する 2 つのケース スタディを示します。

クラスタ内 Cisco Unified IP Phone コールのトラブルシューティング

この項のケース スタディでは、クラスタ内コールと呼ばれる、クラスタ内の 2 台の Cisco Unified IP Phone 間のコール フローについて詳しく説明します。このケース スタディでは、Unified Communications Manager と Cisco Unified IP Phone の初期化、登録、およびキープアライブ プロセスについても説明します。このプロセスについて説明してから、クラスタ内コール フローについて詳しく説明します。

関連トピック

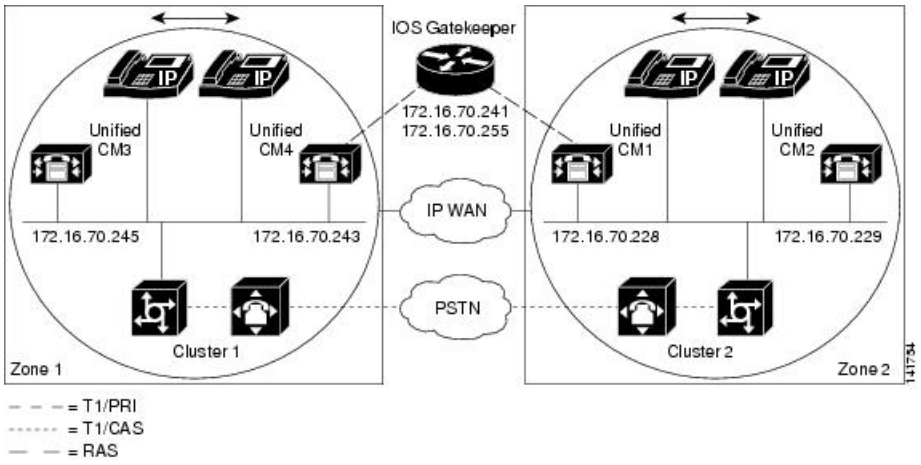
Cisco Unified Communications Manager の初期化プロセス （199 ページ）
Cisco Unified Communications Manager のクラスタ内コール フローのトレース （202 ページ）
Cisco Unified Communications Manager のキープアライブ プロセス （201 ページ）
Cisco Unified Communications Manager の登録プロセス （201 ページ）
Cisco Unified IP Phone の初期化プロセス （198 ページ）
トポロジの例 （198 ページ）
自己起動プロセス （200 ページ）
トラブルシューティング ツール （5 ページ）

トポロジの例

Cluster 1 と Cluster 2 の 2 つのクラスタがあるとします。Cluster 1 には Unified CM3 と Unified CM4 という 2 つの Unified Communications Manager があり、Cluster 2 には Unified CM1 と Unified CM2 という 2 つの Unified Communications Manager があります。

このケース スタディのトレースは、次の図に示すように、Cluster 2 にある Unified CM1 から収集されます。Cluster 2 の 2 台の Cisco Unified IP Phone がコール フローのベースとなります。これら 2 台の Cisco Unified IP Phone の IP アドレスは、それぞれ 172.16.70.230（電話番号 1000）と 172.16.70.231（電話番号 1001）です。

図 *2:* クラスタ内の *Cisco Unified IP Phone* と *Cisco Unified IP Phone* の間のコールのサンプル トポロジ



Cisco Unified IP Phone の初期化プロセス

次に示す手順で、Cisco Unified IP Phone の初期化（ブートアップ）プロセスについて詳しく説明します。

手順

1. DHCP サーバで適切なオプション（オプション 066 やオプション 150 など）を設定済みの場合、Cisco Unified IP Phone は初期化時に DHCP サーバに要求を送信し、IP アドレス、ドメイン ネーム システム（DNS）サーバ アドレス、および TFTP サーバ名またはアドレスを取得します。また、DHCP サーバでこれらのオプション（オプション 003）を設定済みの場合は、デフォルト ゲートウェイ アドレスも取得します。
2. DHCP が TFTP サーバの DNS 名を送信する場合は、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 アドレスが必要です。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 が設定されていないため、DHCP サーバは TFTP の IP アドレスを送信しました。
3. DHCP 応答に TFTP サーバ名が含まれていない場合、Cisco Unified IP Phone はデフォルトのサーバ名を使用します。

