AudioCodes CPE & Access Gateway Products

SIP

Mediant™ 2000, Mediant™ 1000
& MediaPack™ MP-11x

CPE Troubleshooting Guide

Document #: LTRT-57601

January 2009

Contents

1 Introduction 7

2 IP Connectivity 9

2.1 I Cannot Access Web or Ping the Device 9
2.2 How Do I Ping a Network Entity from the Device 10

3 TDM (PSTN) Connectivity 13

3.1 How Do I Clear Trunk Alarms 13
3.2 How Do I Check a Trunk's Physical Integrity 15
3.3 How Do I Check for E1/T1 Clock Slips 15
3.4 How Do I Switch Between E1 and T1 Trunk Protocol Types 16
3.5 Why Can't I Stop an Active Trunk 17
3.6 How Do I Configure PSTN Clock Synchronization 17

4 Call Setup 19

4.1 How Do I Troubleshoot IP-to-Tel Call Setup 19
4.1.1 Initial IP-to-Tel Troubleshooting 20
4.1.2 Advanced IP-to-Tel Troubleshooting for Digital Interfaces 23
4.1.3 Advanced IP-to-Tel Troubleshooting for FXS Interfaces 24
4.1.4 Advanced IP-to-Tel Troubleshooting for FXO Interfaces (1-Stage Dialing) 25
4.1.5 Advanced IP-to-Tel Troubleshooting for FXO Interfaces (2-Stage Dialing) 27
4.2 How Do I Troubleshoot Tel-to-IP Call Setup 28
4.2.1 How Do I Check Device (Tel-to-IP) Connectivity 28
4.2.2 Initial Call Setup Troubleshooting 28
4.2.3 Advanced Tel-to-IP Troubleshooting for Digital Interfaces 32
4.2.4 Advanced Tel-to-IP Troubleshooting for FXO Interfaces 34
4.2.5 Advanced Tel-to-IP Troubleshooting 36

5 Caller ID 39

5.1 Why Doesn't the FXO Device Detect Caller ID 39
5.2 Why Doesn't the Phone Detect Caller ID (FXS) 41
5.3 Why Doesn't Digital Device Detect Tel-to-IP Caller ID 42
5.4 Why Doesn't Digital Device Generate Caller ID to Tel 42

6 Voice Quality 43

6.1 How Do I Troubleshoot Distorted Voice 43
6.2 How Do I Troubleshoot Voice Echo 44
6.3 How Do I Troubleshoot Voice Delay 46

7 Call Disconnect 47

7.1 Why Doesn't the FXO End a PBX/PSTN Call 47
7.2 Why Do Calls Randomly Disconnect? 49
7.3 Why Don't Calls Disconnect Upon ISDN Disconnect Message 50
7.4 Why Does the PBX Disconnect IP-to-Tel Calls 50

8 Fax and Modem 51

8.1 Why Do Fax Sessions Fail 51

9 Call Transfer 55

9.1 Why Does PBX Terminate Call Transfer by the FXO Device 55

9.2 Why Can't I Transfer a Call Between FXS Interfaces 56

10 IP Voice Mail and Unified Messaging 57

10.1 I Cannot Retrieve Voice Mail Messages 57

10.2 Why Does IP Voice Mail Request My Extension Number for Retrieving Voice Mail 57

10.3 I Cannot Leave Voice Mail Messages 58

10.4 Message Waiting Indication Does Not Function 59

10.5 I Cannot Transfer Calls to Users in Unified Messaging 60

11 Common Web, SNMP and ini File Issues 61

11.1 How Do I Restore Web Interface Username and Password Without Losing Configuration 61

11.2 How Do I Obtain the Complete ini File 61

11.3 Where Do I Place a Parameter in the ini File 61

11.4 How Can I Update the ini File Via SNMP 61

11.5 How Do I Obtain the ini File Via SNMP 62

11.6 How Do I Change Web Username and Password Via SNMP 62

11.7 How Do I Reset the Device Via SNMP 62

11.8 How Do I Force the Device to Send a SIP REGISTER via SNMP 62

11.9 How Do I Remove/Insert Mediant 1000 Modules Via SNMP 63

11.10 How Do I View PSTN Alarms Via SNMP 63

11.11 How Do I Work with Row-Status 63

11.12 Why Doesn't BootP Install on Windows Vista 64

12 Traffic Debug Analysis 65

12.1 Why Can't I Record the Device's Traffic 65

12.2 Why Doesn't Wireshark Decode Messages 65

13 Debugging Procedures 67

13.1 Case Reporting Procedures 67

13.2 Syslog 68

13.3 Wireshark Network Sniffer 69

13.4 CLI Debug Recording 73

14 Management Utilities 77

14.1 CPTWizard 77

14.2 BootP/TFTP Server 77

Notice

This document provides troubleshooting procedures for AudioCodes customer premises equipment (CPE), Voice-over-IP (VoIP) media gateway devices.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents can be viewed by registered customers at http://www.audiocodes.com/downloads.

Date Published: January-05-2009

Tip: When viewing this manual on CD, Web site or on any other electronic copy, all cross-references are hyperlinked. Click on the page or section numbers (shown in blue) to reach the individual cross-referenced item directly. To return back to the point from where you accessed the cross-reference, press the **ALT** and ← keys

Trademarks

AC logo, Ardito, AudioCoded, AudioCodes, AudioCodes logo, CTI², CTI Squared, InTouch, IPmedia, Mediant, MediaPack, MP-MLQ, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, 3GX, TrunkPack, VoicePacketizer, VoIPerfect, What's Inside Matters, Your Gateway To VoIP, are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased.

- For technical support for products purchased directly from AudioCodes and for customers registered to AudioCodes' iSupport, logon to http://crm.audiocodes.com.
- For all other AudioCodes' customers, contact support@audiocodes.com.

Reader's Notes

1 Introduction

This guide is intended to assist you in troubleshooting various problems that may arise in your network environment in which AudioCodes' VoIP gateway (hereafter referred to as *device*) is deployed.

This guide includes troubleshooting concerning the following AudioCodes SIP CPE devices:

- MediaPack Series MP-11x and MP-124
- Mediant 600
- Mediant 1000
- Mediant 2000

This guide is organized into topics based on troubleshooting areas, for example, troubleshooting voice quality or troubleshooting caller ID, and includes topics describing various debugging and management tools that can aid you in the troubleshooting process:

- "IP Connectivity" on page 9
- "TDM (PSTN) Connectivity" on page 13
- "Call Setup" on page 19
- "Caller ID" on page 39
- "Voice Quality" on page 43
- "Call Disconnect" on page 47
- "Fax and Modem" on page 51
- "Call Transfer" on page 55
- "IP Voice Mail and Unified Messaging" on page 57
- "Common Web, SNMP and ini File Issues" on page 61
- "Traffic Debug Analysis" on page 65
- "Debugging Procedures" on page 67
- "Management Utilities" on page 77

The troubleshooting topics are presented either in table format or FAQ format. The table format (shown below), includes possible causes of the problem and corresponding solutions to the problem. These causes and solutions are organized in chronological order, starting from the top of the table.

Table 1-1: Example of a Table Format for Troubleshooting

Possible Cause		Solution
a.	Cause 1	Solution 1
b.	Cause 2	Solution 2

For the procedure on how to report troubleshooting issues, refer to "Case Reporting Procedures" on page 67.

Reader's Notes

2 IP Connectivity

This section discusses troubleshooting for IP connectivity problems:

- "I Cannot Access Web or Ping the Device" on page 9
- "How Do I Ping a Network Entity from the Device" on page 10

2.1 I Cannot Access Web or Ping the Device

Table 2-1: No Web Access or Ping to the Device Troubleshooting

	Possible Cause	Solution
1.	The device is not receiving power.	**1** Verify that the LED for power is on. **2** If the Power LED is off, verify that the power cable is securely connected to the device and that the power source is functional. If both the cable and power source are ok, replace the device.
2.	The software version is not loaded to the device.	**1** Verify that the Fail LED is off. **2** If the Fail LED is lit red, use a BootP application to burn the firmware version to the device's flash memory (refer to "BootP/TFTP Server" on page 77). **3** If the LED is still on, replace the device.
3.	The Ethernet link is down.	**1** Verify that the device's Link LED is on. **2** If the Link LED is off: **a.** Ensure that the Ethernet cable is securely connected to the device's Ethernet port. **b.** Use a direct network crossover cable to connect directly the device to a PC to rule out any potential network issues. **c.** Ensure that the port on the Ethernet switch is functioning (and the switch is powered on). **d.** Ensure that the speed and connection mode of the switch is the same as the speed and connection mode of the device (for example, if the switch is configured for 100 Mbps full-duplex and the device is configured for 10 Mbps half-duplex, no Ethernet link can be established). the device's Ethernet speed and mode is configured by the *ini* file parameter EthernetPhyConfiguration. **e.** If necessary, use the reset button on the device's front panel to restore the configuration to its factory default settings (refer to the device's *User's Manual*).

	Possible Cause	Solution
4.	The IP address assigned to the device is not suitable for your network environment, or the device's IP address is unknown (forgotten).	**1** Discover the device's IP address: The simplest method is to start the Wireshark application (refer to "Wireshark Network Sniffer" on page 69), reset the device and wait for it to startup. When the device boots, it sends a Gratuitous ARP (GARP) message with its IP address. **2** Assign a new IP address to the device, using BootP or DHCP. **Note:** The device may change its IP address each time it is reset even though DHCP is disabled. Many DHCP servers are backward-compatible with BootP protocol and can be used for device configuration. These DHCP servers reply to BootP requests sent by the device. To configure the device to ignore these BootP replies, set the *ini* file parameter BootPSelectiveEnable to 1. The Selective BootP mechanism enables the device's integral BootP client to filter unsolicited BootP/DHCP replies (accepts only BootP replies that contain the text 'AUDC' in the Vendor Specific Information field).

2.2 How Do I Ping a Network Entity from the Device

The procedure below describes how to ping a network entity from the device.

➢ To ping a network entity from the device:

1. Access the device's FAE page: in your Web browser's URL field, append the case-sensitive suffix "FAE" to the device's IP address (e.g., http://10.1.229.17/FAE).

Figure 2-1: FAE Page

2. On the left pane, click the **Cmd Shell** link; the 'CmD Shell' window opens.

3. In the 'Command-Line' field, enter the following command:

   ping [IP address of the remote destination]

   For example, ping 10.33.2.34.

4. Wait several seconds and then enter the following command:

   show ping

   The following information is displayed:

```
ping 10.33.2.34
Ping process started for address 10.33.2.34. Process ID - 23.
Reply from 10.33.2.34: bytes=0 time=0ms
Reply from 10.33.2.34: bytes=0 time=0ms
Reply from 10.33.2.34: bytes=0 time=0ms
Reply from 10.33.2.34: bytes=0 time=0ms
Ping statistics for 10.33.2.34:
Packets: Sent = 4, Received = 4, Lost 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Reader's Notes

3 TDM (PSTN) Connectivity

This section discusses troubleshooting for TDM (PSTN) connectivity:

- "How Do I Clear Trunk Alarms" on page 13
- "How Do I Check a Trunk's Physical Integrity" on page 15
- "How Do I Check for E1/T1 Clock Slips" on page 15
- "How Do I Switch Between E1 and T1 Trunk Protocol Types" on page 16
- "Why Can't I Stop an Active Trunk" on page 17

3.1 How Do I Clear Trunk Alarms

The status of the E1/T1 Trunks is displayed in the Home page of the device's Web interface. The Trunk status icon should be lit green for normal functioning; otherwise, refer to the table below for possible alarms.

RJ-48c trunk connectors are wired according to the figure below:

Figure 3-1: RJ-48c Connector Pinouts for E1/T1

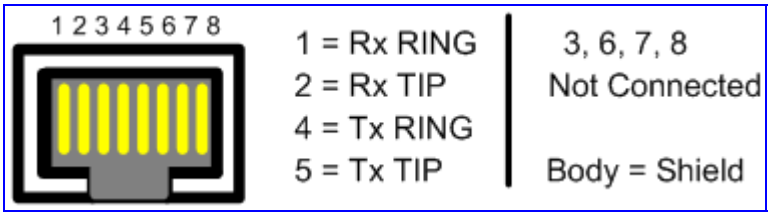


Table 3-1: No Access or Ping to Gateway

Trunk Icon Status		Possible Cause	Solution
Color	**Alarm**		
Gray	Trunk Disabled	The Trunk is not configured	Configure the Trunk in the Web interface's 'Trunk Settings' page. **Note:** If the 'Protocol Type' field displays 'NONE' (i.e., no protocol type selected) and no other trunks have been configured, after selecting a PRI protocol type, you must reset the device.
Red	Loss of Signal (LOS) or Loss of Frame (LOF)	LOS: Indicates a physical problem. LOF: Indicates that the Trunk port is not receiving framing, or has lost synchronization on the received framing.	**To clear the LOS alarm, ensure the following:** 1 The E1/T1 cable is connected securely between the device's PSTN ports and the service provider's equipment (PSTN network). 2 The E1/T1 trunk cable is not physically damaged; if so, replace the cable. 3 The E1/T1 cable is crimped correctly (refer to the figure above). 4 The correct E1/T1 cable is used (crossover / straight). If a straight cable is being used and LOS is still present, try a crossover cable, and vice versa. **To clear the LOF alarm, ensure the following:** 1 The PBX and device are configured to use the same Trunk type (E1 or T1). 2 The Framing method of the PBX and device is identical. 3 The Line code of the PBX and device is identical. 4 The clocks are synchronized (refer to "How Do I Check for E1/T1 Clock Slips" on page 15).
Yellow	Remote Alarm Indication (RAI)	The far-end equipment (e.g., PBX) has a problem with the signal that it receives from the local equipment.	Contact the PBX/PSTN provider and report this alarm to resolve the problem.
Orange	D-Channel	--	**To clear this alarm, perform the following:** 1 Ensure that the correct ISDN variant is selected. 2 If the device is configured as User side, ensure that the PBX/PSTN is configured as Network side, and vice versa. 3 Ensure that the Framing method configured for the device is the same as the Framing method on the PBX/PSTN. 4 If the D-channel alarm isn't cleared, contact the AudioCodes Technical Support team and provide them with the *ini* file of the device and a PSTN trace (refer to "CLI Debug Recording" on page 72).

3.2 How Do I Check a Trunk's Physical Integrity

➢ To check the trunks physical integrity (no hardware problem), perform the following test:

1. Use a crossover RJ-48 cable to make a loop between two active Trunks on the device.
2. In the Web interface's 'Trunk Settings' page (Web path SW Ver. 5.2: Advanced Configuration menu > Trunk Settings; Web path SW Ver. 5.4 and later: Configuration tab > PSTN Settings menu > Trunk Settings), configure the following:
   a. In the 'Protocol Type' field, configure the same protocol type for both Trunks to E1 (or T1) Transparent 30 (or set the *ini* file parameter ProtocolType to 6).
   b. In the 'Clock Master' field, configure **any** one of the Trunks to "Recovered" and the other to "Generated" (or set the *ini* file parameter ClockMaster to 0 and 1 respectively).
3. Verify that the LEDs of both Trunks are lit green.

3.3 How Do I Check for E1/T1 Clock Slips

If timing between devices is not maintained, a condition known as clock slippage (or clock slips) can occur. By definition, a clock slip is the repetition or deletion of a bit (or block of bits) in a synchronous data stream, due to a discrepancy in the read and write rates at a buffer. Slips arise because an equipment buffer store, or other mechanisms, cannot accommodate differences between the phases or frequencies of the incoming and outgoing signals. This occurs in cases where the timing of the outgoing signal is not derived from that of the incoming signal.

➢ To check for clock slips on the trunk and that the clock is synchronized:

1. Access the command shell, and then at the CLI prompt, enter the following commands:

```
pstn
physical
PstnGetPerformanceMonitoring [trunk number] 0
```

Note: Trunks are numbered from 0 to 7.

2. Copy the information that appears in the CLI output window and send it to the Technical Support Department.

Below is an example of the CLI output when using these commands:

```
pstn
CAS/ PHysical/ PstnCOmmon/
/PStn>

physical
IsdnGetDChannelStatus PstnQueryTrunkStatus PstnSendAlarm
PstnLoopCommands PstnGetPerformanceMonitoring
PstnStoPPerformanceMonitoring PstnStarTPerformanceMonitoring
/PStn/PHysical>

