Troubleshooting One Way Voice Issues

Document ID: 5219

Contents

Introduction

This document addresses some of the common issues that can occur in IP Telephony one−way audio conversations that involve Cisco gateways. The Cisco gateways that this document covers are Cisco IOS® gateways and routers, Catalyst switches, and DT−24+ gateways.

Prerequisites

Requirements

This document is intended for personnel who are involved with IP Telephony networks and have basic knowledge of voice networks.

Components Used

This document is not restricted to specific software or hardware versions.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Problem

This document provides scenarios and solutions to these problems:

- When a phone call is established from an IP station through a Cisco IOS voice gateway or router, only one of the parties receives audio (one−way communication).
- When a toll−bypass call is established between two Cisco gateways, only one of the parties receives audio (one−way communication).
- When a phone call is established from an IP station that is placed behind a VPN 3002 Hardware Client, only one of the parties receives audio (one−way communication).

Solutions

The causes of one−way audio in IP Telephony can be varied, but the root of the problem usually involves IP routing issues. This section takes a look at some of the scenarios and solutions that have been found in the field.

Ensure That IP Routing Is Enabled on the Cisco IOS Gateway and Routers

Some Cisco IOS gateways, such as the VG200, disable IP routing by default. This default setting leads to one−way voice problems.

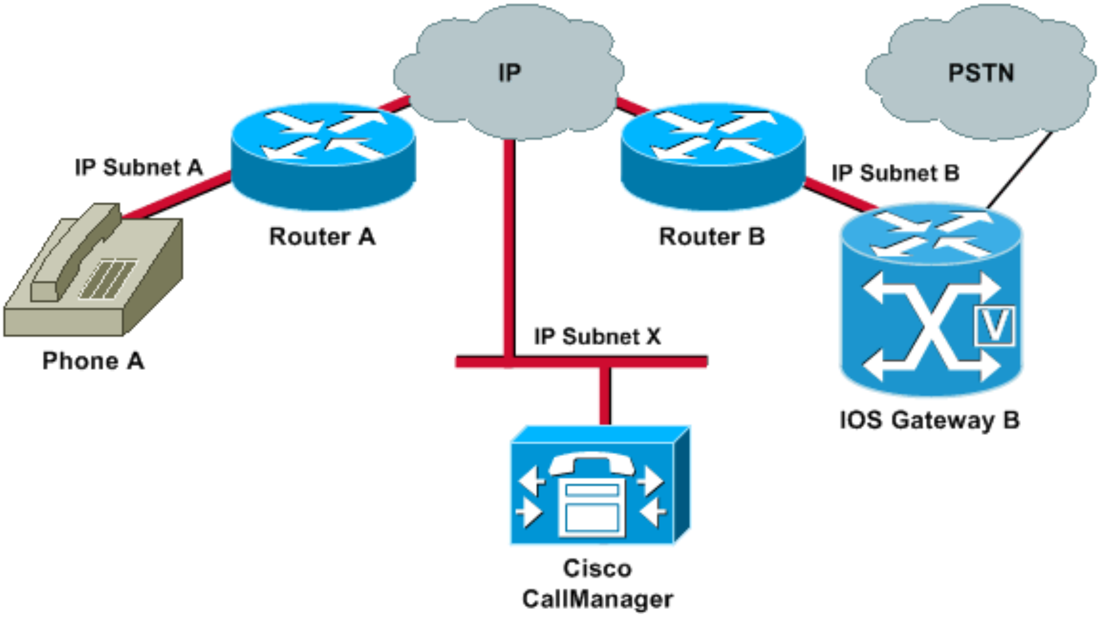
Note: Before you go any further, ensure that IP routing is enabled on your router. In other words, ensure that your router does not have the **no ip routing** global configuration command.

In order to enable IP routing, issue this global configuration command on your Cisco IOS gateway:

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

Check Basic IP Reachability

Always check basic IP reachability first. Because Real−Time Transport Protocol (RTP) streams are connectionless (transported over UDP), traffic may travel successfully in one direction but get *lost* in the opposite direction. This diagram shows a scenario in which this can happen:



Subnets A and B can both reach Subnet X. Subnet X can reach Subnets A and B. This allows the establishment of TCP connections between the end stations (A and B) and the Cisco CallManager. Therefore, signaling can reach both end stations without any problems, which allows the establishment of calls between A and B.

Once a call is established, an RTP stream that carries the audio must flow in both directions between the end stations. In some cases, Subnet B can reach Subnet A, but Subnet A cannot reach Subnet B. Therefore, the audio stream from A to B always gets *lost*.

This is a basic routing issue. Use IP routing troubleshooting methods in order to get to the stage at which you can successfully ping Phone A from Gateway B. Remember that ping is a bidirectional verification.