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。初めて電話機を Unified Communications Manager に登録する場合は、デフォルト ファイルの SEPdefault.cnf が Cisco Unified 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 台めの Cisco Unified IP Phone に IP アドレス 172.16.70.230（MAC アドレスは SEP0010EB001720）を使用し、2 台めの Cisco Unified IP Phone に IP アドレス 172.16.70.231（MAC アドレスは SEP003094C26105）を使用します。
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 Unified Communications Manager の IP アドレスが含まれています。Cisco Unified IP Phone は、この IP アドレスを使用してプライマリ Unified Communications Manager に接続して登録します。
6. Cisco Unified IP Phone が Unified Communications Manager に接続して登録すると、Unified Communications Manager から Cisco Unified IP Phone に、使用する実行ファイルのバージョン（ロード ID と呼ばれる）が通知されます。指定されたバージョンが Cisco Unified 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 Unified IP Phone は TFTP サーバに新しい実行ファイルを要求し、自動的にリセットします。

Cisco Unified Communications Manager の初期化プロセス

ここでは、Unified CM1（IP アドレス 172.16.70.228 で識別される）からキャプチャされるトレースを使用して、Unified Communications Manager の初期化プロセスについて説明します。上記のとおり、SDI トレースはエンドポイント間で送信されるすべてのパケットに関する詳しい情報を出力するため、非常に効果的なトラブルシューティング ツールです。

ここでは、Unified Communications Manager の初期化時に発生するイベントについて説明します。トレースの読み方を理解すると、Unified Communications Manager のさまざまなプロセスや、会議やコール転送などのサービスに対するそれらのプロセスの影響を適切にトラブルシューティングできるようになります。

次のメッセージは Unified Communications Manager の SDI トレース ユーティリティから出力されたもので、Unified Communications Manager の 1 つ（この場合は Unified CM1）での初期化プロセスを示しています。

- 最初のメッセージは、Unified Communications Manager が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、Unified Communications Manager がデフォルト データベース（この場合はプライマリ 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、Unified Communications Manager が TCP ポート 8002 でさまざまな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、これらのメッセージを受信した後、Unified Communications Manager が別の Unified Communications Manager である Unified CM2（172.16.70.229）を自分のリストに追加したことを示しています。

- 5 番目のメッセージは、Unified Communications Manager が起動し、Unified Communications Manager バージョン 3.1(1) を実行中であることを示しています。

```
16:02:47.765 CCM|CMProcMon - Communications ManagerState Changed -
Initialization Started.16:02:47.796 CCM|NodeId: 0, EventId: 107 EventClass:
 3 EventInfo: Cisco CCMDatabase 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

稼働状態になった後、Unified Communications Manager は内部で他のいくつかのプロセスを起動します。こ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、Unified Communications Manager の機能に関連する問題をトラブルシューティングするとき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、使用できないとします。この問題をトラブルシューティングするには、これらのトレースを監視して、Unified Communications Manager が RoutePlanManager を起動したかどうか、および RouteLists をロードしようとしているかどうかを確認します。次の設定の例は、RouteListName=「ipwan」 と RouteGroupName=「ipwan」 がロードされ、起動していることを示しています。

```
16:02:51.031 CCM|MulicastPointManager - Started16:02:51.031
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、デバイス 172.16.70.245 を追加している RouteGroup を示しています。このデバイスは Cluster 1 にある Unified CM3 デバイスで、H.323 デバイスと見なされます。このケース スタディでは、RouteGroup は Cisco IOS ゲートキーパーの許可を受けてコールを Cluster 1 にある Unified CM3 にルーティングするために作成されています。Cluster 1 の Cisco Unified IP Phone にコールをルーティング中に問題が発生した場合は、次のメッセージが問題の原因を見つけるのに役立ちます。

```
16:02:51.671 CCM|RouteGroup - DeviceName=「172.16.70.245」16:02:51.671
CCM|RouteGroup -AllPorts
```