PstnGetPerformanceMonitoring 0 0
TrunkId = 0
Interval = 0
```

3.4 How Do I Switch Between E1 and T1 Trunk Protocol Types

➢ To switch from E1 to T1 (or vice versa):

1. Save the device's current configuration (*ini* file) to a folder on your PC, using the Web interface's 'Configuration File' page (Web path SW Ver. 5.2: Save Configuration menu; Web path SW Ver. 5.4 and later: Management tab > Software Update submenu > Configuration File).
2. Open the saved *ini* file, using a plain text editor (such as Notepad).
3. Change the value of the parameter ProtocolType_x to the required protocol type.
4. Reload the modified *ini* file to the device, using the Web interface's 'Configuration File' page.

3.5 Why Can't I Stop an Active Trunk

Table 3-2: Active Trunk Can't be Stopped Troubleshooting

	Possible Cause	Solution
1.	The Trunk provides the device's clock.	When the clock source is internal (i.e., the device receives clock synchronization from a specific Trunk), you cannot stop this Trunk (assuming that the device is synchronized with the E1/T1 clock). When you try stopping a Trunk that provides clock synchronization, the Web interface displays a warning message notifying you of this. A Trunk that is not used to supply the clock can be stopped and if the clock source is from the network, any Trunk can be stopped. In the Web interface's 'TDM Bus Settings' page (Web path SW Ver. 5.2: Advanced Configuration menu > TDM Bus Settings; Web path SW Ver. 5.4 and later: Configuration tab > TDM Configuration menu > TDM Bus Settings), perform one of the following: ▪ Assign a different E1/T1 Trunk to provide the device's clock, using the 'TDM Bus Local Reference' field (or the *ini* file parameter TDMBusLocalReference). ▪ Enable the PSTN Trunk auto-fallback clock feature, using the 'TDM Bus PSTN Auto Clock' field (or the *ini* file parameter TDMBusPSTNAutoClockEnable).

3.6 How Do I Configure PSTN Clock Synchronization

In a PSTN network, it is important to verify that all components are synchronized to a **single** clock source. Several problems (such as, echo, fax and modem failures) can be caused if the clocks aren't synchronized. Incorrect configuration can occur for example, when the device is configured to provide a clock source to a specific E1 Trunk and at the same time, the PBX is also configured to provide a clock source on the same Trunk.

Refer to "How Do I Check for E1/T1 Clock Slips" on page 15 for information on how to verify whether the device's clocks are synchronized.

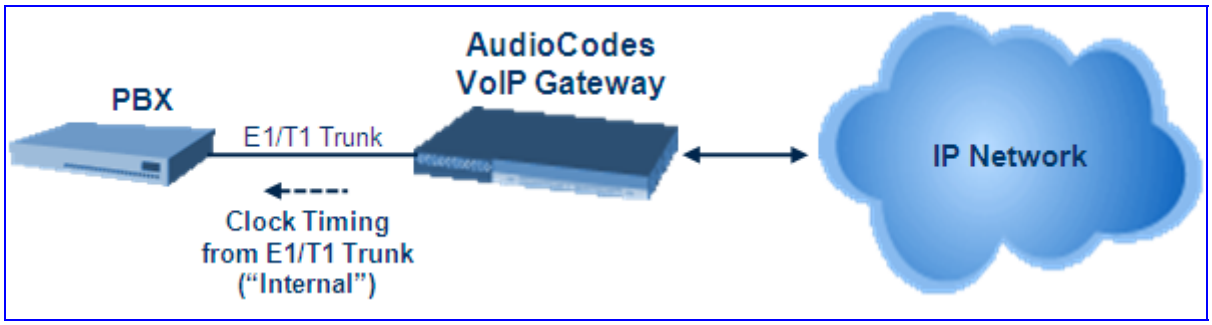
The device can be configured to generate its own timing signals using an internal clock, or recover them from one of the E1/T1 trunks.

➢ To use the device's internal clock source:

- To generate the clock from a local source, set the *ini* file parameter TDMBusClockSource to 1 (or the corresponding Web interface parameter 'TDM Bus Clock Source' to "Internal").

- For all Trunks, set the *ini* file parameter ClockMaster to 1 (or the corresponding Web interface parameter 'Clock Master ' to "Recovered"). This parameter determines the Tx clock source of the E1/T1 lines.

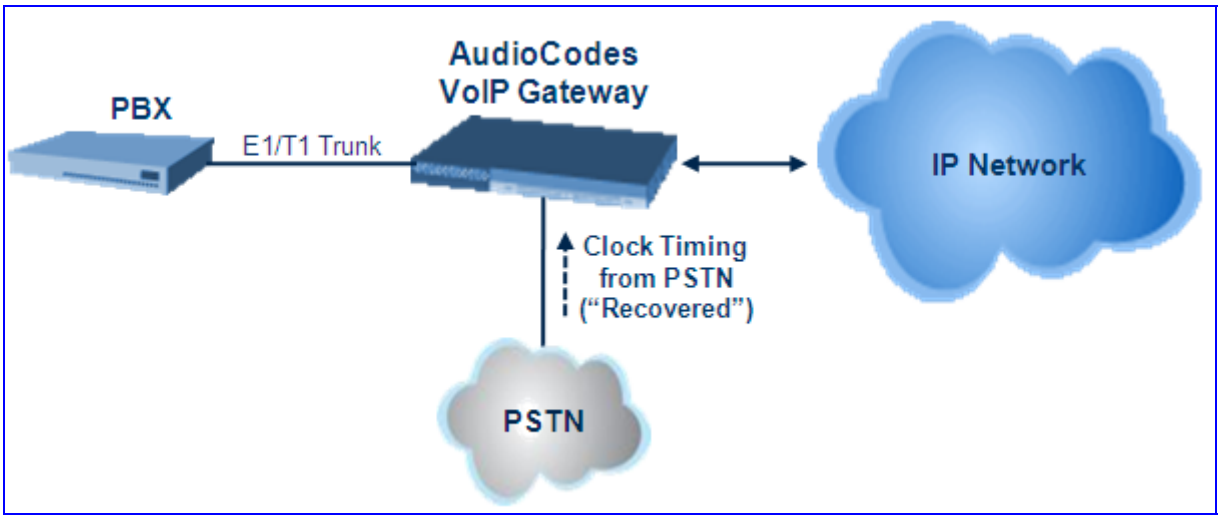
Figure 3-2: Clock Synchronization from Device



➢ To use the recovered clock option:

1. Set the *ini* file parameter TDMBusClockSource to 4 (or the corresponding Web interface parameter 'TDM Bus Clock Source' to "Network").
2. For all 'slave' trunks connected to the PSTN, set the *ini* file parameter ClockMaster_x to 0 (or the corresponding Web interface parameter 'Clock Master' to "Recovered").
3. For all 'master' trunks connected to the PBX, set the *ini* file parameter ClockMaster_x to 1 (or the corresponding Web interface parameter 'Clock Master' to "Generated").

Figure 3-3: Clock Synchronization from PSTN



The example above assumes that the device recovers its internal clock from one of the 'slave' trunks connected to the PSTN and provides a clock source to the PBX on its 'master' trunks. In addition, you must define from which of the 'slave' Trunks the device recovers its clock. The following two options are available:

- To recover the clock from a specific E1/T1 line, use the *ini* file parameter TDMBusLocalReference (range: 1-8 on the Web interface, 0-7 on *ini* file)
- Set the *ini* file parameter TDMBusPSTNAutoClockEnable to 1 to recover the clock from any connected synchronized slave E1/T1 line. If this Trunk loses its synchronization, the device attempts to recover the clock from the next Trunk. Note that initially, the device attempts to recover the clock from the Trunk defined by the *ini* file parameter TDMBusLocalReference.

4 Call Setup

This section discusses troubleshooting for call setup (or call establishment):

- "How Do I Troubleshoot IP-to-Tel Call Setup" on page 19
- "How Do I Troubleshoot Tel-to-IP Call Setup" on page 27

4.1 How Do I Troubleshoot IP-to-Tel Call Setup

This sections deals with troubleshooting for IP-to-Tel call setup:

- "Initial IP-to-Tel Troubleshooting" on page 20
- "Advanced IP-to-Tel Troubleshooting for Digital Interfaces" on page 23
- "Advanced IP-to-Tel Troubleshooting for FXS Interfaces" on page 24
- "Advanced IP-to-Tel Troubleshooting for FXO Interfaces (1-Stage Dialing)" on page 25
- "Advanced IP-to-Tel Troubleshooting for FXO Interfaces (2-Stage Dialing)" on page 27

4.1.1 Initial IP-to-Tel Troubleshooting

Table 4-1: Initial Troubleshooting for IP-to-Tel Call Setup

	Possible Cause	Solution
1.	The ports/Trunks/B-channels are not defined.	Ensure that the ports, Trunks, or B-channels involved in the call are defined (enabled) for the device. This is performed in the Web interface: ▪ For digital devices: 'Trunk Group Table' page (Web path SW Ver. 5.2: Protocol Management menu > Trunk Group; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Trunk Group submenu > Trunk Group) ▪ For MediaPack Series devices: 'Endpoint Phone Number Table' page (Web path SW Ver. 5.2: Protocol Management menu > Endpoint Phone Numbers; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Endpoint Number submenu > Endpoint Phone Number)
2.	IP-to-Tel call routing are not defined or incorrectly configured.	If you have defined Trunk/Hunt Groups (in the Web interface's 'Trunk Group Table' page for digital devices, and in the 'Endpoint Phone Number Table' page for MediaPack Series devices), ensure that you have also defined IP-to-Trunk/Hunt Group routing on the Web interface's 'IP to Trunk/Hunt Group Routing Table' page (Web path SW Ver. 5.2: Protocol Management menu > Routing Tables submenu > IP to Trunk/Hunt Group Routing; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Routing Tables submenu > IP to Trunk/Hunt Group Routing). If no Trunk/Hunt Groups are defined, the device routes IP calls to the default Trunk Group (i.e., 0).
3.	The SIP transport layer of the device and remote SIP User Agent (UA) are not identical.	Ensure that the device and the remote UA use the same SIP transport layer (i.e., UDP, TCP or TLS). The SIP transport type is configured by the *ini* file parameter SIPTransportType.
4.	The voice coders of the device and remote SIP UA are not identical.	Ensure that the coders used by the device are the same as the coders used by the remote UA. The device's coders are configured in the Web interface's 'Coders Table' page (Web path SW Ver. 5.2: Protocol Management menu > Protocol Definition submenu > Coders; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Protocol Definition submenu > Coders).

	Possible Cause	Solution

5.	The device does not receive a SIP INVITE message from the remote UA.	If no SIP INVITE message is received from the remote UA, notify the problem to the remote UA**.**
		To check whether the device receives SIP INVITE messages:
		1 Make an IP call to the device from the remote UA.
		2 Open the Syslog (refer to "Syslog" on page 68), and ensure that an INVITE is displayed (see example below):
		`---- Incoming SIP Message from 10.33.6.101:5060 ----`
		`INVITE sip:588@10.33.4.179;user=phone SIP/2.0`
		`Via: SIP/2.0/UDP 10.33.6.101;branch=z9hG4bKac302222496`
		`Max-Forwards: 70`

6.	Syslog Warning/Error displays "Cant find Endpoint"	If a SIP INVITE message is received but the Syslog shows a warning that an endpoint cannot be located, for example:
		`WARNING: (lgr_TrnkGrp)(61) !! [ERROR] #0:TrunkGroup::AllocateEndPoint- Can't find EndPoint for phone number 2000`
		`WARNING: (lgr_psbrdif)(62) !! [ERROR] MotherBoard::GetEndPoint- Can't find EndPoint for Dest:2000 Source:100 SourceIp:13d2e50`
		`WARNING: (lgr_call)(63) !! [ERROR] Call::GetEndPoint- Can't find endpoint for phone number 2000`
		Check the configurations of the following:
		▪ 'IP to Trunk/Hunt Group Routing Table' page.
		▪ Channel Select Mode in the 'Trunk/Hunt Group Settings' page (Web path SW Ver. 5.2: Protocol Management menu > Trunk Group Settings; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Trunk Group submenu > Trunk Group Settings).

7.	The device is operating behind NAT (a STUN server is not available).	The solution depends on one the following scenarios: ▪ If a SIP INVITE message is not received: Check that the Firewall/NAT server forwards incoming traffic from the public IP address to the internal IP address of the device. ▪ If a SIP INVITE message is received and the device responds with 200 OK: Verify that the Firewall/NAT server changes the IP address, declared in the SDP, to a public one. If the Firewall/NAT server does not change the IP address declared in the SDP, configure the device to perform this, using the 'NAT IP Address' parameter. Configure the public IP address of the device on the Web interface's 'IP Settings' page (Web path SW Ver. 5.2: Advanced Configuration menu > Network Settings submenu > IP Settings; Web path SW Ver. 5.4 and later: Configuration tab > Network Settings menu > IP Settings).

Possible Cause		Solution
8.	The remote peer is operating behind NAT.	Verify that the SIP INVITE message received by the device contains the public IP address of the remote peer. If the remote peer uses an internal IP address, contact the Firewall/NAT server administrator to verify that the remote peer uses and declares its public IP address.
9.	The device is operating behind NAT (a STUN server is available).	1 The solution depends on one the following scenarios: ✓ If a SIP INVITE message is not received: Check that the Firewall/NAT server forwards incoming traffic from the public IP address to the internal IP address of the device. ✓ If a SIP INVITE message is received and the device responds with 200 OK: Verify that the device declares in the SDP of the 200 OK the public IP address as determined by the STUN server. 2 Verify that the device is enabled to use a STUN server ('Enable STUN' parameter) and that its' IP address ('STUN Server Primary IP and/or 'STUN Server Secondary IP' parameters) are defined on the Web interface's 'Application Settings' page (Web path SW Ver. 5.2: Advanced Configuration menu > Network Settings submenu > Application Settings; Web path SW Ver. 5.4 and later: Configuration tab > Network Settings menu > Application Settings).
10.	None of the above has solved the problem.	Refer to the following troubleshooting sections according to your device's interface: ▪ "Advanced IP-to-Tel Troubleshooting for Digital Interfaces" on page 23 ▪ "Advanced IP-to-Tel Troubleshooting for FXS Interfaces" on page 24 ▪ "Advanced IP-to-Tel Troubleshooting for FXO Interfaces (1-Stage Dialing)" on page 25 ▪ "Advanced IP-to-Tel Troubleshooting for FXO Interfaces (2-Stage Dialing)" on page 27

4.1.2 Advanced IP-to-Tel Troubleshooting for Digital Interfaces

Table 4-2: IP-to-Tel Call Setup Troubleshooting - Digital Interfaces

	Possible Cause	Solution
1.	Alarm raised on a Trunk.	Check that there are no Trunk alarms (refer to "How Do I Clear Trunk Alarms" on page 13).
2.	Syslog does not include the **pstn send --> PlaceCall: Trunk:** message	Ensure that the following Syslog message is displayed: `pstn send --> PlaceCall: Trunk:` If the message doesn't appear, contact AudioCodes Technical Support team and provide them with the following information: ▪ *The* device's *ini* file ▪ A debug-level 5 Syslog trace

3.	No response from the PBX.	Ensure that the device receives a response from the PBX, by searching for the following Syslog message:
		`pstn recv <-- CALL_PROCEEDING`
		`pstn recv <-- CALL_ALERTING`
		`pstn recv <-- CALL_CONNECTED`
		If none of the messages appear in the Syslog, contact the PBX service provider and AudioCodes Technical Support team, and provide AudioCodes with the following information:
		▪ The device's *ini* file
		▪ A Syslog trace
		▪ A PSTN trace (refer to "CLI Debug Recording" on page 72)

4.1.3 Advanced IP-to-Tel Troubleshooting for FXS Interfaces

Table 4-3: IP-to-Tel Call Setup Troubleshooting - FXS Interfaces

	Possible Cause	Solution

1.	The Channel Select Mode is incorrectly configured.	The Channels Select Mode is configured incorrectly if a SIP INVITE message is received, but the Syslog displays a warning that an endpoint cannot be located, for example:
		`WARNING: (lgr_TrnkGrp)(61) !! [ERROR] #0:TrunkGroup::AllocateEndPoint- Can't find EndPoint for phone number 2000`
		`WARNING: (lgr_psbrdif)(62) !! [ERROR] MotherBoard::GetEndPoint- Can't find EndPoint for Dest:2000 Source:100 SourceIp:13d2e50`
		`WARNING: (lgr_call)(63) !! [ERROR] Call::GetEndPoint- Can't find endpoint for phone number 2000`
		To resolve this issue, perform one of the following:
		▪ If the Channel Select Mode is "By Dest Phone Number", ensure that this endpoint is assigned with the correct phone number (in the 'Trunk Group Table' page - Web path SW Ver. 5.2: Protocol Management menu > Trunk Group; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Trunk Group submenu > Trunk Group - for Mediant 1000 or 'Endpoint Phone Number Table' page - Web path SW Ver. 5.2: Protocol Management menu > Endpoint Phone Numbers; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Endpoint Number submenu > Endpoint Phone Number - for MediaPack).
		▪ Change the 'Channel Select Mode' field to a channel select mode other than "By Dest Phone Number" (in the 'Trunk/Hunt Group Settings' page).

2.	The phone is not connected to the defined device's port	If all the previous troubleshooting is resolved and the phone still doesn't ring, ensure the following: 1 For phones requiring battery power, that the phone is receiving power (battery or mains). 2 The phone is securely connected to the device's designated FXS port. 3 The relevant channel LED is flashing. If the LED is not flashing, contact AudioCodes Technical Support team and provide the following information: ✓ The device's *ini* file ✓ A debug-level 5 Syslog trace

4.1.4 Advanced IP-to-Tel Troubleshooting for FXO Interfaces (1-Stage Dialing)

Table 4-4: IP-to-Tel Call Setup Troubleshooting - FXO Interfaces (One-Stage Dialing)

	Possible Cause	Solution

1.	Channel Select Mode is incorrectly configured.	If a SIP INVITE message is received but the Syslog shows a warning that an endpoint cannot be located, for example:
		`WARNING: (lgr_TrnkGrp)(61) !! [ERROR] #0:TrunkGroup::AllocateEndPoint- Can't find EndPoint for phone number 2000`
		`WARNING: (lgr_psbrdif)(62) !! [ERROR] MotherBoard::GetEndPoint- Can't find EndPoint for Dest:2000 Source:100 SourceIp:13d2e50`
		`WARNING: (lgr_call)(63) !! [ERROR] Call::GetEndPoint- Can't find endpoint for phone number 2000`
		If the Channel Select Mode is set to "By Dest Phone Number", change the Channel Select Mode to either "Cyclic Ascending", "Cyclic Descending", "Ascending", or "Descending" on the Web interface's 'Trunk/Hunt Group Settings' page (Web path SW Ver. 5.2: Protocol Management menu > Trunk Group Settings; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Trunk Group submenu > Trunk Group Settings).

2.	The FXO interface doesn't seize the FXO line with the PBX.	In the Syslog, ensure that the following message appears: `FXO Seize Line` If this message does not appear, ensure that the physical FXO trunk line is securely connected between the device and PBX. If this message still does not appear, send the Syslog trace and the device's *ini* file to AudioCodes Technical Support team.
3.	The device does not detect a dial tone from the PBX.	In the Syslog, check if the following message appears: `WAIT_FOR_DIAL_TIMER_EXPIRED_EV` By default, the FXO device dials the phone number (to the PSTN/PBX line) only after it detects a dial tone. If the above message doesn't appear in the Syslog, you can perform one of the following: ▪ Define the dial tone that is generated by the PBX in the device's Call Progress Tone (CPT) file. ▪ Disable this option for the device, using the *ini* file parameter IsWaitForDialTone set to 0.
4.	The FXO interface does not dial the correct destination phone number.	In the Syslog, check if the following message appears: `Sending DTMFs` and that the message shows the correct destination number. This message indicates that the FXO dialed the requested number.
5.	The phone does not ring.	Contact the PBX service provider.

	Possible Cause	Solution

6.	The FXO interface does not send a SIP 200 OK response message to the IP side.	The FXO should send a SIP 200 OK response message to the IP side that originally sent the INVITE request message. In the Syslog, ensure that the following message appears:
		`---- Outgoing SIP Message to`
		`NOTICE: SIP/2.0 200 OK`
		If this message does not appear, perform the following:
		1 If the PBX implements Polarity Reversal, ensure that EnableReversalPolarity is set to 1 (the device sends SIP 200 OK message only upon detection of polarity reversal). Otherwise, ensure that EnableReversalPolarity is set to 0.
		2 Check the settings of the parameter EnableVoiceDetection.
		✓ If it is set to 1, the device sends 200 OK (to INVITE) messages when speech is detected from the Tel side. Therefore, start speaking immediately after answering the PBX phone.
		✓ If it is set to 0, the device immediately sends 200 OK messages after the device completes dialing to the Tel side.
		If the problem persists despite all the previous troubleshooting, send the AudioCodes Technical Support team the following information:
		▪ The device's *ini* file
		▪ A Syslog trace

4.1.5 Advanced IP-to-Tel Troubleshooting for FXO Interfaces (2-Stage Dialing)

Table 4-5: IP-to-Tel Call Setup Troubleshooting - FXO Interfaces (Two-Stage Dialing)

	Possible Cause	Solution

