目次

概要

このドキュメントでは、シスコのゲートウェイがかかわっている IP テレフォニーの片通話で発生する可能性のある、いくつかの一般的な問題について説明します。 このドキュメントで説明するシスコのゲートウェイは、Cisco IOS® ゲートウェイおよびルータ、Catalyst スイッチ、DT-24+ ゲートウェイです。

前提条件

要件

このドキュメントは、音声ネットワークに関する基本的な知識を持つ、IP テレフォニー ネットワ

ークに携わる担当者を対象としています。

使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

問題

このドキュメントは、次のような問題に対応し、そのシナリオとソリューションを提供しています。

- 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までの通話が確立されると、通話者のうち 1 人だけが音声を受信します（単方向通信）。
- 2 つのシスコのゲートウェイ間でトール バイパス コールが確立されると、通話者のうち 1 人だけが音声を受信します（単方向通信）。
- VPN 3002 ハードウェア クライアントの背後にある IP ステーションからの通話が確立されると、通話者のうち 1 人だけが音声を受信します（単方向通信）。

解決策

IP テレフォニーの片通話の原因はさまざまですが、根本的な問題は通常、IP ルーティングの問題に関係します。 このセクションでは、この領域で既知のシナリオとソリューションをいくつか取り上げます。

Cisco IOS ゲートウェイおよびルータで IP ルーティングがイネーブルになっていることを確認する

VG200 など、一部の Cisco IOS ゲートウェイは、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。 このデフォルト設定により、単方向音声の問題が生じます。

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

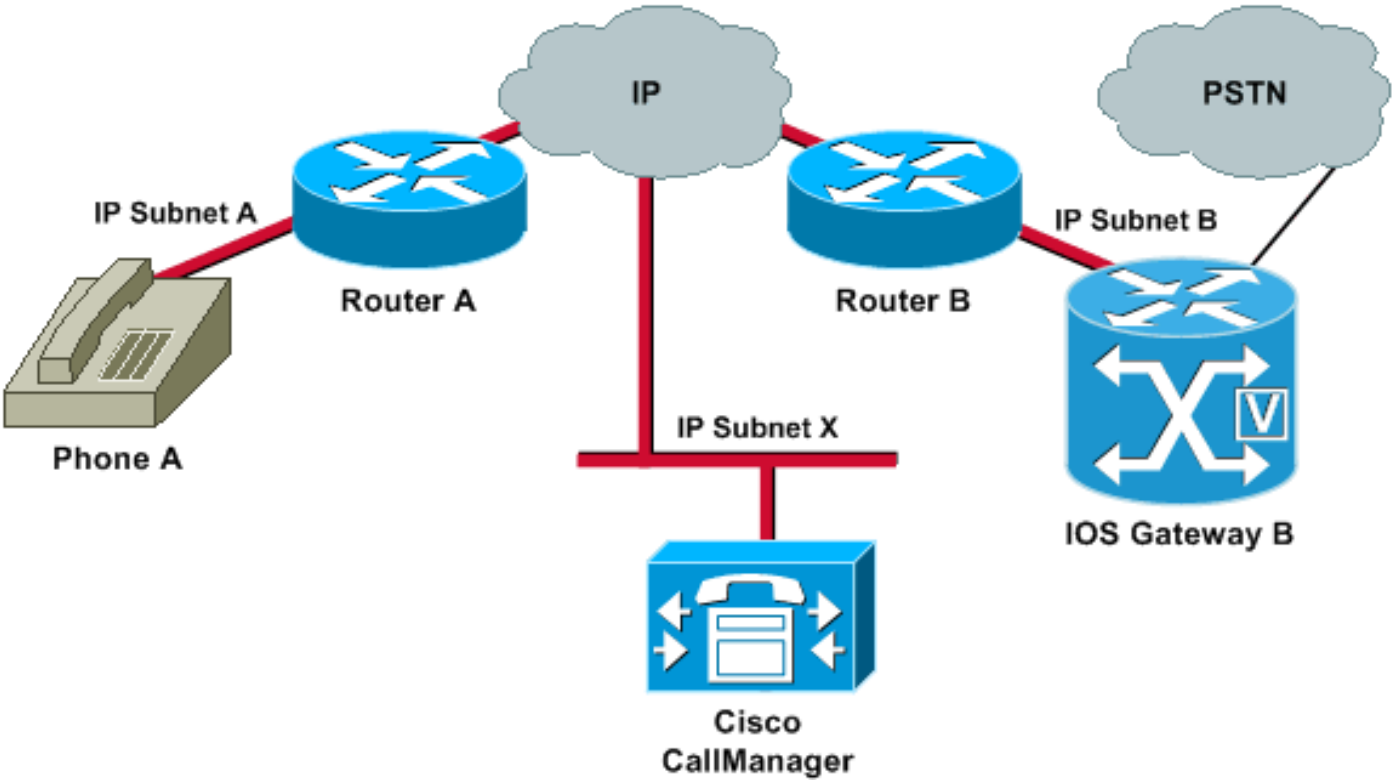
IP ルーティングをイネーブルにするには、Cisco IOS ゲートウェイ上でこのグローバル コンフィギュレーション コマンドを発行します。