初期化プロセスの一部で、Unified Communications Manager が 「Dn」（ディレクトリ番号）を追加していることが示されています。これらのメッセージを確認すると、Unified Communications Manager がデータベースからディレクトリ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
 started16:02:51.843 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、Unified Communications Manager のデバイス マネージャによって 2 つのデバイスが静的に初期化されています。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 Unified Communications Manager を取得します。その Unified Communications Manager は、この Unified Communications Manager に H.323 ゲートウェイとして登録されます。

```
16:02:52.250 CCM|DeviceManager: Statically Initializing Device;
DeviceName=172.16.70.22616:02:52.250 CCM|DeviceManager: Statically Initializing
 Device; DeviceName=172.16.70.245
```

Cisco Unified Communications Manager 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。デバイスの電源がオンになると、デバイスは DHCP を使用して情報を取得し、TFTP サーバに接続して .cnf ファイルを取得した後、.cnf で指定されている Unified Communications Manager に接続します。デバイスは、MGCP ゲートウェイ、Skinny ゲートウェイ、または Cisco Unified IP Phone の可能性があります。そのため、デバイスが Cisco ネットワークで正常に登録されたかどうかを検出できる必要があります。

次のトレースでは、Unified Communications Manager 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（Unified CM1 上の MTP サービス）と CFB_nsa-cm1（Unified CM1 上の会議ブリッジ サービス）です。これらは Unified Communications Manager 上で実行され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 Unified Communications Manager のキープアライブ プロセス

ステーション、デバイス、またはサービスと Unified Communications Manager では、次のメッセージを使用して相互間の通信チャネルの情報を維持します。メッセージは、Unified

Communications Manager とステーション間の通信リンクをアクティブに保つキープアライブ シーケンスを開始します。次のメッセージは、Unified Communications Manager 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]
```

次のトレースのメッセージは、Unified Communications Manager 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キープアライブ シーケンスを示しています。これらのメッセージも、Unified Communications Manager 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=4fa7dc016:03:02.328 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 Unified Communications Manager のクラスタ内コール フローのトレース

次の SDI トレースは、クラスタ内コール フローを詳しく示しています。コール フローの Cisco Unified 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 にある Cisco Unified IP Phone（dn：1001、tcpHandle：0x4fbbc30、IP アドレス：172.16.70.231）が同じクラスタ内の別の Cisco Unified IP Phone（dn：1000、tcpHandle：0x4fbb150、IP アドレス：172.16.70.230）をコールしています。トレースでデバイスを追跡するには、デバイスの TCP ハンドル値、タイムスタンプ、または名前を調べます。デバイスの TCP ハンドル値は、デバイスがリブートされるかオフラインになるまで変わりません。

次のトレースは、Cisco Unified IP Phone（1001）がオフフックになっていることを示しています。次のトレースは、Cisco Unified IP Phone に表示される固有のメッセージ、TCP ハンドル、発信番号を示しています。ユーザはまだ番号をダイヤルしていないため、この時点では発信番号は表示されていません。次の情報は、Cisco Unified IP Phone と Unified Communications Manager 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=0x4fbbc3016:05:41.625 CCM|StationD - stationOutputDisplayText
tcpHandle=0x4fbbc30, Display= 1001
```

次のトレースは、Unified Communications Manager から Cisco Unified IP Phone に発信される Skinny Station メッセージを示しています。最初のメッセージによって、発呼側 Cisco Unified IP Phone のランプがオンになります。

```
16:05:41.625 CCM|StationD - stationOutputSetLamp stim: 9=Line instance=1
lampMode=LampOn tcpHandle=0x4fbbc30
```