1.	Channel Select Mode is by phone number	If a SIP INVITE message is received but the Syslog shows a warning that an endpoint cannot be located, for example:
		`WARNING: (lgr_TrnkGrp)(61) !! [ERROR] #0:TrunkGroup::AllocateEndPoint- Can't find EndPoint for phone number 2000`
		`WARNING: (lgr_psbrdif)(62) !! [ERROR] MotherBoard::GetEndPoint- Can't find EndPoint for Dest:2000 Source:100 SourceIp:13d2e50`
		`WARNING: (lgr_call)(63) !! [ERROR] Call::GetEndPoint- Can't find endpoint for phone number 2000`
		If the Channel Select Mode is set to "By Dest Phone Number" (i.e., by destination phone number), perform one of the following:
		▪ Ensure that the endpoint is assigned with the correct phone number (in the Web interface's 'Trunk Group Table' page for Mediant 1000 or 'Endpoint Phone Number Table' page for MediaPack).
		▪ Change the Channel Select Mode to any select mode other than "By Dest Phone Number" (in the Web interface's 'Trunk/Hunt Group Settings' page).

2.	The FXO interface doesn't seize the FXO line with the PBX.	In the Syslog, ensure that the following message appears: `FXO Seize Line` If this message does not appear, ensure that the physical FXO trunk line is securely connected between the device and PBX. If this message still does not appear, send the Syslog trace and the device's *ini* file to AudioCodes Technical Support team.

3.	The FXO interface does not send the SIP 200 OK response message to the IP side.	The FXO should immediately send a SIP 200 OK response message to the IP side that originally sent the INVITE request message. In the Syslog, ensure that the following message appears:
		`---- Outgoing SIP Message to`
		`NOTICE: SIP/2.0 200 OK`
		If this message does not appear, contact AudioCodes Technical Support.

4.	The IP side does not hear a dial tone.	Contact the PBX service provider.

4.2 How Do I Troubleshoot Tel-to-IP Call Setup

The sections deals with troubleshooting for Tel-to-IP call setup:

- "How Do I Check Device (Tel-to-IP) Connectivity" on page 28
- "Initial Tel-to-IP Troubleshooting" on page 28
- "Advanced Tel-to-IP Troubleshooting for Digital interfaces" on page 32
- "Advanced Tel-to-IP Troubleshooting for FXO Interfaces" on page 34
- "Advanced Tel-to-IP Troubleshooting" on page 35
- "Why is there a Delay in Connecting a Call" on page 30

4.2.1 How Do I Check Device (Tel-to-IP) Connectivity

The procedure below describes how to verify the device's connectivity with a certain IP address (destination).

➢ To check device connectivity with a specific IP destination:

1. Verify that the device's network settings (IP address, subnet mask, and default Gateway) are correct and suit your network environment. Ensure that you have defined a Default gateway in scenarios where the destination IP address is not in the same subnet as the device.
2. Verify that you can ping from the device to the remote IP address (refer to "How Do I Ping a Network Entity from the Device" on page 10).

4.2.2 Initial Call Setup Troubleshooting

4.2.2.1 Initial Tel-to-IP Troubleshooting

Follow the procedures below for troubleshooting Tel-to-IP call setup.

Table 4-6: Tel-to-IP Call Setup Troubleshooting - General

Possible Cause		Solution
1.	The device has no IP connectivity with the IP destination.	Check for IP connectivity as described in "How Do I Check Device (Tel)-to-IP Connectivity" on page 28.
2.	Tel-to-IP call routing is not correctly defined.	When a Proxy server is used (and registration is enabled - in the 'Proxy & Registration' page - Web path SW Ver. 5.2: Protocol Management menu > Protocol Definition submenu > Proxy & Registration; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Protocol Definition submenu > Proxy & Registration), verify that the device is correctly registered to the Proxy**.** You can check this in the Web interface's 'Registered Users' page, or at the Proxy server, or in a Syslog trace (verify SIP 200 OK response to the REGISTER request from the Proxy).

Possible Cause		Solution
		When a Proxy server isn't used, the destination IP address must be defined in the Web interface's 'Tel to IP Routing' page (Web path SW Ver. 5.2: Protocol Management menu > Routing Tables submenu > Tel to IP Routing; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Routing Tables submenu > Tel to IP Routing).
3.	The ports/Trunks/B-channels are not defined.	Ensure that the ports, Trunks, or B-channels involved in the call are defined (enabled) for the device. This is performed in the Web interface's 'Trunk Group Table' page (Web path SW Ver. 5.2: Protocol Management menu > Trunk Group; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Trunk Group submenu > Trunk Group) for digital devices, and in the 'Endpoint Phone Number Table' page (Web path SW Ver. 5.2: Protocol Management menu > Endpoint Phone Numbers; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Endpoint Number submenu > Endpoint Phone Number) for MediaPack Series devices.
4.	The SIP transport layer of the device and remote SIP User Agent (UA) are not identical.	Ensure that the device and the remote UA use the same SIP transport layer (i.e., UDP, TCP or TLS). The SIP transport type is configured by the *ini* file parameter SIPTransportType.
5.	The voice coders of the device and remote SIP UA are not identical.	Ensure that the coders used by the device are the same as the coders used by the remote UA. The device's coders are configured in the Web interface's 'Coders Table' page (Web path SW Ver. 5.2: Protocol Management menu > Protocol Definition submenu > Coders; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Protocol Definition submenu > Coders).
6.	The device is operating behind NAT (a STUN server is not available).	Verify that public IP address declared for the device appears in the SDP of the SIP INVITE message. To verify and configure the setting, use the 'NAT IP Address' parameter in the Web interface's 'IP Settings' page (Web path SW Ver. 5.2: Advanced Configuration menu > Network Settings submenu > IP Settings; Web path SW Ver. 5.4 and later: Configuration tab > Network Settings menu > IP Settings).
7.	The remote peer is operating behind NAT.	If no SIP messages are received, check that the Firewall/NAT server forwards incoming traffic from the public IP address to the internal IP address of the device. If a SIP 200 OK message is received, verify that it contains the public IP address of the remote peer. If the remote peer uses an internal IP address, contact the Firewall/NAT server administrator to verify that the remote peer uses and declares its public IP address.

Possible Cause		Solution
8.	The device is operating behind NAT (a STUN server is available).	1 Verify that public IP address declared for the device appears in the SDP of the SIP INVITE message as assigned to the device by the STUN server. 2 Verify that the device is enabled to use a STUN server ('Enable STUN' parameter) and that its' IP address ('STUN Server Primary IP and/or 'STUN Server Secondary IP' parameters) are defined (in the Web interface's 'Application Settings' page - Web path SW Ver. 5.2: Advanced Configuration menu > Network Settings submenu > Application Settings; Web path SW Ver. 5.4 and later: Configuration tab > Network Settings menu > Application Settings).
9.	None of the above troubleshooting solves the problem.	Refer to the following troubleshooting sections according to your device's interface: ▪ "Advanced Tel-to-IP Troubleshooting for Digital interfaces" on page 32 ▪ "Advanced Tel-to-IP Troubleshooting for FXO Interfaces" on page 34

4.2.2.2 Why is there a Delay in Connecting a Call

After dialing, if there is a delay until the call is connected, refer to the table below for troubleshooting.

Table 4-7: Delay in Connecting Call Troubleshooting

Possible Cause		Solution
1.	The device's digit map plan is not configured or incorrectly configured.	Configure the digit mapping, using the ini file parameter DigitMapping. If the digit string (i.e., dialed number) matches one of the patterns in the digit map, the device stops collecting digits and establishes a call with the collected number. The digit map pattern can contain up to 52 options, each separated by a vertical bar (|). The maximum length of the entire digit pattern is 152 characters. Available notations: ▪ [n-m]: Range of numbers (not letters). ▪ . (single dot): Repeat digits until next notation (e.g., T.). ▪ x: Any single digit. ▪ T: Dial timeout (configured by the parameter TimeBetweenDigits). ▪ S: Immediately applies a specific rule that is part of a general rule. For example, if your digit map includes a general rule 'x.T' and a specific rule '11x', for the specific rule to take precedence over the general rule, append 'S' to the specific rule (i.e., '11xS'). An example of a digit map is shown below: 11xS|00T|[1-7]xxx|8xxxxxxx|#xxxxxxx|*xx|91xxxxxxxxx|9011x.T In the example above, the last rule can apply to

Possible Cause		Solution
		International numbers - 9 for dialing tone, 011 is the Country Code, and then any number of digits for the local number ('x.'). **Note:** For BRI/PRI interfaces, the digitmap mechanism is applicable only when ISDN Overlap dialing is used (ISDNRxOverlap is set to 1).
2.	The device is configured to collect more digits than what is actually dialed.	Ensure that the values of the following Web interface parameters in the 'DTMF & Dialing' page (Web path SW Ver. 5.2: Protocol Management menu > Protocol Definition submenu > DTMF & Dialing; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Protocol Definition submenu > DTMF & Dialing) are not configured too high: ▪ 'Max Digits In Phone Num' (MaxDigits). ▪ 'Inter Digit Timeout for Overlap Dialing' (TimeBetweenDigits)
3.	The device takes a long time to detect a dial tone. **Note:** Only applicable to IP-to-Tel calls in FXO interfaces for One-Stage Dialing.	If the 'Waiting For Dial Tone' parameter is configured to "Yes" (i.e., wait for dial tone, default), it can take the device 1 to 3 seconds to detect a dial tone (according to the dial tone configuration in the Call Progress Tones file). Therefore, to resolve this problem, you can configure the parameter 'Waiting For Dial Tone' to "No". However, this configuration is not recommended.

4.2.2.3 Why No Response from Dialing Digits (DTMF) During a Call

A common issue is that during an active call, you may be required to press digits (touch-tone dialing) such as in IVR applications, but no response occurs. For example, when accessing your voice mail you need to enter (press) the digits of your account number or PIN.

Table 4-8: DTMF Digit Dialing Troubleshooting

	Possible Cause	Solution
1.	The selected DTMF method for sending DTMF signals during active calls is not compatible.	You can configure the transport method for sending DTMF digits over the IP network to the remote peer (during active calls). The following modes are supported: ▪ Using INFO messages according to Nortel mode. ▪ Using INFO messages according to Cisco mode. ▪ Using INFO messages according to Korea mode. ▪ Using NOTIFY messages. ▪ Using RFC 2833 relay with Payload type negotiation. ▪ Sending DTMF digits (in RTP packets) as part of the audio stream. Note that this method is normally used with G.711 coders; with other low-bit rate (LBR) coders, the quality of the DTMF digits is reduced. Verify that the 'Tx DTMF Options' parameter in the Web interface's 'DTMF & Dialing' page (Web path SW Ver. 5.2: Protocol Management menu > Protocol Definition submenu > DTMF & Dialing; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Protocol Definition submenu > DTMF & Dialing) is compatible with the selected method.

4.2.3 Advanced Tel-to-IP Troubleshooting for Digital Interfaces

Table 4-9: Tel-to-IP Call Setup Troubleshooting - Digital Interfaces

	Possible Cause	Solution
1.	Alarm raised on a Trunk.	Check that there are no Trunk alarms (refer to "How Do I Clear Trunk Alarms" on page 13).
2.	The device does not receive PSTN messages from the PBX.	Ensure that the PSTN messages from the PBX are received by the device: 1 Enable Syslog. 2 Make a call from the PBX to the remote IP UA (via the device). 3 Start a Syslog session, and verify that the following message appears: `pstn recv <-- INCOMING_CALL` 4 If this message is not received, contact the PBX service provider.

	Possible Cause	Solution
3.	The PBX is configured to operate in overlap dialing while the device is configured to en-bloc dialing.	The device sends a SIP INVITE message only after the complete number is received from the PBX. The PBX should indicate that the whole number has been sent, by including the Sending Complete Information Element (IE) in the ISDN SETUP message and/or subsequent INFO Q.931 messages. **1** Verify that the device has been enabled to receive ISDN overlap dialing, by ensuring that the Web interface's parameter 'Enable Receiving of Overlap Dialing' is configured to "Enable" in the 'Trunk Settings' page (Web path SW Ver. 5.2: Advanced Configuration menu > Trunk Settings; Web path SW Ver. 5.4 and later: Configuration tab > PSTN Settings menu > Trunk Settings) or the *ini* file parameter ISDNRxOverlap is set to 1. **2** Verify that the device is correctly configured to identify the end of the number that is sent by the PBX (only relevant when a Sending Complete IE isn't sent by the PBX). The following parameters define how the device detects when dialing is complete (refer to "Why is there a Delay in Connecting a Call" on page 30): ✓ Web parameter 'Max Digits in Phone Num' (MaxDigits) ✓ Web 'Digit Mapping Rules' ✓ Web parameter 'Inter Digit Timeout for Overlap Dialing' (TimeBetweenDigits) These parameters are located in the Web interface's 'DTMF & Dialing' page (Web path SW Ver. 5.2: Protocol Management menu > Protocol Definition submenu > DTMF & Dialing; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Protocol Definition submenu > DTMF & Dialing).
4.	The device is not configured to play a dial tone to the ISDN side and collect digits from the user.	Some BRI phones operating in Point-to-MultiPoint mode and configured for overlap dialing, expect that the device plays a dial tone. To play a dial tone to the ISDN user side when an empty called number is received, set the *ini* file parameter ISDNINCallsBehavior to 65536. This results in the Progress Indicator to be included in the SetupAck ISDN message.
5.	None of the above solves the problem.	Refer to "Advanced Tel-to-IP Troubleshooting" on page 35.

4.2.4 Advanced Tel-to-IP Troubleshooting for FXO Interfaces

Table 4-10: Tel-to-IP Call Setup Troubleshooting - FXO Interfaces

	Possible Cause	Solution

1.	The PSTN ringing signal from the PBX is not received by the device due to incorrect physical connection of PBX trunk line to the device's FXO port.	Verify that the physical PBX trunk line connection is correct, by performing the following:
		1 Enable Syslog.
		2 Make a call from the PBX to an IP destination (via the device).
		3 Open a Syslog session and verify that the following messages appear:
		`18:19:58.398: 10.15.6.1: NOTICE: (lgr_psbrdex)(373) recv <-- ANALOG_IF_RING_START Ch:4 type(0)`
		`18:19:58.398: 10.15.6.1: NOTICE: (lgr_flow)(374) #4:RING_START_EV`
		`18:19:58.414: 10.15.6.1: NOTICE: (lgr_flow)(375) | #4:RING_START_EV`
		`18:19:59.351: 10.15.6.1: NOTICE: (lgr_psbrdex)(376) recv <-- EV_ANALOG_IF_RING_END Ch:4 type(0)`
		`18:19:59.351: 10.15.6.1: NOTICE: (lgr_flow)(377) #4:RING_END_EV`
		`18:19:59.351: 10.15.6.1: NOTICE: (lgr_flow)(378) | #4:RING_END_EV`
		4 If the Syslog messages above do not appear, check that the correct PBX trunk line is connected to the device's FXO port, or contact the PBX service provider.

2.	The Automatic Dialing mode is not correctly configured.	If you are implementing the Automatic Dialing feature, ensure that it is configured correctly. This is configured in the Web interface's 'Automatic Dialing' page (Web path SW Ver. 5.2: Protocol Management menu > Endpoint Settings submenu > Automatic Dialing; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Endpoint Settings submenu > Automatic Dialing). **Note:** There are two types of Automatic Dialing: ▪ When making a call, the number in the 'Destination Phone Number' field is automatically dialed if the phone is off-hooked (for FXS interfaces) or a ring signal is applied to a port (FXO interfaces). ▪ When a phone is off-hooked and no digit is dialed for a user-defined period (HotLineToneDuration), the number in the 'Destination Phone Number' field is automatically dialed (applies to FXS and FXO interfaces).

	Possible Cause	Solution

3.	The CPT file does not include a dial tone entry when Automatic Dialing is not used.	If you are not implementing Automatic Dialing, you should hear a dial tone and then dial the destination number.
		1 Open the Syslog and verify that the following messages appear:
		`18:19:59.383: 10.15.6.1: NOTICE: (lgr_flow)(385) | #4:FXO Seize Line`
		`18:19:59.398: 10.15.6.1: NOTICE: (lgr_psbrdif)(387) #4:PSOSBoardInterface::PlayTone - Called Tone=DIAL_TONE Direction=PLAY_TONE_2_TEL`
		2 If you can't hear a dial tone, check that the CPT file contains a dial tone entry.

4.	None of the above solves the problem.	Refer to "Advanced Tel-to-IP Troubleshooting" on page 35.

4.2.5 Advanced Tel-to-IP Troubleshooting

If none of the previous troubleshooting procedures have solved the problem, follow the troubleshooting described in the table below.

Table 4-11: Tel-to-IP Call Setup Advanced Troubleshooting

	Possible Cause	Solution

1.	The device does not send a SIP INVITE request to the remote UA.	1 Ensure that the device sends SIP INVITE messages to the remote UA. Open the Syslog (refer to "Syslog" on page 68), and ensure that an INVITE is displayed:
		`---- Outgoing SIP Message to`
		`INVITE sip:102@10.33.6.100;user=phone SIP/2.0`
		✓ If no SIP INVITE message appears in the Syslog, then the device incorrectly processes the information received from the Tel side (telephone/PBX/PSTN). Send the Syslog Debug Level 5 trace and the device's *ini* file to AudioCodes Technical Support team.
		✓ If the SIP INVITE message appears in the Syslog, verify that the IP address displayed in the "Outgoing SIP Message to" is the correct IP address of the remote peer.
		2 Ensure that the 'Tel-to-IP Routing' table is correctly configured (refer to "Initial Tel-to-IP Troubleshooting" on page 28).