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

基本的な IP 到達可能性の確認

最初に必ず、基本的な IP 到達可能性を確認します。 Real-Time Transport Protocol（RTP）ストリームはコネクションレス型（UDP 経由で転送される）であるため、一方向のトラフィックは正常に転送されますが、反対方向のトラフィックは*失われます*。 次の図に、これが発生するシナリ

オを示します。



サブネット A とサブネット B はどちらもサブネット X に到達可能です。サブネット X はサブネット A とサブネット B に到達可能です。 このため、端末（A および B）と Cisco CallManager との間で TCP 接続を確立できます。 したがって、シグナリングは問題なく両方の端末に到達でき、A と B 間のコールを確立できます。

コールが確立されたら、音声を伝送する RTP ストリームは、端末間を両方向に流れる必要があります。 サブネット B はサブネット A に到達可能ですが、サブネット A はサブネット B に到達できない場合があります。 このため、A から B への音声ストリームがいつも*失われます*。

これは、基本的なルーティングの問題です。 ゲートウェイ B から電話機 A への ping を正常に実行できる状態にするには、IP ルーティングのトラブルシューティング方法を使用します。ping は双方向の IP 到達性の検証手段であることを覚えておいてください。

このドキュメントでは、IP ルーティングのトラブルシューティングについては説明していません。 ただし、初期手順の一環として以降を確認してください。

- デフォルト ゲートウェイを端末で設定している。
- このデフォルト ゲートウェイ上の IP ルートが宛先ネットワークに到達している。

注このリストでは、各種 Cisco IP Phone 上でデフォルト ルータまたはゲートウェイの設定を確認する方法について説明します。

- Cisco IP Phone 7910?Press **設定は、6 つを**『Option』 を選択 し、Default Router フィールドが出て来るまで『Volume』 を押します。
- Cisco IP Phone 7960/40?Press **設定は、3 つを**『Option』 を選択 し、Default Router フィールドが出て来るまでスクロールします。
- Cisco IP Phone 2sp+/30vip?Press は**** `gtwy=` 現われるまで**#**、それから**#**押し。

注Cisco IP SoftPhone アプリケーションを使用していて、その本体に 2 つ以上の Network Interface Card（NIC; ネットワーク インターフェイス カード）が取り付けられている場合は、本体からの送信元が正しい NIC になっていることを確認します。 この問題は、IP SoftPhone ソフ

トウェア バージョン 1.1.x に共通して存在します。 この問題は、バージョン 1.2 で解決されています。

注Cisco DT-24+ ゲートウェイを使用する場合、DHCP スコープを確認し、そのスコープ内にデフォルト ゲートウェイ (003 ルータ) オプションがあることを確認します。 003 ルータ パラメータは、デバイスおよび PC のデフォルト ゲートウェイ フィールドに取り込まれます。 スコープ オプション 3 では、ゲートウェイにルートするルータ インターフェイスの IP アドレスを使用する必要があります。