This document does not cover IP routing troubleshooting. However, confirm these as some initial steps to follow:

- Default gateways are configured at the end stations.
- IP routes on those default gateways lead to the destination networks.

Note: This list explains how to verify the default router or gateway configuration on various Cisco IP phones:

- Cisco IP Phone 7910 Press **Settings**, select option **6**, and press volume down until the Default Router field shows up.
- Cisco IP Phone 7960/40 Press **Settings**, select option **3**, and scroll down until the Default Router field shows up.
- Cisco IP Phone 2sp+/30vip Press ****#**, and then press **#** until `gtwy=` appears.

Note: When you use the Cisco IP SoftPhone application and more than one network interface card (NIC) is installed in the box, ensure that the box sources the correct NIC. This issue is commonly present in IP SoftPhone software version 1.1.x. Version 1.2 should resolve this issue.

Note: When you use Cisco DT−24+ Gateways, check the DHCP Scope and ensure that there is a Default Gateway (003 router) option in the scope. The 003 router parameter populates the Default Gateway field in the devices and PCs. Scope option 3 should have the IP address of the router interface that will route for the gateway.

Verify Correct Media Termination Point Configuration

If transcoding is configured for an intercluster trunk (ICT), ensure that a Media Termination Point (MTP) is configured in the Media Resource Group and Media Resource Group List associated with the trunk. If you specify an MTP when one is not needed, or fail to configure an MTP if it is needed, it has been known to cause one way voice issues for ICT configurations.

Bind the H.323 Signaling to a Specific IP Address on the Cisco IOS Gateway and Routers

When the Cisco IOS gateway has multiple active IP interfaces, some of the H.323 signaling may be sourced from one IP address and other parts of it may reference a different source address. This can generate various kinds of problems. One such problem is one−way audio.

In order to get around this problem, you can bind the H.323 signaling to a specific source address. The source address can belong to a physical or virtual interface (loopback). Use the **h323−gateway voip bind srcaddr** *ip−address* command in interface configuration mode. Configure this command under the interface with the IP address to which the Cisco CallManager points.

This command was introduced in Cisco IOS Software Release 12.1(2)T. Refer to H.323 Support for Virtual Interfaces.

Caution: A bug exists in Cisco IOS Software Release 12.2(6) in which this solution can actually *cause* a one−way audio problem. For more information, refer to Cisco bug ID CSCdw69681 (registered customers only) .

Bind the MGCP Signaling to the MGCP Media Packet Source Interface on the Cisco IOS Gateway

One−way voice can occur in Media Gateway Control Protocol (MGCP) gateways if the source interface for signaling and media packets is not specified. You can bind the MGCP media to the source interface if you issue the **mgcp bind media source−interface** *interface−id* command and then the **mgcp bind control source−interface** *interface−id* command. Reset the MGCP gateway in Cisco CallManager after you issue the commands.

If the **mgcp bind** command is not enabled, the IP layer still provides the best local address.

The guidelines for the **mgcp bind** command are:

- When there are active MGCP calls on the gateway, the **mgcp bind** command is rejected for both control and media.
- If the bind interface is not up, the command is accepted but does not take effect until the interface comes up.
- If the IP address is not assigned on the bind interface, the **mgcp bind** command is accepted but takes effect only after a valid IP address is assigned. During this time, if MGCP calls are up, the **mgcp bind** command is rejected.
- When the bound interface goes down, either because of a manual shutdown on the interface or because of operational failure, the bind activity is disabled on that interface.
- When bind is not configured on the Media Gateway Controller (MGC), the IP address that is used to source MGCP control and media is the best available IP address.

Check That the Telco or Switch Correctly Sends and Receives Answer Supervision

If you have a Cisco IOS gateway that connects to a Telco or switch, verify that answer supervision is sent correctly when the called device behind the Telco or switch answers the call. Failure to receive the answer supervision causes the Cisco IOS gateway to fail to cut through (open) the audio path in a forward direction. This failure causes one−way voice. A workaround is to issue the **voice rtp send−recv on** command.

For more information, see Cut Through Two−Way Audio Early with the voice rtp send−recv Command on the Cisco IOS Gateway and Routers.

Cut Through Two−Way Audio Early with the voice rtp send−recv Command on the Cisco IOS Gateway and Routers

The voice path is established in the backward direction at the start of the RTP stream. The forward audio path is not cut through until the Cisco IOS gateway receives a Connect message from the remote end.

In some cases, it is necessary to establish a two−way audio path as soon as the RTP channel is opened, which is before the Connect message is received. In order to achieve this, issue the **voice rtp send−recv** global configuration command.