Unified Communications Manager は stationOutputCallState メッセージを使用して、特定のコール関連情報をステーションに通知します。

```
16:05:41.625 CCM|StationD - stationOutputCallState tcpHandle=0x4fbbc30
```

Unified Communications Manager は stationOutputDisplayPromptStatus メッセージを使用して、Cisco Unified IP Phone にコール関連のプロンプト メッセージを表示します。

```
16:05:41.625 CCM|StationD - stationOutputDisplayPromptStatus tcpHandle=0x4fbbc30
```

Unified Communications Manager は stationOutputSelectSoftKey メッセージを使用して、Skinny Station で特定のソフトキー セットを選択します。

```
16:05:41.625 CCM|StationD - stationOutputSelectSoftKeys tcpHandle=0x4fbbc30
```

Unified Communications Manager は次のメッセージを使用して、表示用の正しい回線コンテキストを Skinny Station に通知します。

```
16:05:41.625 CCM|StationD - stationOutputActivateCallPlane tcpHandle=0x4fbbc30
```

次のメッセージは、番号分析プロセスで着信番号の識別、データベース内のルーティング一致の確認ができる状態になっていることを示しています。エントリ cn=1001 は発呼側番号、dd=「」 はダイヤルされた番号（着信番号になる）を示しています。電話機が StationInit メッセージを送信し、Unified Communications Manager が StationD メッセージを送信し、Unified Communications Manager が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、Unified Communications Manager が内部ダイヤル トーンを発呼側 Cisco Unified IP Phone で鳴らしていることを示します。

```
16:05:41.625 CCM|StationD - stationOutputStartTone: 33=InsideDialTone
tcpHandle=0x4fbbc30
```

Unified Communications Manager は着信メッセージを検出し、Cisco Unified 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、すぐに出力トーンを停止します。

```
16:05:42.890 CCM|StationInit - InboundStim - KeypadButtonMessageID kpButton:
1 tcpHandle=0x4fbbc3016:05:42.890 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」)
```

Unified Communications Manager は、番号一致を判別できるだけの十分な番号を受信すると、番号分析の結果を表形式で出力します。一致する番号はすでに見つかっているため、Unified Communications Manager は、この時点以降に電話機で押される番号は無視します。

```
16:05:43.562 CCM|Digit analysis: analysis results16:05:43.562
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、Unified Communications Manager 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、Unified Communications Manager が着信側の Cisco Unified IP Phone に、着信コールを示す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
```

次のトレースでは、Unified Communications Manager が着信側の Cisco Unified IP Phone に、呼び出し音やディスプレイ通知などのコール関連情報を提供しています。ここでも、トレース全体で同じ tcpHandle が使用されているため、すべてのメッセージが同じ Cisco Unified 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=0x4fbb15016:05:43.578 CCM|StationD - stationOutputDisplayNotify
tcpHandle=0x4fbb150 16:05:43.578 CCM|StationD - stationOutputDisplayPromptStatus
 tcpHandle=0x4fbb150 16:05:43.578 CCM|StationD - stationOutputSelectSoftKeys
tcpHandle=0x4fbb150
```

Unified Communications Manager は、同様の情報を発呼側の Cisco Unified IP Phone にも提供しています。ここでも、Cisco Unified IP Phone は tcpHandle で識別されます。

```
16:05:43.578 CCM|StationD - stationOutputCallInfo CallingPartyName=1001,
CallingParty=1001, CalledPartyName=, CalledParty=1000,
tcpHandle=0x4fbbc3016:05:43.578 CCM|StationD - stationOutputCallInfo
CallingPartyName=1001, CallingParty=1001, CalledPartyName=1000, CalledParty=1000,
 tcpHandle=0x4fbbc30
```

次のトレースでは、Unified Communications Manager が発呼側の Cisco Unified IP Phone でアラート音または呼び出し音を鳴らし、接続が確立したことを通知しています。