正しいメディア ターミネーション ポイント設定の確認

Intercluster Trunk (ICT) 用にトランスコーディングを設定する場合、Media Termination Point (MTP; メディア ターミネーション ポイント) が、トランクに関連付けられたメディア リソース グループおよびメディア リソース グループ リストに設定されていることを確認します。 MTP が不要な場合に MTP を指定したり、必要であっても MTP の設定に失敗したりすると、ICT 設定のために単方向音声の問題を引き起こすことがわかっています。

Cisco IOS ゲートウェイおよびルータでの特定の 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な 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分が 1 つの IP アドレスを送信元とし、他の部分が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、さまざまな問題が生じます。 このような問題の 1 つに片通話の問題があります。

この問題を回避するために、H.323 シグナリングを特定の送信元アドレスにバインドできます。 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 (ループバック) のものを使用できます。 インターフェイス コンフィギュレーション モードで **h323-gateway voip bind srcaddr ip-address コマンド**を使用します。 Cisco CallManager が参照先とする 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 ソフトウェア リリース 12.1(2)T で導入されました。 詳細については、『仮想インターフェイスの H.323 のサポート』を参照してください。

注意： Cisco IOS ソフトウェア リリース 12.2(6) には不具合があり、このリリースでは、このソリューションによって片通話の問題の実際の*原因*になることがあります。 詳細については、Cisco Bug ID CSCdw69681 (登録ユーザ専用) を参照してください。

Cisco IOS ゲートウェイでの MGCP メディア パケット送信元インターフェイスへの MGCP シグナリングのバインド

シグナリングおよびメディア パケット用の送信元インターフェイスを指定しないと、Media Gateway Control Protocol (MGCP; メディア ゲートウェイ コントロール プロトコル) ゲートウェイで単方向音声が発生することがあります。 mgcp bind media source-interface interface-id コマンドの発行後、mgcp bind control source-interface interface-id コマンドを発行すると、MGCP メディアを送信元インターフェイスにバインドできます。 コマンドを発行した後、Cisco CallManager で MGCP ゲートウェイをリセットします。

mgcp bind コマンドが有効になっていない場合でも、IP レイヤは最適なローカル アドレスを提供します。

mgcp bind コマンドのガイドラインは次のとおりです。

- ゲートウェイにアクティブな MGCP コールがある場合、制御およびメディアに対する **mgcp bind** コマンドは拒否されます。
- バインド インターフェイスがアップ状態ではない場合、コマンドを受け入れますが、インターフェイスがアップ状態になるまでは有効になりません。
- バインド インターフェイスで IP アドレスが割り当てられていない場合、**mgcp bind** コマンドを受け入れますが、コマンドが有効になるのは、有効な IP アドレスが割り当てられた後に限られます。 この間、MGCP コールがアップ状態である場合は、**mgcp bind** コマンドは拒否されます。
- インターフェイスの手動シャットダウンまたは操作上の失敗が原因で、バインドされたインターフェイスがダウン状態になると、そのインターフェイスでのバインド動作はディセーブルになります。
- Media Gateway Controller（MGC; メディア ゲートウェイ コントローラ）でバインドが設定されていない場合、MGCP 制御およびメディアの送信元として使用される IP アドレスが、最適に使用可能な IP アドレスです。

Telco またはスイッチが応答監視を正しく送受信することを確認する

Telco またはスイッチに接続する Cisco IOS ゲートウェイがある場合、Telco またはスイッチの背後にある着信側デバイスがコールに応答するときに応答監視が正しく送信されることを確認します。 応答監視の受信に失敗すると、Cisco IOS ゲートウェイが順方向の音声パスのカットスルー（オープン）に失敗します。 この失敗により、単方向音声が発生します。 回避策は、**voice rtp send-recv on** コマンドを発行することです。

詳細については、『Cisco IOS ゲートウェイおよびルータで voice rtp send-recv コマンドを使用した双方向音声の早期カットスルー』を参照してください。