Check cRTP Settings on a Link−by−Link Basis on Cisco IOS Gateway and Routers

This issue applies to scenarios, such as toll−bypass, in which more than one Cisco IOS router or gateway is involved in the voice path and compressed RTP (cRTP) is used. cRTP, or RTP Header Compression, is a method to make the VoIP packet headers smaller in order to regain bandwidth. cRTP takes the 40−byte IP, User Datagram Protocol (UDP), or RTP header on a VoIP packet and compresses it to 2 to 4 bytes per packet. This compression yields approximately 12 kbps of bandwidth for a G.729 encoded call with cRTP. For more information on cRTP, refer to Voice Over IP − Per Call Bandwidth Consumption.

cRTP is done on a hop−by−hop basis, with decompression and recompression on every hop. Each packet header must be examined for routing. Therefore, cRTP needs to be enabled on both sides of an IP link.

It is also important to verify that cRTP is working as expected on both ends of the link. Cisco IOS Software release levels vary in terms of switching paths and concurrent cRTP support.

In summary, the history is:

- In Cisco IOS Software releases earlier than Cisco IOS Software Release 12.0(5)T, cRTP is process−switched.
- In Cisco IOS Software Release 12.0(7)T, and in Cisco IOS Software Release 12.1(1)T, fast− and Cisco Express Forwarding (CEF)−switching support for cRTP is introduced.
- In Cisco IOS Software Release 12.1(2)T, algorithmic performance improvements are introduced.

If you run cRTP on Cisco IOS Software platforms (Cisco IOS Software Release 12.1), verify that Cisco bug ID CSCds08210 (registered customers only) does not affect your Cisco IOS Software release. The symptom of this bug is the failure of VoIP and fax over IP to work with the RTP header compression on.

Verify the Clocking Configurations on the Cisco IOS Gateway

If you find that there are clock slips on the E1 or T1 interface from the **show controller {e1 | t1}** command, there might be some mismatch in the clocking configuration on the Voice Gateway. Refer to Clocking Configurations On Voice−Capable IOS−Based Platforms and make sure that the clocking configurations on the Voice Gateway are correct.

Verify Minimum Software Level for NAT on the Cisco IOS Gateway and Routers

If you use Network Address Translation (NAT), you must meet the minimum software−level requirements. Earlier versions of NAT do not support skinny protocol translation. These earlier versions lead to one−way voice issues.

You must run Cisco IOS Software Release 12.1(5)T or later for Cisco IOS gateways to support skinny and H.323 version 2 with NAT simultaneously. For more information, refer to NAT−Support of IP Phone to Cisco CallManager.

Note: If your Cisco CallManager uses a TCP port for skinny signaling that is different than the default port (2000), you must adjust the NAT router. Issue the **ip nat service skinny tcp port** *number* global configuration command.

The minimum software level that is required in order to use NAT and skinny simultaneously on a PIX firewall is 6.0. For more information, refer to Cisco PIX Firewall Version 6.0.

Note: These levels of software do not necessarily support all the Registration, Admission, and Status (RAS) messages that are necessary for full gatekeeper support. Gatekeeper support is outside the scope of this document.

Disable voice−fastpath on AS5350 and AS5400

The Cisco IOS Software command **voice−fastpath enable** is a hidden global configuration command for the AS5350 and AS5400. The command is enabled by default. In order to disable it, issue the **no voice−fastpath enable** global configuration command.

When the command is enabled, it caches the IP address and UDP port number information for the logical channel that is opened for a specific call. The command prevents the RTP stream from reaching the application layer. Instead, the packets are forwarded at a lower layer. This helps to reduce CPU utilization marginally, in high call volume scenarios.

When supplementary services such as hold or transfer are used, the **voice−fastpath** command causes the router to stream the audio to the cached IP address and UDP port. The new logical channel information that is generated after a call on hold is resumed or after a transfer is completed is disregarded. In order to get around this problem, traffic must go to the application layer constantly so that redefinition of the logical channel is taken into account and audio is streamed to the new IP address and UDP port pair. Therefore, be sure to disable **voice−fastpath** in order to support supplementary services.

Configure the VPN IP Address with SoftPhone

Cisco IP SoftPhone allows a PC to work like a Cisco IP Phone 7900 Series phone. Remote users who connect back to their company network through a Virtual Private Network (VPN) must configure some additional settings in order to avoid a one−way voice problem. This is because the media stream needs to know the endpoint of the connection.

The solution is to configure the VPN IP address, instead of the IP address of the network adapter, under the Network Audio Settings. For more information, refer to How to Use Cisco IP SoftPhone over VPN.

Configure VPN 3002 to Work in Network Extension Mode

A Cisco VPN 3002 Hardware Client can operate in two modes: client mode and network extension mode (NEM). In client mode, all the hosts behind the Cisco VPN 3002 client are port address translated to the outside IP address of the VPN 3002 client. H.323 does not work with port address translation (PAT) and results in one−way audio when an IP phone is placed behind a VPN 3002 client. When the VPN 3002 works in NEM, the remote networks can see each other via their real IP addresses, not a NAT−based or PAT−based IP address. If the VPN 3002 is configured to work in NEM, H.323 can work. In other words, IP phones that are behind a VPN 3002 client can only work when VPN 3002 works in NEM. Therefore, in order to avoid one−way voice issues with a VPN 3002 client, configure the VPN 3002 client to use NEM.