```
16:05:43.578 CCM|StationD - stationOutputStartTone: 36=AlertingTone
tcpHandle=0x4fbbc3016:05:43.578 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 Unified IP Phone はオフフックになり、Unified Communications Manager は発呼側での呼び出し音の生成を停止します。

```
16:05:45.140 CCM|StationD - stationOutputStopTone tcpHandle=0x4fbbc30
```

次のメッセージでは、Unified Communications Manager 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、Unified Communications Manager 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）を示す整数です。

（注） 通常、この値は 30 ミリ秒に設定されます。この事例では、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、Unified Communications Manager は情報を着信側（1000）に提供します。

```
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
```

Unified Communications Manager は、RTP ストリーム用のオープン チャネルの確立に対する確認応答メッセージを着信側から受信し、着信側の IP アドレスも受け取ります。このメッセージは、Skinny Station に関する 2 つの情報を Unified Communications Manager に通知します。まず、オープン処理のステータスが通知されます。次に、リモートエンドへの転送に使用される受信ポートのアドレスと番号が通知されます。RTP ストリームのトランスミッタ（発呼側）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
```

Unified Communications Manager は、次のメッセージを使用して、指定されたリモート Cisco Unified IP Phone の IP アドレスとポート番号にオーディオ ストリームとビデオ ストリームの転送を開始するようにステーションに指示します。

```
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、上記のメッセージが着信側に送信されています。これらのメッセージのあとに、着信側と発呼側の間でRTPストリームが開始されたことを示すメッセージが続きます。

```
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
```

最後に発呼側の Cisco IP 電話がオンフックになると、Skinny Station と Unified Communications Manager 間の制御メッセージと 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
```

クラスタ間 Cisco Unified IP Phone コールのトラブルシューティング

この項のケース スタディでは、異なるクラスタにある別の Cisco Unified IP Phone にコールを発信する Cisco Unified 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 Unified IP Phone コールと呼ばれます。

関連トピック

コール フローのトレース （207 ページ）
失敗したコール フロー （208 ページ）
クラスタ間 H.323 通信 （207 ページ）
トポロジの例 （207 ページ）

トポロジの例

このケース スタディでは、次の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2つの Unified Communications Manager があります。また、Cisco IOS ゲートウェイと Cisco IOS ゲートキーパー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 Unified IP Phone にコールを発信します。クラスタ間 Unified Communications Manager 通信は、H.323 バージョン 2 プロトコルを使用して実行されます。Cisco IOS ゲートキーパーもアドミッション制御に使用されます。

Cisco Unified IP Phone は Skinny Station プロトコルを使用して Unified Communications Manager に接続でき、Unified Communications Manager は H.323 RAS（登録、許可、状態）プロトコルを使用して Cisco IOS ゲートキーパーに接続できます。アドミッション要求（ARQ）メッセージが Cisco IOS ゲートキーパーに送信され、ゲートキーパーはクラスタ間コールが H.323 バージョン 2 プロトコルを使用して発信できることを確認したあと、アドミッション確認（ACF）メッセージを送信します。この処理後、RTP プロトコルを使用して、異なるクラスタ内の Cisco Unified IP Phone 間に音声パスが作成されます。

コール フローのトレース

ここでは、CCM000000000 ファイルにキャプチャされる 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 にある Cisco Unified IP Phone（2002）が Cluster 1 にある Cisco Unified IP Phone（1001）にコールを発信します。トレースでデバイスを追跡するには、デバイスの TCP ハンドル値、タイムスタンプ、または名前を調べます。デバイスの TCP ハンドル値は、デバイスがリブートされるかオフラインになるまで変わりません。

次のトレースでは、Cisco Unified IP Phone（2002）がオフフックになっています。トレースは、Cisco Unified IP Phone に表示される固有のメッセージ、TCP ハンドル、発信番号を示しています。次のデバッグ出力には、着信番号（1001）、H.225 接続、および H.245 確認メッセージが示されています。コーデック タイプは G.711 mu-law です。