Cisco IOS ゲートウェイおよびルータで voice rtp send-recv コマンドを使用した双方向音声の早期カットスルー

RTP ストリームの開始時、逆方向の音声パスが確立されます。 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、順方向の音声パスは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らすぐに双方向音声パスの確立が必要なことがあり、この場合は、Connect メッセージを受信する前になります。 このためには、voice rtp send-recv グローバル コンフィギュレーション コマンドを発行します。

Cisco IOS ゲートウェイおよびルータでのリンクごとの cRTP 設定の確認

この問題は、2 つ以上の Cisco IOS ルータまたはゲートウェイが音声パスにかかわっていて、compressed RTP（cRTP; 圧縮 RTP）が使用されている、トール バイパスなどのシナリオに適用されます。 cRTP、つまり、RTP ヘッダー圧縮は、帯域幅を取り戻すために、VoIP パケット ヘッダーを小さくする方法です。 cRTP は、VoIP パケット上で 40 バイトの IP、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）、または RTP ヘッダーを、パケットごとに 2 ~ 4 バイトに圧縮します。 この圧縮により、cRTP を使用する G.729 エンコードされたコールの場合、約 12 kbps の帯域幅が空きます。 cRTP の詳細は、『VoIP：コール単位の帯域幅の使用量』を参照してください。

cRTP は、ホップごとに圧縮解除と再圧縮を行って、ホップ単位に実行されます。 ルーティングするために、各パケット ヘッダーを調べる必要があります。 したがって、cRTP は IP リンクの両側でイネーブルにする必要があります。

また、cRTP がリンクの両端で意図したとおりに動作していることを確認することも重要です。 Cisco IOS ソフトウェア リリースのレベルによっては、スイッチング パスおよび cRTP の同時サポートの点が異なります。

要約すると、次のような経過をたどっています。

- Cisco IOS ソフトウェア リリース 12.0(5)T よりも前の Cisco IOS ソフトウェア リリースでは、cRTP はプロセス スイッチングされます。
- Cisco IOS ソフトウェア リリース 12.0(7)T および Cisco IOS ソフトウェア リリース 12.1(1)T では、cRTP のファースト スイッチングおよび Cisco Express Forwarding（CEF）スイッチングのサポートが導入されました。
- Cisco IOS ソフトウェア リリース 12.1(2)T で、アルゴリズムによってパフォーマンスが改善されました。

Cisco IOS ソフトウェアのプラットフォーム（Cisco IOS ソフトウェア リリース 12.1）で cRTP を実行する場合は、Cisco Bug ID CSCds08210（登録ユーザ専用）が、使用している Cisco IOS ソフトウェア リリースに影響がないことを確認します。 この不具合の症状は、RTP ヘッダー圧縮を使用して動作する VoIP および Fax Over IP が失敗します。

Cisco IOS ゲートウェイでのクロッキング設定の確認

E1 インターフェイスまたは T1 インターフェイス上で **show controller {e1 | t1}** コマンドによってクロック スリップが生じている場合は、音声ゲートウェイ上のクロッキング設定に矛盾がある可能性があります。 『IOS ベースの音声対応プラットフォームでのクロッキング設定』を参照し、音声ゲートウェイ上のクロッキング設定が正しいことを確認してください。

Cisco IOS ゲートウェイおよびルータでの NAT のための最小ソフトウェア レベルの確認

Network Address Translation（NAT; ネットワーク アドレス変換）を使用する場合は、ソフトウェア レベルの最小要件を満たす必要があります。 以前のバージョンの NAT では Skinny プロトコル変換がサポートされていません。 このような以前のバージョンでは、単方向音声の問題が発生します。

NAT を使用して Skinny および H.323 バージョン 2 を同時にサポートするには、Cisco IOS ゲートウェイに Cisco IOS ソフトウェア リリース 12.1(5)T 以降を稼働させる必要があります。 詳細については、『Cisco CallManager に接続する IP Phone における NAT のサポート』を参照してください。