2.	The remote UA does not respond.	Ensure that the remote UA responds to the INVITE message sent from the device: 1 Open the Syslog and verify that the remote UA responds with the SIP message 100 Trying, for example: `---- Incoming SIP Message from SIP/2.0 100 Trying` 2 If the SIP 100 Trying message is not received, check the remote UA.
3.	The device receives a SIP 407 response from the remote IP UA.	If the response for the REGISTER is "407 Proxy Authorization Required", the device must send another REGISTER request with the SIP user name and password in the Proxy-Authorization header. If the device sent the second REGISTER and there is still no 200 OK response from the proxy, check that the user name and password is properly defined in the Web interface's 'Authentication' page (Web path SW Ver. 5.2: Protocol Management menu > Endpoint Settings submenu > Authentication; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Endpoint Settings submenu > Authentication).
4.	The device receives a SIP 401 response from the remote IP UA.	If the response for the INVITE is "401 Unauthorized", the device must send another INVITE request with the SIP user name and password in the Proxy- WWW-Authenticate header. If the device sent the second INVITE and the call fails, verify the user name and password in the Web interface's 'Authentication' page.

	Possible Cause	Solution
5.	The device receives a SIP 415 response from the remote IP UA.	If the response from the remote UA for the INVITE is "415 Unsupported Media Type", then the media type contained in the INVITE request is not supported. This may mean a problem with coder negotiation. Therefore, check your coder settings in the Web interface's 'Coders' page (Web path SW Ver. 5.2: Protocol Management menu > Protocol Definition submenu > Coders; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Protocol Definition submenu > Coders).
6.	The device receives a SIP 484 or 404 response from the remote IP UA.	**1** If the response for the INVITE is "484 Address Incomplete" or "404 Not Found", verify that the number sent in the INVITE is correct. **2** If you dial the full number, but the INVITE only displays part of the number, verify the following parameters in the Web interface's 'DTMF & Dialing' page (Web path SW Ver. 5.2: Protocol Management menu > Protocol Definition submenu > DTMF & Dialing; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Protocol Definition submenu > DTMF & Dialing): ✓ 'Max Digits In Phone Num' (MaxDigits) is not too low. ✓ 'Inter Digit Timeout for Overlap Dialing' (TimeBetweenDigits) parameter is not too short. ✓ Verify that the number the user is dialing matches the device's digit map rules (refer to "Why is there a Delay in Connecting a Call" on page 30). **3** If you dial the full number, but a different (i.e., incorrect) number is displayed in the SIP INVITE message, check the number manipulation settings in the 'Destination Phone Number Manipulation Table for Tel to IP Calls' page (Web path SW Ver. 5.2: Protocol Management menu > Manipulation Tables submenu > Tel to IP Destination Numbers; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Manipulation Tables submenu > Dest Number Tel to IP).
7.	The device receives other Client-Error SIP responses (not mentioned previously) from the remote IP UA.	For all other Failure of Request (4xx), Server Failure (5xx), or Global Error (6xx) responses such as "403 Forbidden", "500 Server Internal Error" or "603 Decline", contact the proxy or the remote user agent team.

Reader's Notes

5 Caller ID

This section discusses troubleshooting for caller ID:

- "Why Doesn't the FXO Device Detect Caller ID" on page 39
- "Why Doesn't the Phone Detect Caller ID (FXS)" on page 40
- "Why Doesn't Digital Device Detect Tel-to-IP Caller ID" on page 41
- "Why Doesn't Digital Device Generate Caller ID to Tel" on page 42

5.1 Why Doesn't the FXO Device Detect Caller ID

The troubleshooting information below is relevant to FXO devices that do not detect the Caller ID signal that is sent by the PBX (i.e. Tel-to-IP calls).

Table 5-1: PBX Caller ID not Detected by FXO Device Troubleshooting

	Possible Cause	Solution
1.	Caller ID is not enabled on the device.	Verify that the parameter EnableCallerID is set to 1.
2.	The Caller ID standard of the device and the PBX are not the same.	Verify that the caller ID standard (and substandard) of the device match the standard (and substandard) of the PBX/Tel, using the following *ini* file parameters: ▪ CallerIDType ▪ BellcoreCallerIDTypeOneSubStandard ▪ ETSICallerIDTypeOneSubStandard
3.	The DC offset from the PBX prevents Caller ID detection.	Enable DC removal option, by setting the *ini* file parameter ECDCRemoval to 1 (using the Web interface's AdminPage). **Note:** The device must be reset for this setting to take effect.
4.	Caller ID Transfer type is not configured to mute.	Verify that the parameter CallerIDTransportType is set to default (i.e., 3 or "Mute" in the Web interface's 'Fax/Modem/CID Settings' page - Web path SW Ver. 5.2: Advanced Configuration menu > Media Settings menu > Fax/Modem/CID Settings; Web path SW Ver. 5.4 and later: Configuration tab > Media Settings menu > Fax/Modem/CID Settings).
5.	Distorted Caller ID signal due to incorrect line characteristics.	If the caller ID signal is distorted, the device does not recognize it. Verify that the correct line characteristics are used (using the *ini* file parameter CountryCoefficients).
6.	Number of rings before device begins detecting Caller ID signal is not configured.	Configure the number of rings (using the *ini* file parameter RingsBeforeCallerID) before the device starts detection of caller ID. Typically, the Caller ID signals are detected between the first and second rings. However, sometimes the Caller ID is detected before the first ring signal (in such a scenario, set the *ini* file parameter RingsBeforeCallerID to 0). **Note:** The number of rings before sending Caller ID is determined by the PBX providing the analog line.

Possible Cause		Solution
7.	If none of the above solves the problem.	1 Connect a phone to the analog line of the PBX (instead of the FXO device) and then verify that the phone displays the caller ID. 2 If the FXO device still does not detect the caller ID signal that is sent by the PBX, record the signal using the procedure below and send it to AudioCodes Technical Support (along with the *ini* file and a debug level 5 Syslog trace).

➢ To record the caller ID signal that is sent by the PBX to the FXO, take the following steps:

1. In the 'Tel to IP Routing' table, route everything to the PC that you use for capturing.
2. Configure the following *ini* file parameters:
   - FXOSeizeLine = 0.
   - RTPOnlyMode = 1 (or 2) – this allows the RTP to be sent without SIP signaling.
   - Set the Coder to G.711.
   - EnableCallerID = 0.
   - RingsBeforeCallerID = 0.
   - Set the automatic dialing to hotline, for example: TargetOfChannel7 = 9005,2
   - HotLineToneDuration = 0.
   - CallerIDTransportType = 0
3. These settings force the FXO to send RTP to your PC, by seizing the line immediately after receiving the first ring. Capture the RTP using Wireshark (refer to "Wireshark Network Sniffer" on page 69) or you can also use DSP traces. Send the file to AudioCodes Technical Support.

Note: To stop the RTP stream, reset the port using the Web interface, by clicking the port icon in the 'Home' page.

5.2 Why Doesn't the Phone Detect Caller ID (FXS)

The troubleshooting information below is for FXS devices whose generated Caller ID signal is not detected by the phone connected to their analog ports (i.e., IP to Tel).

Table 5-2: FXS Caller ID not Detected by Phone Troubleshooting

	Possible Cause	Solution
1.	Caller ID is not enabled on the device.	Verify that the parameter EnableCallerID is set to 1.
2.	The Caller ID standard of the device and the phone set are not the same.	Verify that the caller ID standard (and substandard) of the device match the standard (and substandard) of the telephone set, using the following *ini* file parameters: ▪ CallerIDType ▪ BellcoreCallerIDTypeOneSubStandard ▪ ETSICallerIDTypeOneSubStandard
3.	Caller ID Transfer type is not set to mute.	Verify that the parameter CallerIDTransportType is set to default (i.e., 3 or "Mute" in the Web interface's 'Fax/Modem/CID Settings' page - Web path SW Ver. 5.2: Advanced Configuration menu > Media Settings menu > Fax/Modem/CID Settings; Web path SW Ver. 5.4 and later: Configuration tab > Media Settings menu > Fax/Modem/CID Settings).
4.	Incorrect coefficient file loaded to the device.	If the caller ID signal is distorted, the device does not recognize it. Verify that the coefficient file that is loaded to the device is correct. To load the correct coefficient file, refer the *User Manual*.
5.	If none of the above solves the problem.	If the phone that is connected to the FXS device still doesn't detect the caller ID signal that is sent by the device, perform the following: 1 Connect the phone that was connected to the FXS port to a PBX/PSTN analog line and then verify that the phone correctly displays its Caller ID. 2 Connect the FXO device to the same PBX analog line and record its Caller ID signal (refer to "Why Doesn't the FXO Device Detect Caller ID" on page 39 for recording the caller ID signal sent by the PBX to the FXO) and send it to AudioCodes Technical Support (along with the *ini* file and a debug-level 5 Syslog trace).

5.3 Why Doesn't Digital Device Detect Tel-to-IP Caller ID

Table 5-3: Device Doesn't Detect Caller ID from PBX Troubleshooting

	Possible Cause	Solution
1.	The device does not receive Caller ID and presentation permission from PBX.	Verify that the device receives Caller ID and presentation permission from the PBX. Open the Syslog, and verify that the following message received: `LOCAL_INCOMING_CALL_EV(Trunk:0 Conn:255 Bchannel:29 ServiceCap=V` **`SrcPN=4247`** `DstPN=4777 SrcSN= DstSN= SrcNT=4 SrcNP=9` **`SrcPres=0`** `SrcScrn=0 DstNT=4 DstNP=9 RdrctNum= RdNT=0 RdNP=0 RdPres=0 RdScrn=0 RdRsn=0 Excl=1 Display= OrigPN= CPC=-1 TpEv=66)`
2.	The device sends the incorrect Caller ID to the IP in the INVITE message.	Verify that the device sends the correct Caller ID in the From header of the outgoing SIP INVITE message.
3.	The configuration in the Web interface restricts Caller ID.	Verify that the 'Presentation' field in the Web interface's 'Source Phone Number Manipulation Table for Tel to IP Calls' page (Web path SW Ver. 5.2: Protocol Management menu > Manipulation Tables submenu > Tel to IP Source Numbers; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Manipulation Tables submenu > Source Number Tel to IP) is not set to "Restricted".

5.4 Why Doesn't Digital Device Generate Caller ID to Tel

Table 5-4: Device Doesn't Generate Caller ID from IP to Tel Troubleshooting

	Possible Cause	Solution
1.	No Caller ID in incoming SIP INVITE message.	Verify that the correct caller ID is received in the From header of the incoming INVITE message.
2.	The configuration in the Web interface restricts Caller ID.	Verify that the 'Presentation' field in the Web interface's 'Source Phone Number Manipulation Table for IP -> Tel Calls' page (Web path SW Ver. 5.2: Protocol Management menu > Manipulation Tables submenu > Tel to IP Source Numbers; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > Manipulation Tables submenu > Source Number Tel to IP) is not set to "Restricted".
3.	Incorrect Caller ID and Presentation is sent to the PBX.	Verify that the correct message (Caller ID and presentation) is sent to the PBX, by performing the following: 1 Open the Syslog. 2 Verify that the following message received: `pstn send --> PlaceCall: Trunk:0 BChannel:19 ConnID:0` **`SrcPN=4247`** `SrcSN= DstPN=90547533330 DstSN= SrcNT=0 SrcNP=0` **`SrcPres=0`** `SrcScrn=0 DstNT=0 DstNP=0 ServiceCap=M RdrctNum= RdNT=0 RdNP=0 RdPres=0 RdScrn=0 RdRsn=-1 Excl=1 Display= IE= UUIE=0,, CLIRReason:-1 OrigPN= OLI=-1`

6 Voice Quality

This section discusses troubleshooting for voice quality:

- "How Do I Troubleshoot Distorted Voice" on page 43
- "How Do I Troubleshoot Voice Echo" on page 44
- "How Do I Troubleshoot Voice Delay" on page 45

6.1 How Do I Troubleshoot Distorted Voice

Table 6-1: Distorted Voice Troubleshooting

	Possible Cause	Solution
1.	Problem at remote UA (not at the device).	If the coder used is G.711, verify whether the distortion is caused by the remote UA and not the device. You can perform this by running Wireshark (refer to "Wireshark Network Sniffer" on page 69) and checking the RTP streams (i.e., listen to the actual voice if G.711 is used). If the distortion occurs before it is received by the device, then the cause of the problem is at the remote UA. In this case, notify your network administrator. If the voice is fine before it arrives at the device, then the cause of the problem is at the device. In this case, follow the subsequent troubleshooting procedures in this table.
2.	Mismatch between the protocol type (E1/T1) and the selected PCM encoder. **Note:** Only for digital interfaces.	A common problem that usually occurs when the device is initially installed is that there is a mismatch between the protocol type (E1 or T1) and the selected PCM encoder (in the Web interface's 'TDM Bus Settings' page - Web path SW Ver. 5.2: Advanced Configuration menu > TDM Bus Settings; Web path SW Ver. 5.4 and later: Configuration tab > TDM Configuration menu > TDM Bus Settings). When E1 is used, the PCM Law Select must be set to A-law. When T1 is used, it must be set to Mu-law.
3.	Incorrect coefficients defined. **Note:** Only for FXO interfaces.	Verify that the correct coefficients are defined (using the *ini* file parameter CountryCoefficients).
4.	A Coefficient file has not been loaded to the device. **Note:** Only for FXS interfaces.	Verify that a coefficient file is loaded to the device. To load a coefficient file to the device, refer the *User's Manual*.

5.	Occurrence of RTP packet loss.	Verify that there is no RTP packet loss. Packet loss higher than 3% results in poor voice quality.
		To check whether RTP packet loss occurs, perform one of the following:
		▪ Syslog trace - search for the following message:
		`WARNING: PL:`
		`After the PL, the Syslog message indicates the number of missing packets.`
		▪ In Wireshark - Statistics > RTP > Stream Analysis.

6.2 How Do I Troubleshoot Voice Echo

Before you start debugging echo problems, you should first note that when the echo is heard by a user that is connected directly to the device – it does not indicate any problem on the device itself, the problem is in the echo canceller at the remote UA. A problem exists on the device only when echo is heard by the remote UA.

Table 6-2: Voice Echo Troubleshooting

Possible Cause		Solution
1.	Acoustic echo (interference) from extraneous sources.	Verify that there is no acoustic distortion and interference caused from equipment located near to the phone such as speaker phones, headsets, cellular phones, and talkers. If so, relocate them to separate rooms (acoustic echo isn't removed by the device itself).
2.	The device is not running the latest software version.	Verify that the device is running an updated software version.
3.	The clocks are not synchronized. **Note:** Only for digital interfaces.	Verify that the clocks are synchronized. One indication of echo caused by clock drifts is that the echo appears and disappears in the middle of the call. To verify that there are no clock drifts, refer to "How Do I Check for E1/T1 Clock Slips" on page 15.
4.	Echo cancellation is not enabled on the device.	Verify that the *ini* file parameter EnableEchoCanceller is set to 1. If Profiles are configured, ensure that this parameter is also set.
5.	The tail length of the echo canceller is configured too short.	Increase the echo canceller's length to 64 msec (setting the *ini* file parameter MaxEchoCancellerLength to 11). For digital gateways only: If this new setting still doesn't help, change it to 128 msec (MaxEchoCancellerLength is set to 22). Note that when 128-msec tail length is used, the channel capacity might be reduced (refer to the *User's Manual*).
6.	The echo canceller does not handle echo occurring at the beginning of a call.	When the echo is only at the beginning of the call, set the *ini* file parameter EchoCancellerAggressiveNLP to 1. This parameter enables the Aggressive NLP at the first 0.5 second of the call.
7.	High jitter buffer delay.	Modify the jitter buffer parameters (as shown below) of the device that hears the echo (not the device that doesn't cancel the echo). When the jitter is reduced, the existing echo is less conspicuous. ▪ DJBufOptFactor = 10 ▪ DJBufMinDelay = 10
8.	The received (Tel-to-IP) signal level settings have been modified from default settings.	Verify that the parameter InputGain is set to default (i.e., 0 dB).
9.	The level configured for the transmitted (IP-to-Tel) signal is too high.	Reduce the voice gain control, by setting the *ini* file parameter VoiceVolume to -3 or -6 dB in the device that hears the echo.
10.	The specific analog phone is not working properly.	Verify that echo exists when using different analog circuits (e.g. different telephones).

	Possible Cause	Solution
11.	The incoming signal has a DC offset. **Note:** Only for analog interfaces.	Enable the DC removal option (set the *ini* file parameter ECDCRemoval to 1).
12.	None of the above troubleshooting resolves the problem.	If you have verified all the above solutions and still experience echo, send AudioCodes Technical Support the following information and traces: ▪ Accurate and complete network diagram including all network components between the two end connections. ▪ The device's *ini* file. ▪ An accurate description of the echo problem (how often it appears, how long, etc.). ▪ PCM recordings in G.711, using the same equipment where the echo problems occurred. Refer to "CLI Debug Recording" **on page 72** for information on making PCM recordings. Note the following: ✓ The call duration should be at least 30 seconds. ✓ Both talkers should be physically separated (in different rooms). ▪ When the device includes several concurrent calls, there is a need to locate a specific call in a DSP recording. Therefore, in addition to the above, provide details of the problematic call (CDR, phone numbers, etc.) and a Syslog trace.

6.3 How Do I Troubleshoot Voice Delay