```
16:06:13.921 CCM|StationInit - InboundStim - OffHookMessageID
tcpHandle=0x1c6431016:06:13.953 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アドレスと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。これらのトレースのあとに、接続解除メッセージ、オンフック メッセージが続きます。

```
RemoteRtpPortNumber: 29626 msecPacketSize: 20
compressionType:(4)Media_Payload_G711Ulaw64k16:06:16.515 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
```

失敗したコール フロー

次の項では、SDIトレースで示されているように、失敗したクラスタ間コールフローについて説明します。次のトレースでは、Cisco Unified IP Phone（1001）がオフフックになります。TCPハンドルがCisco Unified IP Phoneに割り当てられます。

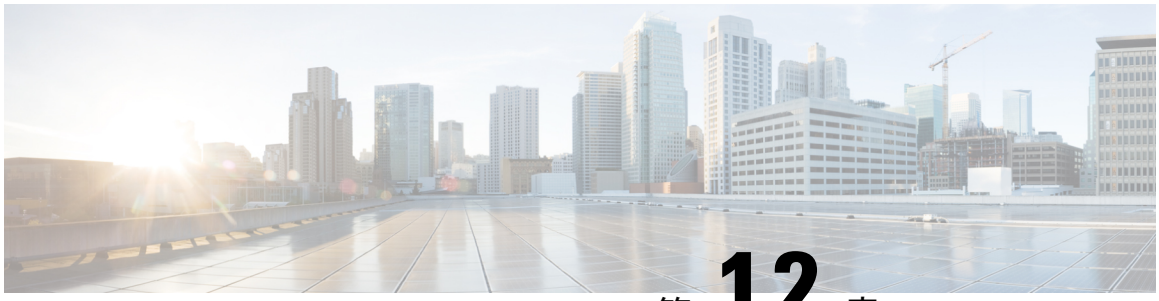
```
16:05:33.468 CCM|StationInit - InboundStim - OffHookMessageID
tcpHandle=0x4fbbc3016:05:33.468 CCM|StationD - stationOutputDisplayText
tcpHandle=0x4fbbc30, Display= 1001 16:05:33.484 CCM|StationD -
stationOutputSetLamp stim: 9=Line instance=1 lampMode=LampOn tcpHandle=0x4fbbc30
```

次のトレースでは、ユーザが着信側Cisco Unified IP Phoneの番号（2000）をダイヤルし、番号分析プロセスによって番号の一致が試行されています。

```
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")
```

これで番号分析は完了し、結果が次のトレースに表示されています。次の PotentialMatches=NoPotentialMatchesExist 参照は、Unified Communications Manager でこのディレクトリ番号との一致が見つからないことを示しています。最後に、リオーダー トーンが発呼側（1001）に送信され、オンフック メッセージが続きます。

```
16:05:36.812 CCM|Digit analysis: analysis results16:05:36.812
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
```



第 12 章

ケース スタディ：Cisco Unified IP Phone と Cisco IOS ゲートウェイ間のコールのトラブルシューティング

このケース スタディでは、ローカル PBX を経由して接続している電話機、または公衆電話交換網（PSTN）上の電話機に、Cisco IOS ゲートウェイを経由してコールを発信する Cisco Unified IP Phone について説明します。概念的には、コールが Cisco IOS ゲートウェイに到達すると、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いずれかに転送します。PBX に転送されたコールは、ローカル PBX に接続された電話機で終端するか、または PBX によって PSTN 経由で転送され、PSTN 上で終端します。

コール フローのトレース

ここでは、Cisco Communications Manager 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。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。詳細なトレース情報については、Cisco Unified IP Phone コールに関連するトピックを参照してください（たとえば、初期化、登録、およびキープアライブ メカニズムなど）。

このコール フローでは、Cluster 2 にある Cisco Unified IP Phone（電話番号 1001）が PSTN 上の電話機（電話番号 3333）にコールを発信します。トレースでデバイスを追跡するには、デバイスの TCP ハンドル値、タイムスタンプ、または名前を調べます。デバイスの TCP ハンドル値は、デバイスがリブートされるかオフラインになるまで変わりません。