注Cisco CallManager で Skinny シグナリングにデフォルト ポート（2000）以外の TCP ポートを使用する場合は、NAT ルータを調整する必要があります。 **ip nat service skinny tcp port number** グローバル コンフィギュレーション コマンドを発行します。

PIX Firewall 上で 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 6.0 です。 詳細については、『Cisco PIX Firewall バージョン 6.0』を参照してください。

注完全なゲートキーパーのサポートに必要なすべての Registration, Admission, and Status（RAS）メッセージに、これらのレベルのソフトウェアが必ず対応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については、この文章の適用範囲外です。

AS5350 および AS5400 での voice-fastpath の無効化

Cisco IOS ソフトウェアのコマンド **voice-fastpath enable** は、AS5350 および AS5400 の隠しグローバル コンフィギュレーション コマンドです。 このコマンドはデフォルトでイネーブルになっています。 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 コマンドを発行します。

コマンドがイネーブルになっている場合、特定のコールに対してオープンになっている論理チャネルの IP アドレスと UDP ポート番号の情報をキャッシュします。 このコマンドにより、RTP ストリームがアプリケーション層に到達しないようになります。 代わりに、パケットは下位の層で転送されます。 これによって、コールの量が多いシナリオでは、CPU 使用率を多少減少させることができます。

保留や転送などの補足サービスを使用する場合は、**voice-fastpath** コマンドにより、ルータがキャッシュされた IP アドレスおよび UDP ポートに音声を流すようになります。 保留中のコールが再開された後、または転送が完了した後に生成される新しい論理チャネル情報は無視されます。 この問題を回避するには、トラフィックが絶えずアプリケーション層に到達する必要があります。 この結果、論理チャネルの再定義がアカウントに取り込まれ、新しい IP アドレスと UDP ポートのペアに音声が流れるようになります。 したがって、補足サービスをサポートするには、**voice-fastpath** をディセーブルにしてください。

SoftPhone での VPN IP アドレスの設定

Cisco IP SoftPhone を使用すると、PC を Cisco IP Phone 7900 シリーズの電話のように動作させることができます。 Virtual Private Network (VPN; バーチャル プライベート ネットワーク) を経由して企業ネットワークに接続するリモート ユーザは、単方向音声の問題を回避するために追加の設定をいくつか行う必要があります。 これは、メディア ストリームが接続のエンド ポイントを識別する必要があるためです。

このソリューションは、ネットワーク音声設定で、ネットワーク アダプタの IP アドレスではなく、VPN の IP アドレスを設定することです。 詳細は、『VPN 経由での Cisco IP SoftPhone の使用方法』を参照してください。

Network Extension Mode で動作させる VPN 3002 の設定

Cisco VPN 3002 ハードウェア クライアントは、2 つのモードで動作可能です。 クライアント モードと Network Extension Mode (NEM) です。 クライアント モードでは、Cisco VPN 3002 クライアントの背後にあるすべてのホストは、VPN 3002 クライアントの外部 IP アドレスにポート アドレス変換されます。 H.323 は、Port Address Translation (PAT; ポート アドレス変換) を使用して動作しないため、IP Phone が VPN 3002 クライアントの背後にある場合は片通話になります。 VPN 3002 が NEM で動作する場合、リモート ネットワークは、NAT ベースや PAT ベースの IP アドレスではなく、実際の IP アドレスを使用して相互に認識し合います。 VPN 3002 が NEM で動作するように設定されている場合は、H.323 は動作可能です。 つまり、VPN 3002 クライアントの背後にある IP Phone は、VPN 3002 が NEM で動作する場合だけ動作可能です。 このため、VPN 3002 クライアントでの単方向音声を回避するには、NEM を使用するように VPN 3002 クライアントを設定します。

NEM を使用するように Cisco VPN 3002 Hardware Client を設定するには、[Configuration] > [Quick] > [PAT] を選択し、[PAT] ウィンドウで [No, use Network Extension mode] をクリックし