Delay is when each component in the path (such as sender, network, and receiver) adds delay. ITU-T G.114 recommends 150 msec as maximum desired latency to achieve high voice quality.

Jitter-Variable delay is caused when voice packets suffer different transit delays, causing variation in arrival times at the receiver. It is calculated based on inter-arrival time of successive packets and minimized by buffering voice at the receiver for a period longer than expected delay variation.

Table 6-3: Voice Delay Troubleshooting

Possible Cause		Solution
1.	A high round-trip time when pinging the remote UA.	Verify that that round trip time for pinging the remote UA is less than 350 msec. Refer to "How Do I Ping a Network Entity from the Device" on page 10.
2.	Delay caused by network condition.	Verify your network condition, by contacting your network administrator.
3.	None of the above.	If all the above is functioning properly, contact AudioCodes Technical Support team.

7 Call Disconnect

This section discusses troubleshooting for call disconnect:

- "Why Doesn't the FXO End a PBX/PSTN Call" on page 47
- "Why Do Calls Randomly Disconnect?" on page 49
- "Why Don't Calls Disconnect upon ISDN Disconnect Message" on page 49
- "Why Does the PBX/PSTN Disconnect IP-to-Tel Calls" on page 50

7.1 Why Doesn't the FXO End a PBX/PSTN Call

A common issue is that a call from a PBX that is connected to the FXO device is not disconnected by the device and the voice channel remains open and a BYE message is not sent to the IP. This is because the device has not been properly configured to recognize the disconnection signaling that is used by the PBX.

Tip: When this occurs, there is no need to reset the device. Instead, access the Web interface's Home page of the device and click the channel that is still open. Select the option ‘Reset Channel’ to release the channel.

Table 7-1: Unterminated PBX FXO Call Troubleshooting

	Possible Cause	Solution
1.	The device is not correctly configured to identify the disconnection signaling used by the PBX.	The following disconnection methods are supported: ▪ **Detection of polarity reversal / current disconnect:** This is the recommended method. The call is immediately disconnected after polarity reversal or current disconnect is detected on the Tel side (assuming the PBX / CO produces this signal). Relevant parameters: EnableReversalPolarity, EnableCurrentDisconnect, CurrentDisconnectDuration, CurrentDisconnectDefaultThreshold, and TimeToSampleAnalogLineVoltage. ▪ **Detection of Reorder / Busy / Dial tones:** The call is immediately disconnected after Reorder / Busy / Dial tone is detected on the Tel side (assuming the PBX / CO generates this tone). This method requires that the correct tone frequencies and cadence are defined in the Call Progress Tones (CPT) file. If these frequencies are unknown, you can detect them using the procedure described below and configure them in the CPT file. This method is slightly less reliable than the previous one. Relevant parameters: DisconnectOnBusyTone and DisconnectOnDialTone. ▪ **A special DTMF code:** A digit pattern that when received from the Tel side, indicates to the device to disconnect the call. Relevant parameter: TelDisconnectCode. ▪ **Detection of silence:** The call is disconnected after silence is detected on both call directions for a user-defined time. The call isn't disconnected immediately; therefore, this method should only be used as a backup mode. Relevant parameters: EnableSilenceDisconnect and FarEndDisconnectSilencePeriod.

To detect the frequency and cadence of reorder/busy tones sent by a PBX, you can perform one of the following:

- Create a new CPT file, using the CPTwizard (refer to "CPTWizard" on page 77).
- Identify the busy or re-order tones used by the PBX - refer to the procedure below.

➢ To detect the frequency and cadence of the reorder or busy tones sent by the PBX:

1. Make a call (using G.711) between the FXO device, which is connected to the PBX, and a remote entity in the IP network.
2. Capture the call using a network sniffer such as Wireshark (refer to "Wireshark Network Sniffer" on page 69).
3. Disconnect the call from the PBX side, and then wait approximately 30 seconds before stopping the Wireshark recording.

4. In the network trace, locate the RTP stream sent from the FXO, and then save the RTP payload on your PC as a **.pcm* file, by clicking **Save Payload** (Statistics menu > RTP > Stream Analysis. (**Note:** Ensure that you select the 'forward' option.)
5. Open the **.pcm* file in a voice recording utility such as CoolEdit.
6. Locate the tone that the PBX played to indicate the disconnected call (if such a tone exists) and locate the attributes of the tone -- its frequency and interval (on / off time).
7. In the Call Progress Tones file, add a new Reorder Tone with the attributes you found in the previous step. Ensure that you update the numbers of the successive tones and the total number of tones in the beginning of the file.
8. Create a Call Progress Tones **.dat* file using the DConvert Utility.
9. Load the new file to the device, and then reset the device.

7.2 Why Do Calls Randomly Disconnect?

Table 7-2: Random Call Disconnect Troubleshooting

	Possible Cause	Solution

1.	A common reason for call disconnection is the broken connection mechanism, which is enabled by default. This mechanism causes the device to release the call if RTP packets are not received within a user-defined time. This occurs when the remote SIP UA does not send RTP packets during silence periods.	Before resolving this issue, verify that the cause for the call disconnection is the Broken Disconnect mechanism, by searching for the following in the syslog:
		`recv <-- acEV_BROKEN_CONNECTION, Ch:30`
		`push LOCAL_MANUAL_DISCONNECT_CALL_EV #30:LOCAL_MANUAL_DISCONNECT_CALL_EV(Trunk: 0 Conn:-100 Bchannel:31 TpEv=38)`
		`#30:LOCAL_MANUAL_DISCONNECT_CALL_EV`
		To resolve the problem, perform one of the following:
		▪ Disable this mechanism, by setting the *ini* file parameter DisconnectOnBrokenConnection to 0.
		▪ Increase the broken connection timeout, by using the ini file parameter BrokenConnectionEventTimeout.

7.3 Why Don't Calls Disconnect Upon ISDN Disconnect Message

Table 7-3: Calls Not Disconnected Upon Receipt of ISDN Disconnect Troubleshooting

	Possible Cause	Solution
1.	The device is configured to disconnect calls when a Disconnect message is received from the ISDN, before a Connect message is received.	By default, when the device receives a Disconnect message with Progress Indicator (PI) from the ISDN before a Connect message is received, the device sends a SIP 183 response, enabling the PSTN to play a voice announcement to the IP side. The call is disconnected only after 30 seconds or if a Release Complete message is received from the PBX. This device configuration can be changed, by setting the *ini* file parameter PIForDisconnectMsg_ID to 0 (where ID depicts the trunk number). In this setting, the call is immediately released by the device.

7.4 Why Does the PBX Disconnect IP-to-Tel Calls

Table 7-4: PBX Disconnects IP-to-Tel Calls Troubleshooting

	Possible Cause	Solution
1.	The device is not configured to send a Q.931 Connect ACK message immediately upon receipt of a Connect message.	Some PBXs expect the device to send a Q.931 Connect ACK message immediately upon receiving a Connect message. By default, the device doesn't send this message. Configure the device to send a Connect ACK message in response to a Connect message. You can perform this using an *ini* file or the Web interface: ▪ Ini file: Set the *ini* file parameter ISDNIBehavior to 128. ▪ Web interface: **a.** Stop the Trunk, using the 'Trunk Settings' page (Web path SW Ver. 5.2: Advanced Configuration menu > Trunk Settings; Web path SW Ver. 5.4 and later: Configuration tab > PSTN Settings menu > Trunk Settings). **b.** From the 'Trunk Settings' page, open the 'Q.931 Layer Response Behavior' page, and then set 'SEND USER CONNECT ACK' to 1. **c.** In the 'Trunk Settings' page, apply the Trunk settings. **Notes:** ▪ Applicable only to Euro-ISDN User side. ▪ Network side always sends a CONNECT ACK.

8 Fax and Modem

This section discusses troubleshooting for fax and modem calls.

8.1 Why Do Fax Sessions Fail

Each fax session begins with a regular voice call setup process. Only after this voice channel has been successfully established does fax negotiation begin.

Table 8-1: Fax Failure Troubleshooting

	Possible Cause	Solution
1.	Voice call setup prior to fax negotiation failed.	Verify normal SIP/VoIP call setup establishment (refer to "Call Setup" on page 19).
2.	Incorrect Fax transport type.	Ensure that the fax transport type configured for the device is the same fax transport type supported by the remote gateway or UA. The supported fax transport methods to send fax over IP include the following: ▪ T.38 fax relay - fax signals are sent using the T.38 protocol. Relevant parameters include the following: ✓ IsFaxUsed (= 1 for switching to T.38 mode using SIP Re-INVITE; = 0 for automatically switching to T.38 mode without SIP Re-INVITE) ✓ FaxTransportMode = 1 (only for automatically switching to T.38 mode without SIP Re-INVITE) ✓ FaxRelayEnhancedRedundancyDepth ✓ FaxRelayRedundancyDepth ✓ FaxRelayECMEnable ✓ FaxRelayMaxRate ▪ Fax bypass - a proprietary method that uses a high bit-rate coder. Relevant parameters include the following: ✓ IsFaxUsed = 0 ✓ FaxTransportMode = 2 ✓ V21ModemTransportType = 2 ✓ V22ModemTransportType = 2 ✓ V23ModemTransportType = 2 ✓ V32ModemTransportType = 2 ✓ V34ModemTransportType = 2 ✓ BellModemTransportType = 2 ✓ FaxModemBypassCoderType ✓ FaxBypassPayloadType ✓ ModemBypassPayloadType ✓ FaxModemBypassBasicRTPPacketInterval ✓ FaxModemBypassDJBufMinDelay ▪ NSE Cisco's Pass-through bypass mode for fax. Relevant parameters include the following: ✓ IsFaxUsed = 0 ✓ FaxTransportMode = 2 ✓ NSEMode = 1 ✓ NSEPayloadType = 100 ✓ V21ModemTransportType = 2 ✓ V22ModemTransportType = 2 ✓ V23ModemTransportType = 2 ✓ V32ModemTransportType = 2

Possible Cause		Solution
		✓ V34ModemTransportType = 2 ✓ BellModemTransportType = 2 ▪ Transparent - sends the fax signal in the current voice coder. Relevant parameters include the following: ✓ IsFaxUsed = 0 ✓ FaxTransportMode = 0 ✓ V21ModemTransportType = 0 ✓ V22ModemTransportType = 0 ✓ V23ModemTransportType = 0 ✓ V32ModemTransportType = 0 ✓ V34ModemTransportType = 0 ✓ BellModemTransportType = 0 ✓ CoderName ✓ DJBufOptFactor ✓ EnableSilenceCompression ✓ EnableEchoCanceller ▪ Transparent with events - sends the fax signal in the current voice coder with adaptations. Relevant parameters include the following: ✓ IsFaxUsed = 0 ✓ FaxTransportMode = 3 ✓ V21ModemTransportType = 3 ✓ V22ModemTransportType = 3 ✓ V23ModemTransportType = 3 ✓ V32ModemTransportType = 3 ✓ V34ModemTransportType = 3 ✓ BellModemTransportType = 3 ▪ G.711 Transport - switches to G.711 when fax is detected. Relevant parameter includes the following: IsFaxUsed = 2. ▪ Fax fallback to G.711 if T.38 is not supported. Relevant parameter includes the following: IsFaxUsed to 3. For detailed information on these supported fax transport types, refer to the device's *User's Manual*.
3.	The device does not send a SIP Re-INVITE message in T.38 mode.	Determine the side that initiates the fax session. By default, the device that is connected to the called fax machine sends a Re-INVITE with T.38 when it detects a Preamble signal. Therefore, a device on the calling fax side does not enter T.38 mode until it receives a Re-INVITE from the called fax. Therefore, ensure that the remote device sends such a message. If the remote device doesn't send a Re-INVITE when it is on the called fax side, configure the device to send a Re-INVITE also when it is on the calling fax side, by setting the *ini* file parameter CNGDetectorMode to 2.

Possible Cause		Solution
4.	The device at the calling fax side is located behind a firewall that blocks incoming T.38 packets on ports that have not yet received T.38 packets from the internal network.	When the device on the calling fax side is located behind a firewall that blocks incoming T.38 packets on ports that have not yet received T.38 packets from the internal network, the fax will fail. To overcome this problem, perform the following: 1 Configure the device so that when the Calling tone (CNG) is detected by the device on the calling fax side, CNG packets are sent to the called fax side in T.38 mode. These packets open the firewall and allow T.38 packets to be received (CNGDetectorMode is set to 1). 2 Use the same port as the RTP port to send and/or receive T.38 packets. **Note:** This method must be supported by the remote device as well. T38UseRTPPort is set to 1.
5.	Profile settings overriding device configurations.	If Profiles have been configured, ensure that they are correct as Profile definitions override the device definitions.
6.	The coefficient file is not loaded to the device. **Note:** Only for FXS interfaces.	Verify that a coefficient file is loaded to the device. If not, then load this file using the Web interface.
7.	Clock slippage (clock slips) between devices. **Note:** Only for Digital interfaces.	For troubleshooting clock slips, refer to "How Do I Check for E1/T1 Clock Slips" on page 15.

8.	RTP packet loss occurs in the network.	Verify that there is no RTP packet loss. Packet loss greater than 3% results in poor voice quality. To check whether RTP packet loss occurs, perform one of the following:
		▪ **Syslog trace:** Search for the following message:
		`WARNING: PL:`
		`After the PL, the Syslog message indicates the number of missing packets.`
		▪ **Wireshark:** Statistics > RTP > Stream Analysis.
		When T.38 is used, you can try to increase the number of times each fax relay payload is retransmitted to the network, using the *ini* file parameter FaxRelayRedundancyDepth.

9.	None of the above.	If the problem is still present, contact AudioCodes Technical Support team and provide them with the following information: ▪ INI file ▪ Debug level 5 Syslog trace ▪ A PCM recording

Reader's Notes

9 Call Transfer

This section discusses troubleshooting for call transfer:

- "Why is a Call Transfer by the FXO Terminated" on page 55
- "Why Can't I Transfer a Call Between FXS Interfaces" on page 55

9.1 Why Does PBX Terminate Call Transfer by the FXO Device

After receiving a SIP REFER message from the IP side (to initiate call transfer), the FXO device performs the following in chronological order:

1. Sends a hook-flash to the PBX.
2. Dials the digits (received in the SIP Refer-To header) to the PBX.
3. When blind transfer is used, for example, the device immediately drops the FXO line (on-hook).
4. The PBX performs the call transfer internally.

Table 9-1: FXO Call Transfer Troubleshooting

	Possible Cause	Solution
1.	The PBX mistakenly recognizes the Hook-Flash sent by the device as an on-hook signal and then terminates the call.	When the PBX mistakenly recognizes the hook-flash as an on-hook signal, it terminates the call. The scenario is as follows: 1 The FXO device sends a hook-flash to the PBX. However, since the off time (of the hook-flash) is too long, the PBX recognizes this as an on-hook and releases the call. When the FXO device completes the hook-flash signal by off-hooking, the PBX assumes that this is a new call. 2 The FXO device dials the digits (that are received in the SIP Refer-To header) after which the required phone starts ringing. 3 The FXO device then drops the line and the remote phone stops ringing. Therefore, to solve this problem, decrease the length of the hook-flash signal that is generated by the FXO device, using the *ini* file parameter FlashHookPeriod.

9.2 Why Can't I Transfer a Call Between FXS Interfaces

Troubleshooting for call transfer between FXS interfaces can include the following issues:

- The call disconnects between the initial call parties (e.g., A and B) when one of the parties (e.g., A) presses the Flash Hook button to try transfer the call to another party (e.g., C).
- No secondary dial tone is played when one party (e.g., A) tries to transfer a call (with, for example, B) to another party (e.g., C), by pressing the Flash Hook button. The call between the two initial call parties (e.g., A and B) continues as usual.

Table 9-2: FXS Call Transfer Troubleshooting

Possible Cause		Solution
1.	The time for detecting a hook-flash signal is too short or too long.	To re-define the minimum time (in msec) for detection of a hook-flash event, use the parameter MinFlashHookTime. To define the maximum hook-flash detection period, use the *ini* file parameter FlashHookPeriod.

10 IP Voice Mail and Unified Messaging

This section deals with troubleshooting for IP voice mail and Unified Messaging:

- "I Cannot Retrieve Voice Mail Messages" on page 57
- "Why Does IP Voice Mail Request My Extension Number for Retrieving Voice Mail" on page 57
- "I Cannot Leave Voice Mail Messages" on page 58
- "Message Waiting Indication Does Not Function" on page 59
- "I Cannot Transfer Calls to Users in Unified Messaging" on page 60

10.1 I Cannot Retrieve Voice Mail Messages

Table 10-1: Voice Mail Retrieval Troubleshooting

	Possible Cause	Solution
1.	The Tel-to-IP call setup is not configured correctly.	Ensure that the device receives a call from the PBX and that it sends a SIP INVITE message to the IP voice mail system. If it does not, refer to troubleshooting for Tel-to-IP calls (refer to "How Do I Troubleshoot Tel-to-IP Call Setup" on page 27).

10.2 Why Does IP Voice Mail Request My Extension Number for Retrieving Voice Mail

The correct operation for retrieving IP voice mail is for the user to enter only a PIN number. However, the IP voice mail system may erroneously request the user's extension number in addition to the PIN number for access to voice mail.

Table 10-2: Extension Number for Voice Mail Retrieval Troubleshooting

	Possible Cause	Solution