次のトレースでは、Cisco Unified IP Phone（1001）がオフフックになっています。トレースは、Cisco Unified IP Phone に表示される固有のメッセージ、TCP ハンドル、発信番号を示していま

す。ユーザはまだ番号をダイヤルしていないため、この時点では着信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 つずつダイヤルします）。番号 3333 は、PSTN ネットワーク上の電話機の宛先番号です。現在アクティブな Unified Communications Manager の番号分析プロセスが番号を分析して、コールのルーティング先を検出します。番号分析の詳細については、Cisco Unified IP Phone コールに関連するトピックを参照してください。

```
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、情報が解析されています。

```
|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 が発信元のロケーションを示し、番号 1 が宛先のロケーションを示しています。BW = -1 は、発信元のロケーションの帯域幅を示します。値 -1 は、帯域幅が無限であることを暗黙的に示します。コールは LAN 環境にある Cisco Unified IP Phone から発信されたため、帯域幅は無限であると見なされます。BW = 64 は、宛先のロケーションの帯域幅を示します。コールの宛先は PSTN 上にある電話機で、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、発信側および着信側の情報を示しています。この例では、管理者が表示名（John Smith など）を設定していないため、発呼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、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、16 進表記の着信側の 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=
H225Protocol15:20:21.421 CCM|MMan_Id= 1. (iep= 0 dsl= 0 sapi= 0 ces= 0
IpAddr=e24610ac IpPort=47110)
```

次のトレースは、発信側および着信側の情報と H.225 アラート メッセージを示しています。また、Cisco Unified IP Phone の 16 進数値と IP アドレスのマッピングも示されています。Cisco Unified 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=0x5138d9815:20:21.453 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、このコールで使用されている圧縮タイプ（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.323 は H.225 アラート メッセージが送信されたあとで、H.245 を初期化します。次のトレースは、発信側および着信側の情報と 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同じで、同じコールが続い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 接続メッセージと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、コールが接続します。

```
15:20:22.968 CCM|In Message -- H225ConnectMsg -- Protocol=
H225Protocol15:20:22.968 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 Unified IP Phone（1001）からのオンフック メッセージを受信していることを示しています。オンフック メッセージを受信するとすぐに、H.225 と Skinny Station デバイスの接続解除メッセージが送信され、H.225 メッセージの全文が表示されます。この最後のメッセージには、コールが終端したことが示されています。

```
15:20:27.296 CCM|StationInit - InboundStim - OnHookMessageID
tcpHandle=0x5138d9815:20:27.296 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>
```

関連トピック

ケース スタディ：Cisco Unified IP Phone コールのトラブルシューティング （197 ページ）

Cisco IOS ゲートキーパーのデバッグ メッセージと表示コマンド

このケース スタディのトポロジでは、Cisco IOS ゲートキーパーで debug ras コマンドがオンになっています。SDI トレースの詳細については、コール フロー トレースに関するトピックを参照してください。

次のデバッグ メッセージは、Cisco IOS ゲートキーパーが Unified Communications Manager（172.16.70.228）に対するアドミッション要求（ARQ）を受信し、その他の正常なリモート アクセス サーバ（RAS）メッセージが後続していることを示しています。最後に、Cisco IOS ゲートキーパーがアドミッション確認（ACF）メッセージを Unified Communications Manager に送信しています。

```
*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 ゲートキーパーが Unified Communications Manager（172.16.70.228）から解除要求（DRQ）を受信し、Cisco IOS ゲートキーパーが解除確認（DCF）を Unified Communications Manager 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 ゲートキーパーで show gatekeeper endpoints コマンドを実行すると、4 つの Unified Communications Manager がすべて Cisco IOS ゲートキーパーに登録されていることが示されます。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、4 つの Unified Communications Manager があります。この Cisco IOS ゲートキーパーには 2 つのゾーンがあり、各ゾーンに 2 つの Unified Communications Manager 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
```