ます。

詳細は、『[Network Extension Mode で EzVPN を使用した Cisco IOS ルータへの Cisco VPN 3002 Hardware Client の設定]』を参照してください。

関連情報 片通話の確認

パケット フローの確認に使用する便利な 2 つのコマンドに、**debug cch323 rtp** コマンドと **debug voip rtp** コマンドがあります。 **debug cch323 rtp** コマンドは、ルータが送信（X）および受信（R）したパケットを表示します。 大文字は、送信または受信の成功を示します。 小文字はドロップされたパケットを示します。

```
voice-ios-gwy#debug cch323 rtpRTP packet tracing is enabledvoice-ios-gwy#voice-ios-gwy#voice-
ios-gwy#voice-ios-gwy#voice-ios-gwy#!--- This is an unanswered outgoing call. !--- Notice that
the voice path only cuts through in the forward direction and !--- that packets are dropped.
Indeed, received packets are traffic from the !--- IP phone to the PSTN phone. These are dropped
until the call is answered. Mar 3 23:46:23.690: ****** cut through in FORWARD direction
*****XXXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrX
rXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXXrrrrrrrrrrrrrrrrv
oice-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
*****XXXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrX
rXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXXrrrrrXrXrXrXrXrXrXr
XrXrXrXrrXXrrXrXrXrXrXrXXXXXXXXXXXXXXXXXrXXXXXXXXrXrXrXXrrXrXrXrXrXrXrXrXrXrXXrrrrrrrrrrrrrrrrrr
rrrrrrrrrrr!--- At this point, the remote end picks up the phone.*Mar 3 23:53:30.378: ****** cut
through in BOTH direction
*****XRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXRXRXRXRXRX
RXRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXXRRXRXRXXRRXRXRXRXRXXR
XRXRXRXRXRRXRXXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRRRRRRRR
RRRRRRRRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRR
RRRRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRXXRXRXRXRXRXRXRRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRRRRRRXRXRX
RXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRX
RXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRXR!--- This is
the end of the conversation.
```

注Cisco IOS ソフトウェア リリース 12.2(11)T 以降では、**debug cch323 rtp** コマンドライン インターフェイス（CLI）コマンドが **debug voip rtp** コマンドに代わっています。

```
voice-ios-gwy#debug voip rtp--------cut through in BOTH direction-------------------*Mar 27
19:52:08.259: RTP(32886): fs rx d=10.48.79.181(20002),pt=0, ts=4FFBF0, ssrc=8E5FC294*Mar 27
19:52:08.275: RTP(247): fs tx d=10.48.79.181(20002),pt=0, ts=5D00C8D9, ssrc=1F1E5093*Mar 27
19:52:08.279: RTP(32887): fs rx d=10.48.79.181(20002),pt=0, ts=4FFC90, ssrc=8E5FC294*Mar 27
19:52:08.295: RTP(248): fs tx d=10.48.79.181(20002),pt=0, ts=5D00C979, ssrc=1F1E5093*Mar 27
19:52:08.299: RTP(32888): fs rx d=10.48.79.181(20002),pt=0, ts=4FFD30, ssrc=8E5FC294*Mar 27
19:52:08.315: RTP(249): fs tx d=10.48.79.181(20002),pt=0, ts=5D00CA19, ssrc=1F1E5093*Mar 27
19:52:08.319: RTP(32889): fs rx d=10.48.79.181(20002),pt=0, ts=4FFDD0, ssrc=8E5FC294*Mar 27
19:52:08.335: RTP(250): fs tx d=10.48.79.181(20002),pt=0, ts=5D00CAB9, ssrc=1F1E5093*Mar 27
19:52:08.339: RTP(32890): fs rx d=10.48.79.181(20002),pt=0, ts=4FFE70, ssrc=8E5FC294*Mar 27
19:52:08.355: RTP(251): fs tx d=10.48.79.181(20002),pt=0, ts=5D00CB59, ssrc=1F1E5093*Mar 27
19:52:08.359: RTP(32891): fs rx d=10.48.79.181(20002),pt=0, ts=4FFF10, ssrc=8E5FC294*Mar 27
19:52:08.375: RTP(252): fs tx d=10.48.79.181(20002),pt=0, ts=5D00CBF9, ssrc=1F1E5093*Mar 27
19:52:08.379: RTP(32892): fs rx d=10.48.79.181(20002),pt=0, ts=4FFFB0, ssrc=8E5FC294*Mar 27
19:52:08.395: RTP(253): fs tx d=10.48.79.181(20002),pt=0, ts=5D00CC99, ssrc=1F1E5093*Mar 27
19:52:08.399: RTP(32893): fs rx d=10.48.79.181(20002),pt=0, ts=500050, ssrc=8E5FC294*Mar 27
19:52:08.976: RTP(282): fs tx d=10.48.79.181(20002),pt=0, ts=5D00DEB9, ssrc=1F1E5093*Mar 27
19:52:08.980: RTP(32922): fs rx d=10.48.79.181(20002),pt=0, ts=501270, ssrc=8E5FC294*Mar 27
19:52:08.996: RTP(283): fs tx d=10.48.79.181(20002),pt=0, ts=5D00DF59, ssrc=1F1E5093*Mar 27
19:52:09.000: RTP(32923): fs rx d=10.48.79.181(20002),pt=0, ts=501310, ssrc=8E5FC294*Mar 27
19:52:09.016: RTP(284): fs tx d=10.48.79.181(20002),pt=0, ts=5D00DFF9, ssrc=1F1E5093
```