In order to configure the Cisco VPN 3002 Hardware Client to use NEM, choose **Configuration > Quick > PAT** and click **No, use Network Extension mode** in the PAT window.

For more information, refer to Configuring Cisco VPN 3002 Hardware Client to Cisco IOS Router with EzVPN in Network Extension Mode

Additional Information: Verify One−Way Audio

Two useful commands to use in order to verify packet flow are the **debug cch323 rtp** command and the **debug voip rtp** command. The **debug cch323 rtp** command displays packets that are transmitted (X) and received (R) by the router. An uppercase character indicates successful transmission or reception. A lowercase character indicates a dropped packet.

```
voice−ios−gwy#debug cch323 rtp

RTP packet tracing is enabled
voice−ios−gwy#
voice−ios−gwy#
voice−ios−gwy#
voice−ios−gwy#
voice−ios−gwy#

!−−− This is an unanswered outgoing call.
!−−− Notice that 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 *****
XXXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXXrrrrrrrrrrrrrrrr
voice−ios−gwy#
voice−ios−gwy#

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

voice−ios−gwy#
voice−ios−gwy#
*Mar 3 23:53:26.570: ****** cut through in FORWARD direction *****
XXXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXrXr
XXrrrrrXrXrXrXrXrXrXrXrXrXrXrXrrXXrrXrXrXrXrXrXrXXXXXXXXXXXXXXXXrXXXXXXXXrXrXrXXrrXr
XrXrXrXrXrXrXrXrXXrrrrrrrrrrrrrrrrrrrrrrrrrrrrrr

!−−− At this point, the remote end picks up the phone.
```

```
*Mar 3 23:53:30.378: ****** cut through in BOTH direction *****
XRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXR
XXRRXRXRXXRRXRXRXRXRXXRXRXRXRXRRXRXXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRRRRRRRRRRRRRRRRRRRRRRRRRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRRR
RRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRRXXRXRXRXRXRXRRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXXRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XXRRRRRRRRRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXRXR
XRXRXRXRXRXRXRXRXRXRXRXRXXRRRXR

!--- This is the end of the conversation.
```

Note: In Cisco IOS Software Release 12.2(11)T and later, the **debug cch323 rtp** command−line interface (CLI) command has been replaced by the **debug voip rtp** command.

```
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
```

Collect Call Traffic Information over the PIX Firewall

You can troubleshoot one way calls by gathering call traffic information across the PIX Firewall. The PIX **capture** command can be used to verify the port open and used when a call occurs. Refer to Handle VoIP Traffic with the PIX Firewall for more information on VoIP traffic across the PIX Firewall.

Note: Make sure to disable the **capture** command after you generate the capture files that you need in order to troubleshoot.

Cisco Unified Communications Manager One−Way Audio Issue

This issue can only occur in an outgoing initial SIP call setup where MTP is required. In this case, the outgoing SIP INVITE message will contain an SDP offer. The issue may occur in these scenarios:

- Outgoing SIP trunk calls with Media Termination Point Required checked on the SIP trunk
- Calls between IPv6−only endpoints and IPv4−only endpoints

Solution

MTP resources may be intermittently leaked, which results in failure of SIP calls that require MTP resources. From RTMT, available MTP resources reach 0 and MTP allocation failure counts go up for each call requiring an MTP. The SDP portion of the initial INVITE will incorrectly contain **a=inactive**.

Complete these steps in order to resolve the issue:

1. Uncheck **Media Termination Point Required** on the SIP Trunk configuration, if possible.
2. If Early Offer is required, configure Early Offer, but leave Media Termination Point Required unchecked.
3. For IPv6 deployment, use dual−stack rather than IPv6−only endpoints.

Note: This is documented in Bug ID CSCtk77040 (registered customers only) .

Related Information

- **CallManager H.323: One−way Voice Issue after Transfer or Hold**
- **NAT−Support of IP Phone to Cisco CallManager**
- **H.323 Support for Virtual Interfaces**
- **Configuring Cisco VPN 3002 Hardware Client to Cisco IOS Router with EzVPN in Network Extension Mode**
- **Cisco Unity with Cisco CallManager: One Way Audio**
- **Configuring and Troubleshooting Dual NICs for Cisco Unity**
- **Voice Technology Support**
- **Voice and Unified Communications Product Support**
- **Troubleshooting Cisco IP Telephony**
- **Technical Support & Documentation − Cisco Systems**

Contacts & Feedback | Help | Site Map

Updated: Oct 13, 2008 Document ID: 5219