関連トピック

コール フローのトレース （211 ページ）

Cisco IOS ゲートウェイのデバッグ メッセージと表示コマンド

ここでは、Cisco IOS ゲートウェイのデバッグ出力と表示コマンドについて説明します。このケース スタディのトポロジでは、コールが Cisco IOS ゲートウェイを通過します。Cisco IOS ゲートウェイは T1/CAS または T1/PRI のいずれかのインターフェイスを使用して PSTN または PBX に接続します。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です。

次のデバッグ出力では、Cisco IOS ゲートウェイが Unified Communications Manager（172.16.70.228）からの TCP 接続要求を H.225 のポート 2328 で受け入れています。

```
*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、H.225 データが Unified Communications Manager から送信されていることを示しています。このデバッグ出力には、使用されている H.323 バージョンを表す protocolIdentifier が示されています。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。また、着信側と発呼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 は着信コールを示します。次の出力では、着信側および発呼側の情報も確認できます。CCAPi は、デフォルトのダイヤル ピアであるダイヤル ピア 0 に一致します。CCAPi がダイヤル ピア 0 に一致するのは、発信番号に対する他のダイヤル ピアが見つからず、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（着信番号 3333）を照合します。peer_tag はダイヤル ピアを意味します。要求パケット内の発信側と着信側の番号が示されています。

```
*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 Unified Communications Manager 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 Unified Communications Manager に送信しています。Cisco IOS ゲートウェイは到達不能なアドレスを送信する場合があるため、無音声または片通話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 セッションが開始され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、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、両方の側が適切にネゴシエートし、160 バイト データの 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後続します。

```
*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)
```

関連トピック

Cisco IOS ゲートキーパーのデバッグ メッセージと表示コマンド （215 ページ）

T1/PRI インターフェイスを使用する Cisco IOS ゲートウェイ

上記のように、2 つのタイプのコールが Cisco IOS ゲートウェイを通過します。Cisco IOS ゲートウェイは T1/CAS または T1/PRI のいずれかのインターフェイスを使用して PSTN または PBX

に接続します。次の例は、Cisco IOS ゲートウェイが T1/PRI インターフェイスを使用する場合のデバッグ出力です。

Cisco IOS ゲートウェイの debug isdn q931 コマンドがオンになり、それにより 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 がイネーブルになります。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、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 のデータ コールです。これが 0x8890218F だった場合は、56 Kbps のデータ コールになり、音声コールの場合は 0x8090A3 になります。次のデバッグ出力では、ベアラ機能は 0x8090A3 で、音声に適用されます。例には、着信側と発呼側の番号が示されています。

callref では、最初の数字に異なる値を使用し（TX と RX を識別するため）、2 番めの値は同じです（SETUP の最後の数字は 0、CONNECT_ACK も 0 です）。ルータはベアラ チャネル（B チャネル）を割り当てる際に PSTN または PBX に完全に依存します。PSTN または PBX がルータにチャネルを割り当てないと、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、交換機から受信される CONNECT メッセージに、ALERTING 用に受信されたものと同じ参照番号（0x800B）が含まれています。最後に、コールが接続解除されるとき、DISCONNECT メッセージの交換後に RELEASE メッセージと RELEASE _COMP メッセージが続くことを確認できます。RELEASE_COMP メッセージのあとには、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 ゲートウェイ

2 つのタイプのコールが Cisco IOS ゲートウェイを通過します。Cisco IOS ゲートウェイは T1/CAS または T1/PRI のいずれかのインターフェイスを使用して PSTN または PBX に接続します。次のデバッグ出力は、Cisco IOS ゲートウェイが T1/CAS インターフェイスを使用する場合に発生します。Cisco IOS ゲートウェイでは debug cas がオンになっています。

次のデバッグ メッセージは、Cisco IOS ゲートウェイ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 ゲートウェイから閉ループ信号を受信後、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 ゲートウェイ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、コールが進行中の Cisco IOS ゲートウェイでの show call active voice brief を示しています。出力には、着信側と発呼側の番号およびその他の役立つ情報も示されています。

```
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
```