PIX Firewall を介するコール トラフィック情報の収集

PIX Firewall を通過するコール トラフィック情報を集めることで、単方向コールのトラブルシューティングを行うことができます。 PIX の capture コマンドを使用して、コール発生時にオープンして使用されたポートを確認できます。 PIX Firewall を通過する VoIP トラフィックについては、『PIX ファイアウォールでの VoIP トラフィックの処理』を参照してください。

注トラブルシューティングを行うために必要なキャプチャ ファイルを生成した後は、必ず **capture** コマンドを無効にしてください。

Cisco Unified Communications Manager の片通話の問題

この問題は、MTP が必要な発信初期 SIP コール セットアップでのみ発生します。 この場合は、発信 SIP INVITE メッセージに SDP オファーが追加されます。 この問題は、次のようなシナリオで発生する可能性があります。

- SIP トランクで [Media Termination Point Required] がオンになっている発信 SIP トランク コール
- IPv6 専用エンドポイントと IPv4 専用エンドポイント間のコール

解決策

MTP リソースの断続的な漏洩が、MTP リソースが必要な SIP コールの失敗につながっている可能性があります。 RTMT から使用可能な MTP リソース数が 0 に達し、MTP が必要なコールごとに MTP 割り当て失敗回数が増加します。 初期 INVITE の SDP 部分に不正な **a=inactive** が追加されます。

この問題を解決するには、次の手順を実行します。

1. 可能な場合は、SIP トランク設定の [Media Termination Point Required] をオフにします。
2. アーリー オファーが必要な場合は、アーリー オファーを設定しますが、[Media Termination Point Required] はオフのままにします。
3. IPv6 導入では、IPv6 専用エンドポイント以外のデュアル スタックを使用します。

注この問題は、Cisco Bug ID CSCtk77040（登録ユーザ専用）で文書化されています。

関連情報

- CallManager H.323： 転送後または保留後に音声が単方向しか通じない問題
- IP Phone から Cisco CallManager への NAT サポート
- 仮想インターフェイスの H.323 のサポート
- EzVPN 機能を備えた Cisco IOS ルータに接続する Cisco VPN 3002 ハードウェア クライアントの Network Extension モードでの設定
- Cisco CallManager を使用する Cisco Unity： 片通話
- Cisco Unity 用二重 NIC の設定およびトラブルシューティング
- 音声に関する技術サポート
- 音声とユニファイド コミュニケーションに関する製品サポート
- Cisco IP Telephony のトラブルシューティング
- テクニカルサポートとドキュメント - Cisco Systems