1.	The PBX does not send calling number information to the device.	The solution to this problem depends on the type of voice mail integration: ▪ Using DTMF: **a.** Use the Syslog to verify that after the device seizes the line, the PBX sends a digit pattern that includes the calling number information. **b.** Verify that the correct digit patterns are configured for the parameters 'Internal Call Digit Pattern' and 'External Call Digit Pattern' on the 'Voice Mail Setting' page (Web path SW Ver. 5.2: Protocol Management menu > Advanced Applications submenu > Voice Mail; Web path SW Ver. 5.4 and later: Configuration tab > Advanced Applications menu > Voice Mail Settings). ▪ Using SMDI: Use the Syslog to verify that the PBX sends an SMDI message which includes the calling number. ▪ Using QSIG: Use the Syslog to verify that the calling number is included in the SETUP message received from the PBX.

10.3 I Cannot Leave Voice Mail Messages

Table 10-3: Leaving Voice Mail Troubleshooting

	Possible Cause	Solution
1.	There is no SIP Diversion header in the outgoing INVITE message sent to the IP voice mail system.	Ensure that the voice mail interface is configured according to your deployment, on the Web interface's 'Voice Mail Setting' page (Web path SW Ver. 5.2: Protocol Management menu > Advanced Applications submenu > Voice Mail; Web path SW Ver. 5.4 and later: Configuration tab > Advanced Applications menu > Voice Mail Settings).
2.	The digit patterns are not configured (or configured incorrectly) when the voice mail interface is DTMF.	When the device detects a ringing signal, it seizes the line and collects the received DTMF digits sent by the PBX. The collected digits are compared against the user-defined patterns (configured on the Web interface's 'Voice Mail Setting page) to extract the Redirect Number. Ensure that all digit patterns are configured according to the PBX specifications. You can use the Syslog to identify the DTMF patterns sent by the PBX and compare it with the digit patterns configured on the 'Voice Mail Settings' page.
3.	The serial cable is not working when the voice mail interface is SMDI.	When routing a call (to the voice mail system), the PBX sends an SMDI message to the device (through an RS-232 connection), informing the device of the line being used, the type of call being forwarded, and information about the source and destination of the call. 1 Disconnect the serial cable from the device and connect the cable to a PC. Setup a communication link between the PC and PBX, using HyperTerminal. Ensure that an SMDI message is displayed on the PC. 2 If an SMDI message is displayed on the PC, re-connect the cable to the device and check whether the SMDI message appears in the Syslog. 3 Ensure that the SerialBaudRate, SerialData, SerialParity, SerialStop and SerialFlowControl parameters are configured correctly (defaults are 9600, 8, None, 1, and None respectively). 4 Verify that the Endpoint/Trunk phone number configured on the device is identified with the line/trunk phone numbers on the PBX. This number should appear in the SMDI message 'line identifier' field.
4.	The SMDI variant is not configured correctly when the voice mail interface is SMDI.	Ensure that the parameter 'Enable SMDI' is configured according to the PBX SDMI variant. Modifying this parameter takes effect only after a device reset.
5.	The SMDI time out is too short when the voice mail interface is SMDI.	The SMDITimeOut parameter determines the time (in msec) for which the device waits for an SMDI Call Status message before or after a SETUP message is received. Increase this parameter to a value that is greater than the period between receiving the SETUP message and receiving the SMDI message.
6.	The PBX does not send the redirect number when the voice mail interface is QSIG.	Use the Syslog to verify that the PBX sends the ISDN's Facility IE (ISDN_FACILITY_INFORMATION_ELEMENT) with the redirect number.

10.4 Message Waiting Indication Does Not Function

Table 10-4: MWI for Voice Mail Troubleshooting

	Possible Cause	Solution
1.	The IP voice mail system does not send SIP NOTIFY messages to the device.	Use Syslog or Wireshark to verify that the device receives SIP NOTIFY messages from the IP voice mail system (for example, if you are implementing Microsoft Exchange Server 2007, the MWI service is provided by Geomant's MWI2007 application and therefore, the NOTIFY is sent from this application). The NOTIFY message should include the following headers: ▪ Messages-Waiting: yes or no ▪ Message-Account: Extension number@GW IP address ▪ Voice-Message: number of waiting message If NOTIFY messages are not received from the IP voice mail system, report this problem to the IP voice mail system administrator.
2.	The Message Waiting Inidication (MWI) digit pattern is not configured when using DTMF voice mail interface.	Ensure that the parameter EnableMWI is set to 1 and that the digit patterns of the MWI on and off codes are configured (using the Web interface's 'Voice Mail Setting page - Web path SW Ver. 5.2: Protocol Management menu > Advanced Applications submenu > Voice Mail; Web path SW Ver. 5.4 and later: Configuration tab > Advanced Applications menu > Voice Mail Settings), according to the PBX's requirements.
3.	The MWI parameters are not configured correctly when using QSIG voice mail interface.	Ensure that the following parameters are configured as follow: ▪ ISDNIBehavior = 1073741824 (for Integer coding) or 0 (for Object Identifier coding) ▪ SubscriptionMode = 1 ▪ EnableMWI = 1 ▪ DefaultNumber = 'serveduser'
4.	MWI is not enabled on the device when using SMDI voice mail interface.	Ensure that the parameter EnableMWI is set to 1.

10.5 I Cannot Transfer Calls to Users in Unified Messaging

Table 10-5: Call Transfer for UM Troubleshooting

	Possible Cause	Solution
1.	The PBX does not detect hook-flash signals when using DTMF or SMDI voice mail interface.	Ensure that the following has been configured: ▪ LineTransferMode = 1. ▪ For FXO interfaces only: Modify the parameter FlashHookPeriod according to the PBX requirements. This parameter determines the hook-flash generation period (in msec). The valid range is 300 to 1,500 (default is 400). ▪ For digital interfaces only: Ensure that the TrunkTransferMode_x = 3 (for CAS Normal) or 1 (for CAS NFA).

11 Common Web, SNMP and ini File Issues

This section discusses common Web, SNMP, and *ini* file issues.

11.1 How Do I Restore Web Interface Username and Password Without Losing Configuration

➢ **To restore the Web Interface's user name and password without losing existing configuration:**

- If your configuration is backed up as an *ini* file, include the parameter ResetWebPassword=1 to the *ini* file and load it to the device using BootP; the user name and password will be set to their default values ('Admin' and 'Admin' respectively).
- If you don't have a backup *ini* file, load the parameter ResetWebPassword to the device, using SNMP. Set the acSysGenericINILine to ResetWebPassword = 1. Reset the device, using SNMP with the burn-to-FLASH option (refer to "How Do I Reset the Device Via SNMP" on page 62).
- You can always restore the parameters of the device to their default values, using the reset button (refer to the device's *User's Manual* for more information) and re-configure the device.

11.2 How Do I Obtain the Complete ini File

The *ini* file containing all your device's parameter configurations is located on the FAE page. It is protected by a password mechanism that is different from the password used to access the Web Interface. This password can be created by AudioCodes based on the device's IP address. However, there is no need to use the Complete *ini* file since it includes internal parameters that (if changed) can affect the normal functioning of the device. All necessary information can be obtained from the regular *ini* file.

11.3 Where Do I Place a Parameter in the ini File

You can add a parameter anywhere in the *ini* file; its location in the *ini* file does not affect its functioning. When obtaining the device's *ini* file from the Web interface, the saved *ini* file groups the parameters into sections (such as [Voice Engine Params]); this division is simply for convenience.

11.4 How Can I Update the ini File Via SNMP

Most of the *ini* file parameters have a specific OID and can be updated directly using SNMP. The *ini* file parameters that don't have a specific OID can be set using acSysGenericINILine. Use the format, parameter name = value (this format doesn't apply to complex table parameters). For the changes to take effect, the device must be reset with the burn-to-FLASH option (refer to "How Do I Reset the Device Via SNMP" on page 62).

11.5 How Do I Obtain the ini File Via SNMP

It is not possible to obtain (Get) the *ini* file directly using SNMP. The only available method is to trigger the auto update mechanism (that uses an HTTP server, for example). The relevant parameters are located under cSysHTTPClient.

11.6 How Do I Change Web Username and Password Via SNMP

➢ To change the Web login user name and password, using SNMP:

1. By default, you cannot change the Web interface's user name and password, using SNMP. To enable this option, perform one of the following:
   - Set the parameter WEBPasswordControlViaSNMP = 1 in the *ini* file (or in the AdminPage).
   - Using SNMP, set acSysGenericINILine to WEBPasswordControlViaSNMP = 1 and then reset the device with FLASH burn (set acSysActionSetResetControl to 1 and acSysActionSetReset to 1).
2. Change the user name and/or password using the SNMP table acSysWEBAccessEntry. Use the following format:
   - Username acSysWEBAccessUserName: old/pass/new
   - Password acSysWEBAccessUserCode: username/old/new

11.7 How Do I Reset the Device Via SNMP

➢ To reset the device using SNMP:

1. Determine the reset method you want to apply to the device, using the parameter acSysActionSetResetControl.
2. Reset the device by setting the parameter acSysActionSetReset to 1. The available options are:
   - resetFromFlashAfterBurn(1) – resets the device and saves ('burns') the configuration to flash memory.
   - resetFromFlashNoBurn(2) - resets the device without 'burning' the configuration to flash.
   - resetFromBootP(3) – similar to a physical reset.

11.8 How Do I Force the Device to Send a SIP REGISTER via SNMP

➢ To force the device to send a SIP REGISTER message, using SNMP:

- Use the SNMP parameter h323GKRegister. This parameter performs the same operation as the **REGISTER / Un-REGISTER** buttons on the Web interface.

11.9 How Do I Remove/Insert Mediant 1000 Modules Via SNMP

The FRU (Field Replace Unit) via SNMP:

➢ To replace a module using SNMP:

1. Remove the module, by performing the following:
   a. Set the acSysModuleFRUaction with fruOutOfServiceAction(2), where the instance refers to the corresponding module.
   b. Check that the action succeeds by performing a Get of the value of acSysModuleFRUstatus with the same instance. The value should be moduleOutOfService(3.)
   c. There is no need to stop the trunks before setting the module to OutOfService. But, if one of the trunks on the module provides the clock (assuming that TDM Bus Clock Source = network and TDM Bus PSTN Auto Clock = disable), then you cannot remove this module. Therefore, before removing the module, you must change the clock reference to a trunk on a different module. The last digital module can always be removed even if it provides the clock reference.
2. Insert a module, by performing the following:
   a. Set the acSysModuleFRUaction with fruBackToServiceAction(3), where the instance refers to the corresponding module.
   b. Check that the action succeeds by performing a Get of the value of acSysModuleFRUstatus, with the same instance. The value should be moduleExistOk(2).

11.10 How Do I View PSTN Alarms Via SNMP

➢ To view PSTN alarms, using SNMP:

- The acTrunkStatusEntry table can be used to view the color and status (steady or blinking) of the E1/T1 LEDs that are located on the front panel of the device.
- The dsx1LineStatus table can be used to view Line Status of the interface. It contains loop back, failure, received alarm and transmitted alarms information.
- The AcDChannelStatus trap is sent to indicate a D-channel alarm.

11.11 How Do I Work with Row-Status

Generally, when working with Row-Status there are two modes:

- One-Shot mode - the EMS provides all information within one PDU and uses Create-And-GO.
- Dribble mode - the EMS must first send Create-And-Wait and thereafter the data. Active SET must be sent at the end of the process. For example, to add a row to the channelsEntry table (via a MIB browser), you need to perform the following:
  a. Set the channelRowStatus; the window 'Select Table Instance' is opened.

b. Close the window 'Select Table Instance'. After the window is closed, the 'set channelRowStatus' screen appears.

c. In the field 'OID to Set', select a new OID, and then in the field 'Value to Set', select option 5 (createandWait). After configuring the parameter of the new entry, set the channelRowStatus to 1 (Active).

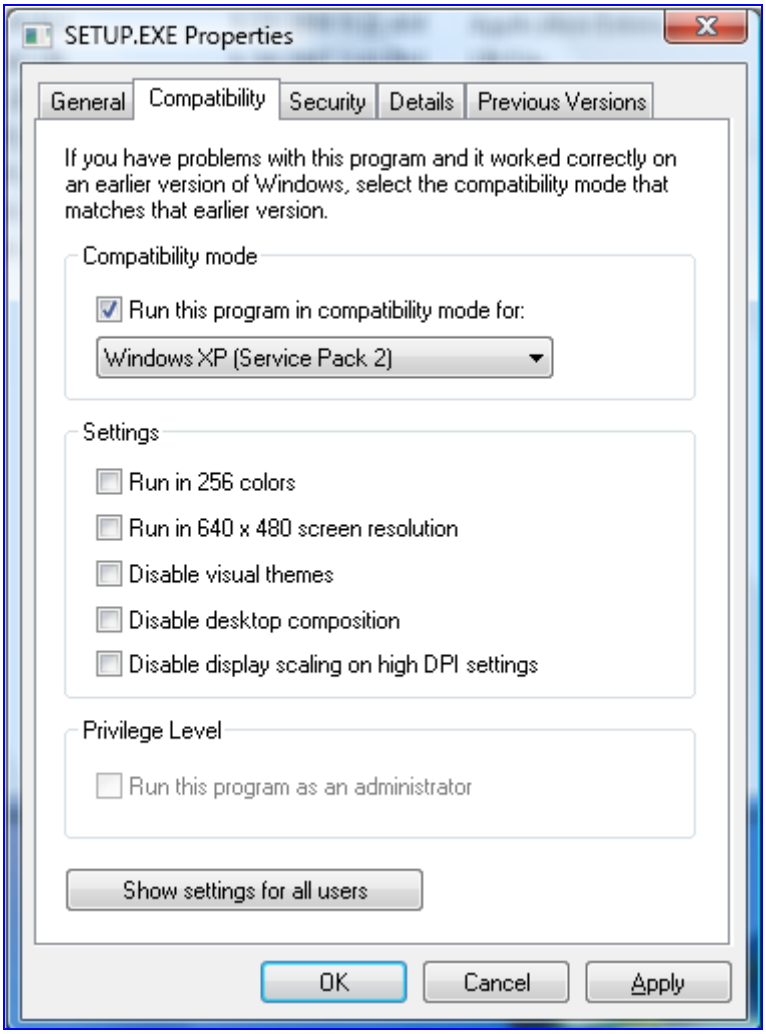
11.12 Why Doesn't BootP Install on Windows Vista

If you have problems installing BootP on your PC, follow the procedure below.

➢ To install the BootP application on a PC running Windows Vista:

1. Install BootP version BootP_2_3_0_12 or later.
2. Right click the *setup.exe* file, and then from the shortcut menu, choose **Properties**; the setup.exe Properties dialog box appears. Perform the following:
   a. Click the **Compatibility** tab.
   b. Under the Compatibility mode group, from the drop-down list, select "Windows XP", and then select the check box.

Figure 11-1: Properties Dialog Box for BootP Compatibility



12 Traffic Debug Analysis

This section discusses troubleshooting for debug troubleshooting:

- "Why Can't I Record the Device's Traffic" on page 65
- "Why Doesn't Wireshark Decode Messages" on page 65

12.1 Why Can't I Record the Device's Traffic

In most deployments, the device is connected to a switch and therefore, it isn't possible to record the network messages that are sent and received by the device. To overcome this issue, you can perform one of the following:

- Connect the PC and the device to the same hub. When a hub receives a packet (chunk) of data at the device's port, it transmits (repeats) the packet to all of its ports and, thus, to the other PC's that are connected to its ports.
- Use port mirroring - if you are using a switch (to which the device and PC are connected).
- Use Debug Recording (refer to "CLI Debug Recording" on page 72) for recording the traffic (the device duplicates the packets it transmits and receives, and then sends them to a user-defined destination).

12.2 Why Doesn't Wireshark Decode Messages

Follow the troubleshooting below when the Wireshark application (refer to "Wireshark Network Sniffer" on page 69) doesn't correctly decode the debug recording messages that are sent by the device.

Table 12-1: Wireshark Decoding Troubleshooting

	Possible Cause	Solution
1.	AudioCodes plugins for recording does not match the Wireshark software version.	For each Wireshark version there is a suitable set of AudioCodes plugins. Verify that you are using the correct plugins with your Wireshark software version: ▪ The plugins that are released with version 5.2 are relevant to Wireshark version 99.04. ▪ The plugins that are released with version 5.4 are relevant to Wireshark version 99.06. ▪ The plugins that are released with version 5.6 are relevant to Wireshark version 99.08. ▪ The plugins are backward compatible, thus, you can use Wireshark version 99.08.
2.	AudioCodes plugins for recording were not copied to the correct directory.	Verify that you copied the required AudioCodes plug-ins to the correct directory. In addition, ensure that you copy the tpncp.dat file from the 'Shared' directory.

Reader's Notes

13 Debugging Procedures

This section discusses debugging procedures:

- "Case Reporting Procedures" on page 67
- "Syslog" on page 68
- "Wireshark Network Sniffer" on page 69
- "CLI Debug Recording" on page 72

13.1 Case Reporting Procedures

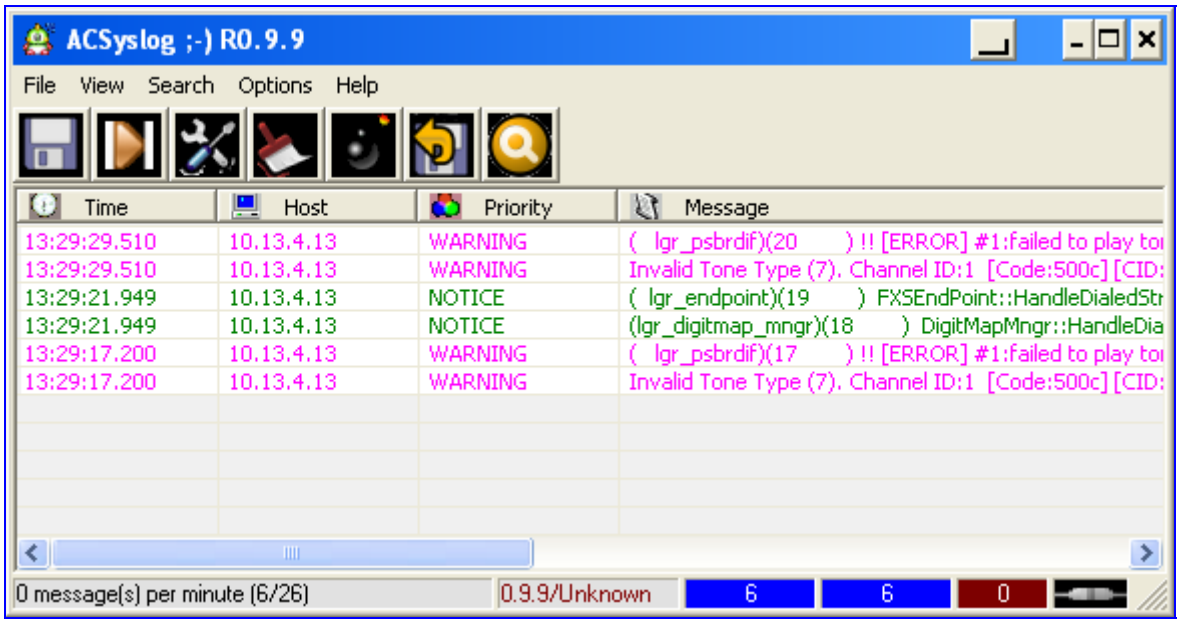
When reporting a problem to AudioCodes' Technical Support department, the following information should be provided:

- Basic information (required for all types of problems):
  - Problem description (nature of failure, symptoms, call direction, etc.)
  - Network diagram
  - *ini* configuration file (downloaded to your PC from the device, using the Web interface)
  - Syslog trace (without missing messages)
  - Unfiltered IP network trace using the Wireshark application
    (Note: If you are unable to collect all the network traffic, then at least collect the mandatory protocols SIP, RTP, and T38.)
- Advanced information (if required upon request):
  - PSTN message traces - for PSTN problems
  - Media stream traces - for problems related to voice quality, modem\fax, DTMF detection, etc.

13.2 Syslog

Syslog is a standard for forwarding log messages in an IP network. A syslog client, embedded in the device sends error reports/events generated by the device to a remote Syslog server using IP/UDP protocol. This information is a collection of error, warning and system messages that record every internal operation of the device. You can use the supplied AudioCodes proprietary Syslog server "ACSyslog" (shown in the figure below) or any other third-party Syslog server for receiving Syslog messages.

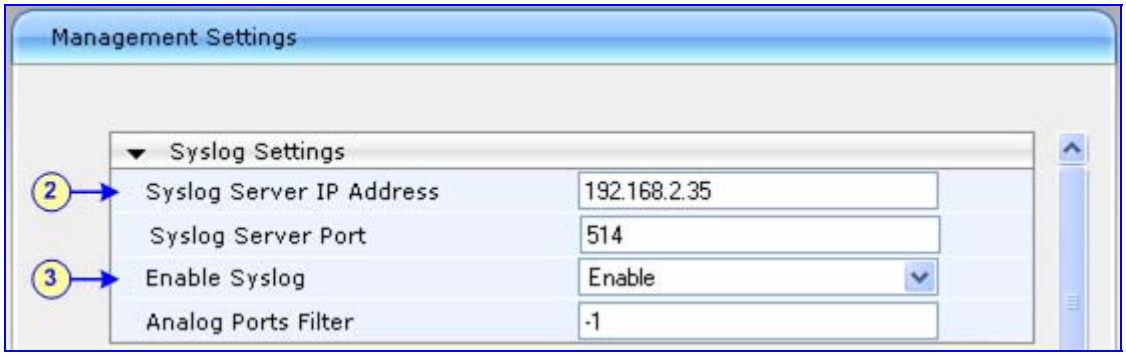
Figure 13-1: AudioCodes' Proprietary Syslog Server



➢ To activate the Syslog client on the device using the Web interface:

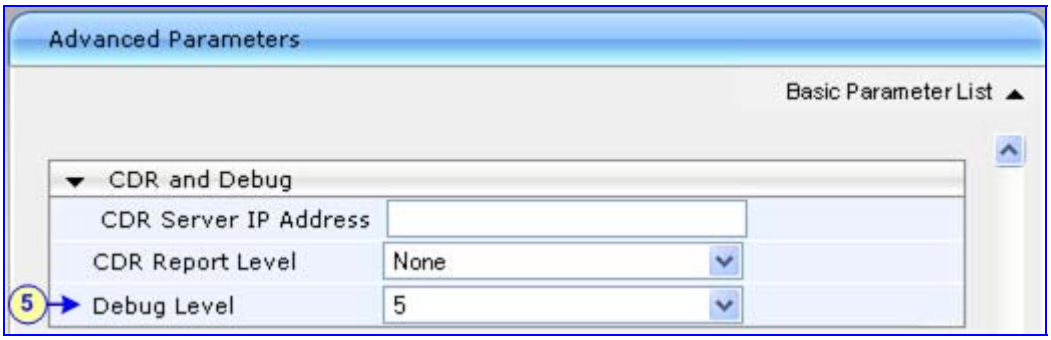
1. Open the Web interface's 'Management Settings' page (Web path SW Ver. 5.2: Advanced Configuration menu > Management Settings; Web path SW Ver. 5.4 and later: Management tab > Management Configuration menu > Management Settings).
2. In the 'Syslog Sever IP Address' field, enter the IP address of the Syslog server (*ini* file parameter SyslogServerIP).
3. From the 'Enable Syslog' drop-down list, select 'Enable' to enable the device to send syslog messages to a Syslog server (defined in Step 2).

Figure 13-2: Enabling Syslog



4. Open the Web interface 'Advanced Parameters' page (Web path SW Ver. 5.2: Protocol Management menu > Advanced Parameters submenu > General Parameters; Web path SW Ver. 5.4 and later: Configuration tab > Protocol Configuration menu > SIP Advanced Parameters submenu > Advanced Parameters).

Figure 13-3: Determining Debug Level



5. From the 'Debug Level' drop-down list, select '5' if debug traces are required.

To enable syslog reporting, using the *ini* file, load an *ini* file to the device with the following settings:

```
[Syslog]
SyslogServerIP = 192.168.2.35
EnableSyslog = 1
SyslogServerPort = 514
GWDebugLevel = 5
```

13.3 Wireshark Network Sniffer

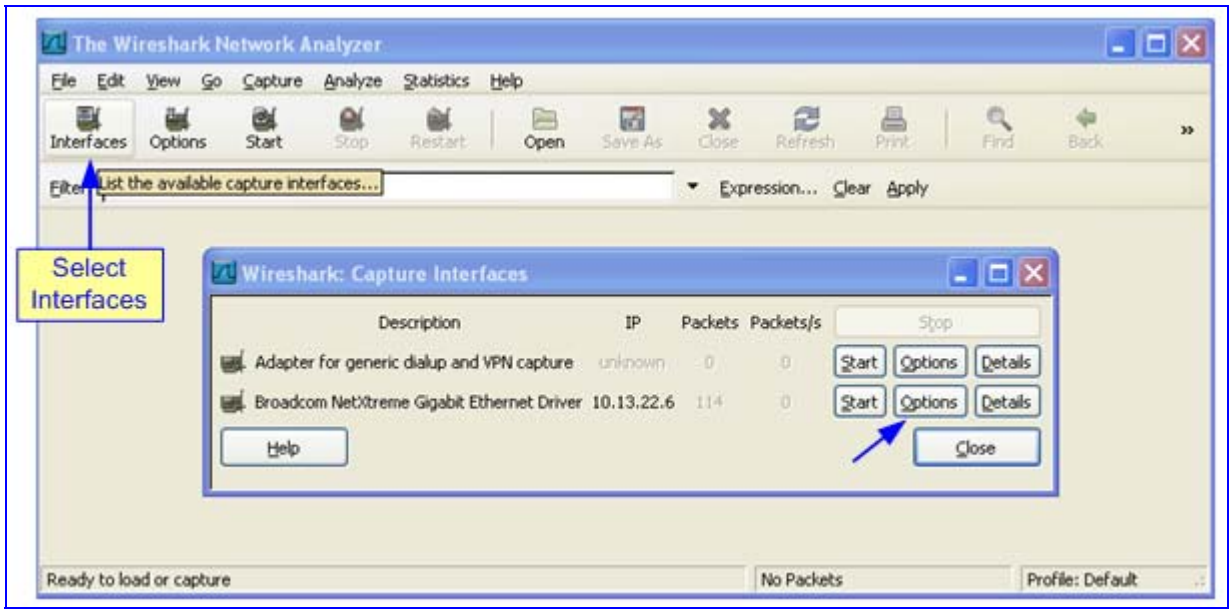
Wireshark is a freeware packet sniffer application that allows you to view the traffic that is being passed over the network. Wireshark can be used to analyze any network packets. Wireshark can also be used to analyze RTP data streams and extract the audio from the data packets (only for G.711). The audio can be saved as a *.pcm file.

➢ To record traffic that is sent to / from the device:

1. Install Wireshark on your PC. (You can download it from the following Web site: http://www.wireshark.org/.)
2. Connect the PC and the device to the same hub.
3. If you are using a switch, use a switch with port mirroring for the port to which the Wireshark is connected.
4. Start Wireshark.

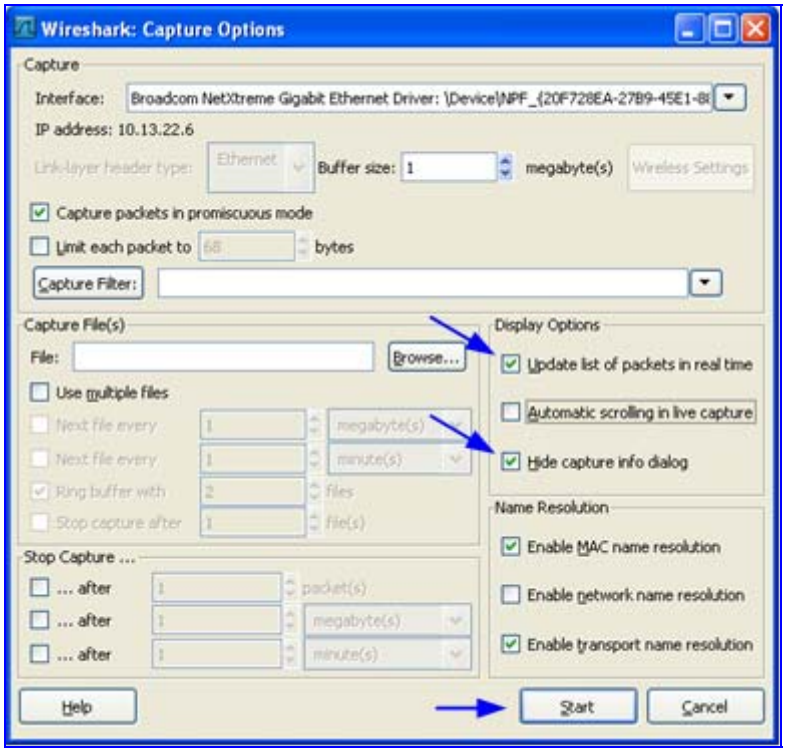
5. Select the network interface that is currently being used by the PC - on the toolbar, click **Interfaces**, and then in the 'Capture Interfaces' dialog box, click the **Options** button corresponding to the network interface:

Figure 13-4: Selecting Interface Currently used by the PC



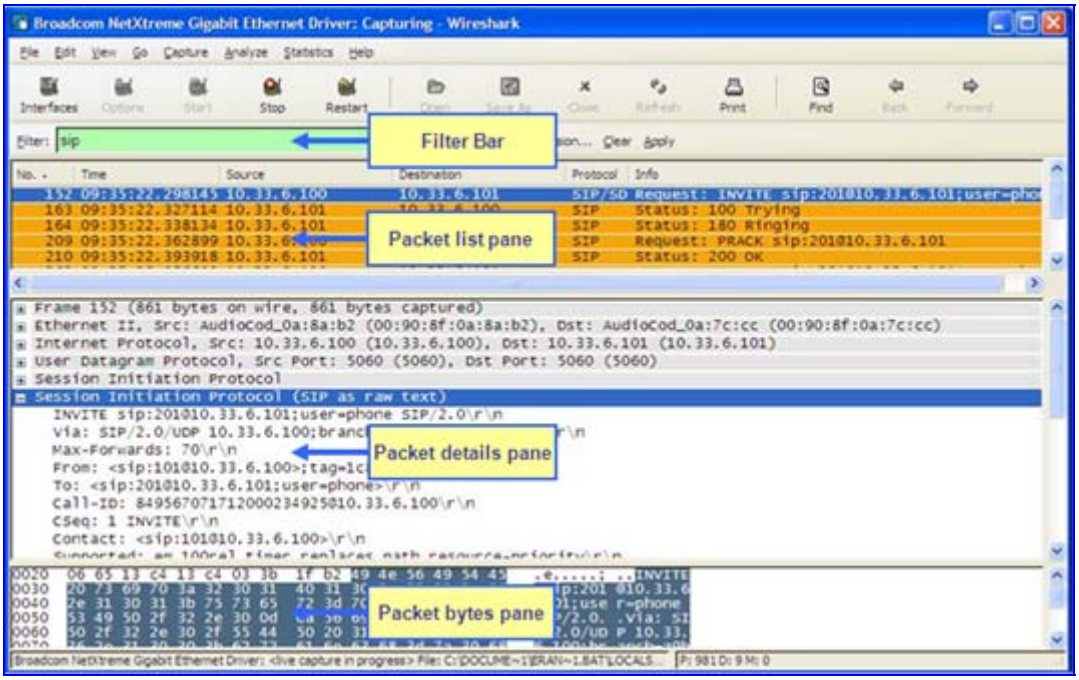
6. In the 'Capture Options' dialog box, select the desired display options:

Figure 13-5: Configuring Wireshark Display Options



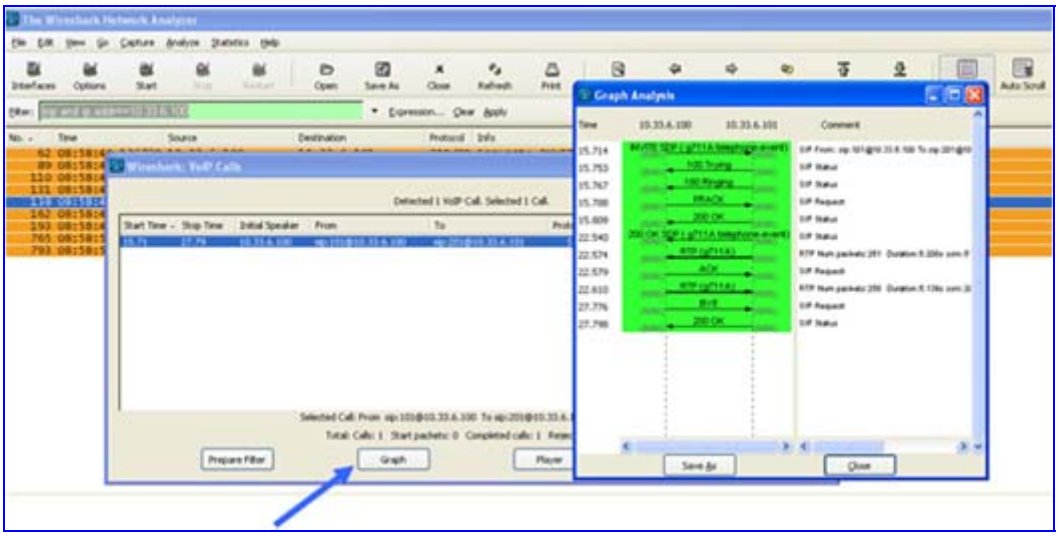
7. Click **Start**.

Figure 13-6: Captures Packets



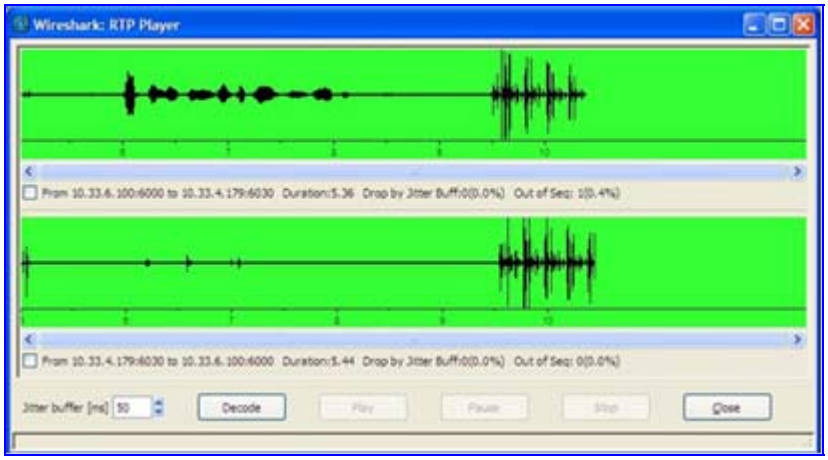
8. To view VoIP call flows, from the **Statistics** menu, choose **VoIP Calls**. You can view the statistics in graph format by clicking **Graph**.

Figure 13-7: Viewing VoIP Call Flows



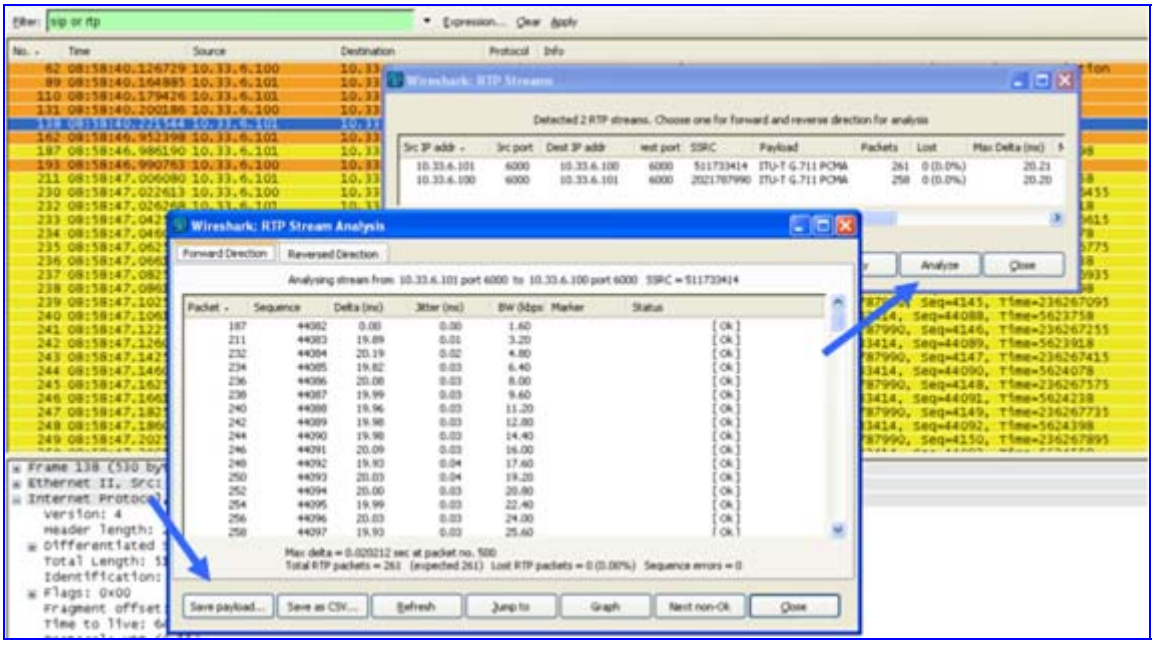
9. To play G.711 RTP streams, click the **Player** button.

Figure 13-8: Playing G.711 RTP Streams



10. To analyze the RTP data stream and extract the audio (which can be played using programs such as CoolEdit) from the data packets (only for G.711), from the **Statistics** menu, point to **RTP**, and then choose **Stream Analysis**.

Figure 13-9: Analyzing the RTP Data



a. Save the audio payload of the RTP stream to a file.

b. Save the Payload as a *.pcm file.

c. Select the 'forward' option.

11. Use Debug Recording (refer to "CLI Debug Recording" on page 72).

13.4 CLI Debug Recording

The Debug Recording (DR) is a mechanism that is used to capture and record the traffic that is sent and received by the device:

- Media streams (RTP, T.38 and PCM)
- PSTN messages (ISDN, CAS, SS7)
- Control messages (SIP, MGCP, MEGACO)
- Networking streams (such as HTTP and SCTP)
- Other internal information (such as DSP Events)

Note: DR packets are captured using Wireshark (refer to "Wireshark Network Sniffer" on page 69).

➢ To collect DR messages:

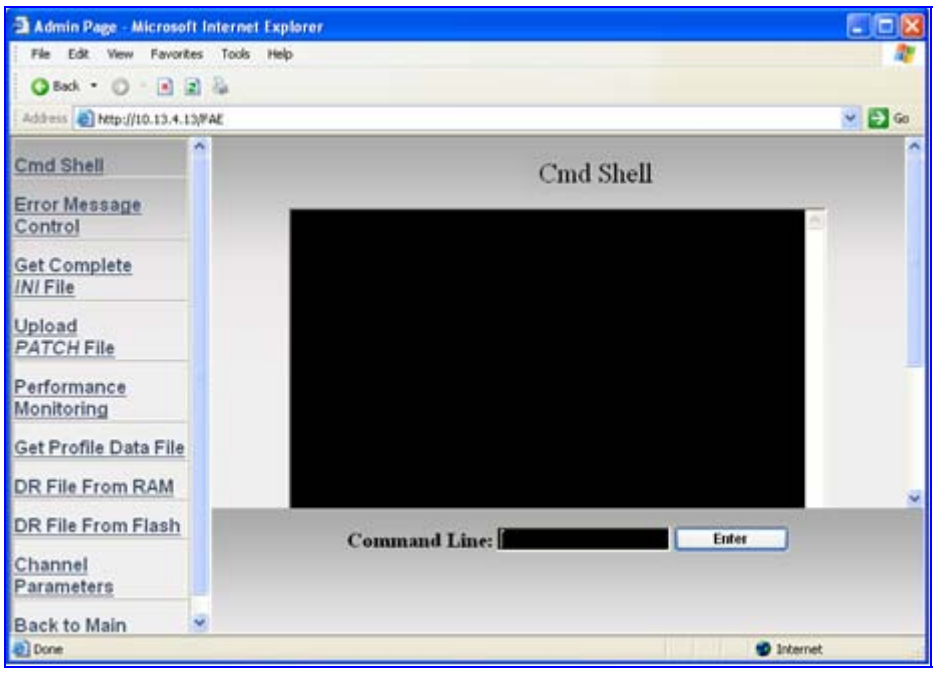
1. Install the open source Wireshark program (which can be downloaded from www.wireshark.org). An Audiocodes proprietary plug-in acdr.dll (supplied in the software kit) must be placed in the 'plugin' folder of the installed Wireshark version (typically, c:\Program Files\WireShark\plugins\<Wireshark version>\). Use the filter "ACDR" or "udp.port==925" to view the DR messages that are sent by the device.

Notes:

- The plugins for DR are per major AudioCodes release. The plug-ins that are released with version 5.4 are applicable to Wireshark version 99.06. The plugins that are released with version 5.6 are applicable to Wireshark version 99.08. The plugins are backward compatible.
- From Wireshark version 99.08, the tpncp.dat file must be placed in the folder ...Wireshark\tpncp and not in the ...Wireshark\plugins directory.

2. Start a CLI management session:
   a. In your Web browser's URL field, append the suffix 'FAE' (case-sensitive) to the IP address of the device (e.g., http://10.1.229.17/FAE). The 'FAE' page is displayed.
   b. On the left pane, click the **Cmd Shell** button.

Figure 13-10: Command Shell Page



   c. At the prompt, type **DR** to access the DebugRecording directory.
   d. At the prompt, type **STOP** to terminate all active recordings, if any.
   e. At the prompt, type **RTR** ALL to remove all previous recording rules.
   f. At the prompt, type **RT ALL** to remove all DR targets (i.e., client IP addresses) from the list.
   g. At the prompt, type **AIT <IP address of the target>** to define the IP address of the PC (running Wireshark) to which the device sends its debug packets.
   h. Continue with the procedures described below for capturing PSTN and/or DSP traces.
3. To capture PSTN (SS7, CAS, ISDN) traces:
   a. Enable PSTN traces on the required trunk (no need to stop the trunk), enter the following commands:

```
<dot><dot><enter> (to exit DR)
pstn
PstnCOmmon
PstnSetTraceLevel <TrunkId> <BChannel> <TraceLevel>
For example, to enable PSTN traces on the first trunk, enter
the following command: PstnSetTraceLevel 0 -1 1
<dot><dot><enter> (to exit PSTN)
DR
```

   b. For SS7 only, set the field 'Trace' to 1 (under **Configuration** tab > **SS7 Configuration** menu > SNs and Links tables).
   c. At the prompt, type **APST** <packet type -- ISDN, CAS, or SS7>.

4. To capture DSP traces (internal DSP packets, RTP, RTCP, PCM, and T.38), at the prompt, type **ANCT ALL-WITH-PCM 1**. The next call on the device will be recorded.
5. To capture IP traces (such as SCTP and HTTP messages), perform the following:
   a. At the prompt, type **AIPTT n2h 132 a a** (132 for SCTP).
   b. At the prompt, type: **AIPTT h2n 132 a a** (132 for SCTP).
6. To capture Syslog messages, at the prompt, type **AIPTT H2N udp a 514**. Note that 514 is the destination port for Syslog messages.
7. To capture SIP messages, at the prompt, type **AddIPControlTrace n2h sip**.
8. To start recording, at the prompt, type **START**; start Wireshark, and filter according to the UDP port (default is 925) to where debug packets will be sent.
9. To stop the DR recording, type **STOP**.

Reader's Notes

14 Management Utilities

This section discusses AudioCodes' proprietary management tools that can be used for debugging:

- "CPTWizard" on page 77
- "BootP/TFTP Server" on page 77

14.1 CPTWizard

The Call Progress Tones Wizard (CPTWizard) is an AudioCodes proprietary application designed to facilitate the provisioning of FXO devices, by recording and analyzing Call Progress Tones (CPT) generated by any PBX or telephone network. These CPT's include tones such as dial tone, busy tone, ring tone, and reorder tone. The CPTWizard creates these CPT files in **.dat* file format, for loading to the device.

For a full description of the CPTWizard, refer to the *Product Reference Manual*.

14.2 BootP/TFTP Server

The Bootstrap Protocol allows a host to configure itself dynamically. AudioCode's proprietary BootP/TFTP Server utility allows you to perform the following:

- Assignment of IP address, subnet mask and default gateway IP address to the device.
- Provides the name of the software (*.cmp) and configuration (*.ini) files to be loaded to the device (via TFTP). (BootP also provides the IP address of the TFTP server).

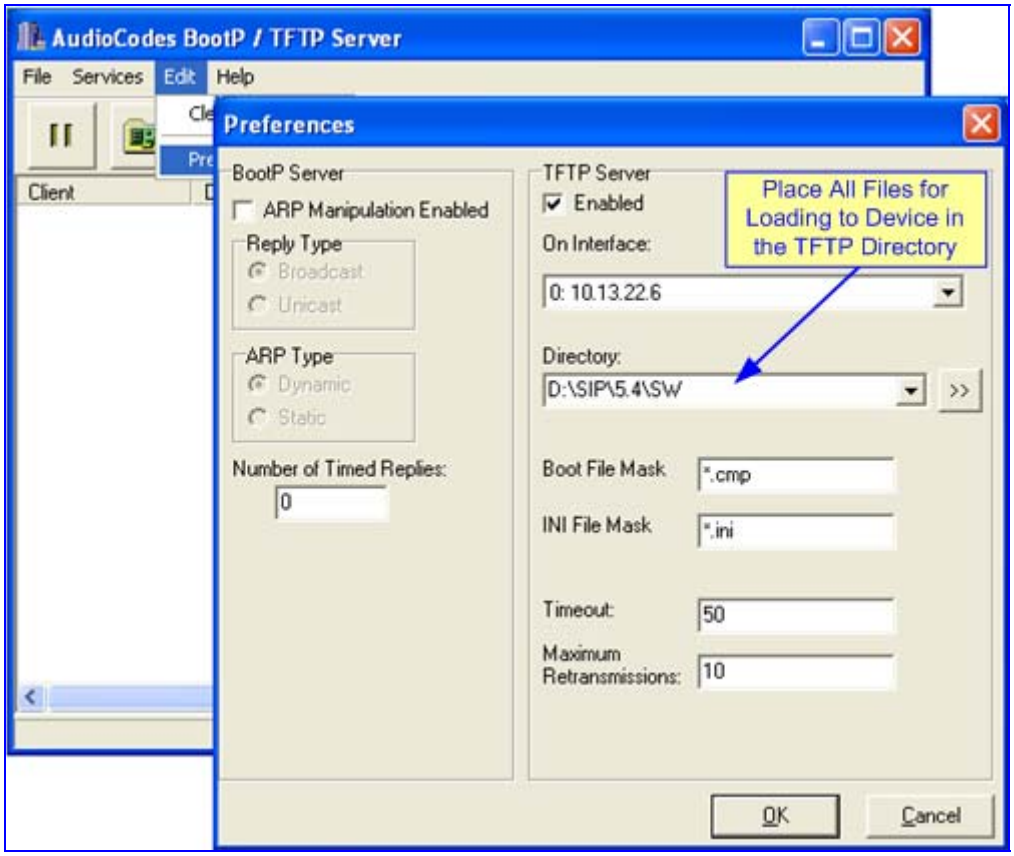
The table below lists the device's default IP addresses:

Table 14-1: Default IP Addresses Per Product

Network Parameter	Default Value
IP Address	▪ **10.1.10.10:** ✓ Mediant 1000 ✓ Mediant 600 ✓ Mediant 2000 (up to 8 trunks) ✓ MP-124 ✓ MP-11x FXS ✓ MP-11x FXS/FXO ▪ **10.1.10.10** (trunks 1-8) and **10.1.10.11** (trunks 9-16): Mediant 2000 with two modules - 16 trunks ▪ **10.1.10.11:** MP-11x FXO
Subnet Mask	255.255.0.0
Default Gateway IP Address	0.0.0.0

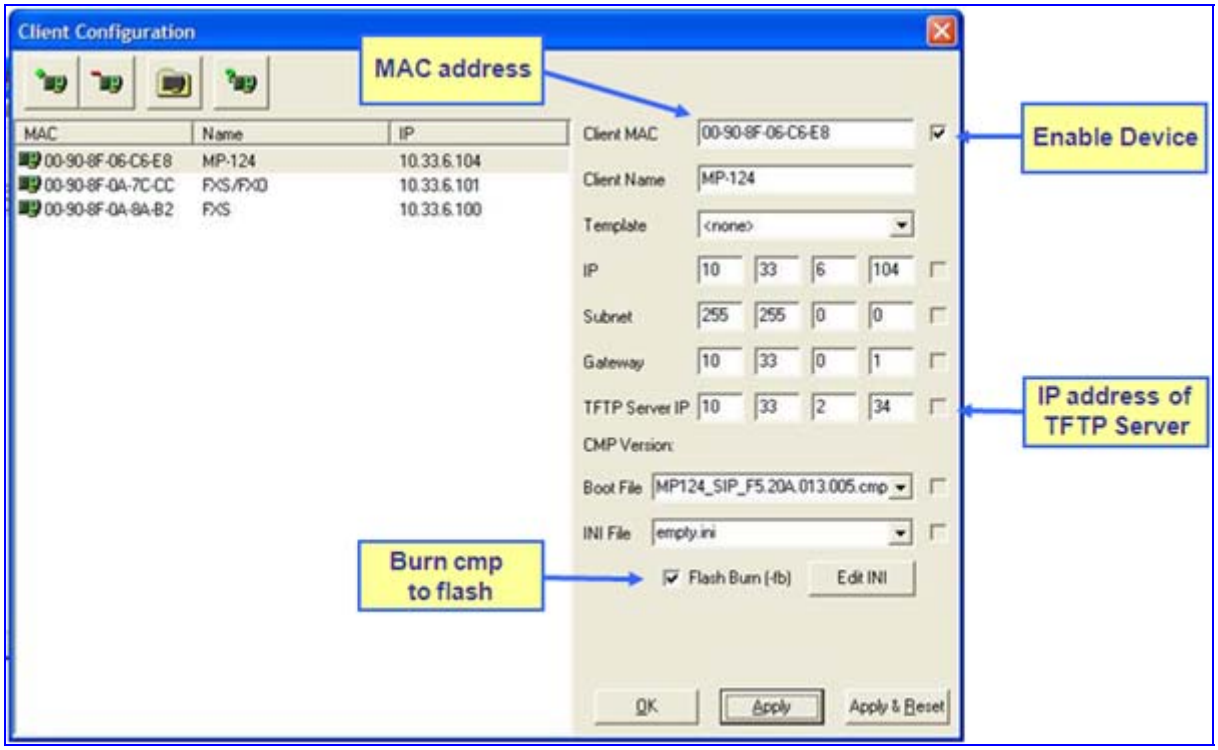
The TFTP server is defined in the BootP/TFTP Server utility's 'Preferences' dialog box, as shown below:

Figure 14-1: Defining TFTP and SW Files



The device to which you want to assign an IP address and load the software files is defined in the BootP/TFTP Server utility's 'Client Configuration' dialog box, as shown below. The device is defined by MAC address. Ensure that the 'Flash Burn' check box is selected in order to save the loaded firmware file (cmp) to the device's flash memory; otherwise, the cmp file is only stored in the volatile memory (RAM) and after a device reset, the device will revert to the previous software version.

Figure 14-2: Defining Device



AudioCodes CPE & Access Gateway Products

SIP

Mediant™ 2000, Mediant™ 1000
& MediaPack™ MP-11x

CPE Troubleshooting Guide

CERTIFIED QMS SI ISO 9001: 2000
THE STANDARDS INSTITUTION OF ISRAEL

AudioCodes

www.audiocodes.com