



Solving Voice Problems

This chapter explains how to solve problems associated with trunks and the transmission of voice packets over phone lines. It includes the following sections:

- [Overview of Voice Troubleshooting, page 9-1](#)
- [Diagnosing and Resolving Voice Quality Problems, page 9-5](#)
- [Debugging VoIP Problems, page 9-25](#)
- [Solving Problems with Cisco IP Phones, page 9-27](#)
- [Solving Problems with VICs, VWICs, and Trunks, page 9-42](#)



Note

For a description of the features, modifications, and caveats for the Cisco Integrated Communications System 7750 (Cisco ICS 7750) release 2.6.0, refer to the [Release Notes for System Software Release 2.6.0 on the Cisco ICS 7750](#).

Overview of Voice Troubleshooting

Transmission of voice and transmission of data across an internetwork differ in a number of ways, including the following:

- TCP-based data applications react to dropped packets, whereas UDP-based voice applications can only conceal dropped packets. Data applications respond to dropped packets through the use of error correction techniques because they are often TCP-based (TCP resends dropped packets). Voice

applications (which rely on the best-effort transmission of UDP) cannot truly respond to and recover from packet loss, although in some cases the complex algorithms underlying voice transmission can conceal packet loss.

- Voice is sensitive to delays, but data is not. *Delay insensitivity* means that data applications can tolerate delay well because they are not real-time-based. Voice responds negatively to delay, creating so-called “holes” in the transmission as heard by the receiver.

Basic Requirements for Voice Traffic

Voice traffic is intolerant of packet loss and delay primarily because these conditions degrade the quality of the voice transmission. Delay must be constant for voice applications. The generally accepted limit for good quality voice connection delay is 200 milliseconds (ms) one-way (or 250 ms as a limit). As delay rises over this measurement, both talkers and listeners become unsynchronized, and often speak at the same time, or wait for the other to speak. While the overall voice quality is acceptable, users may find the stilted nature of the conversation unacceptable.

As a result, voice traffic passing through a network with congestion or other problems is much more likely to be adversely affected than data traffic passing through the same network.

Common Problems Affecting Voice Traffic

The following factors can affect the quality of voice traffic:

- [Delay, page 9-3](#)
- [Echo, page 9-3](#)
- [Jitter, page 9-4](#)
- [Latency, page 9-4](#)
- [Serialization, page 9-4](#)
- [Loss, page 9-5](#)
- [Noise, page 9-5](#)

Delay

Delay is the time it takes for packets to travel between two endpoints. Delay manifests itself when long pauses in conversation cause the person listening to start to talk before the other person has finished. There are two distinct types of delay: *fixed delay* and *variable delay*.

Fixed delay components add directly to the overall delay on the connection. Variable delays arise from queuing delays in the egress trunk buffers on the serial port connected to the Wide Area Network (WAN). These buffers create variable delays, called jitter, across the network. Variable delays are handled via the de-jitter buffer at the receiving router/gateway. For additional information on delay, refer to [Understanding Delay in Packet Voice Networks](#).



Note

You can measure delay by using **ping** tests at various times of the day with different network traffic loads. (For more information about **ping** tests, see the [“Using Extended ping Tests”](#) section on page 6-17.)

Echo

Echo occurs when the speech energy being generated and transmitted down the signal path is coupled into the receive path from the far end. This causes a speaker to hear the sound of his or her own voice, delayed by the total echo path delay time.

In a traditional voice network, voice can reflect back, but it usually goes unnoticed because the delay is so low. In a Voice over IP (VoIP) network, echo is more noticeable because packetization and compression contribute to delay.

It's important to remember that the cause of the echo is always with the analog components and wiring. For instance, IP packets cannot turn around and go back to the source at a lower audio level or on digital T1/E1 circuits. So, on a call from one Cisco IP Phone to another, there should not be any problems. The only exception could be caused by acoustic echo caused by one party using a speakerphone that has the volume set too high or caused by some other situation in which an audio loop is created. For additional information on echo and echo cancellation, refer to [Echo Analysis for Voice over IP](#).

**Note**

Echo cancellation technology is a functional component of a voice gateway that is used to reduce the effects of echo. An echo canceler monitors a caller's speech. If that caller's speech echoes, the echo canceler generates and transmits a signal that is sent back to the caller to cancel out the echo. The amount of time that it takes the echo canceler to locate the echo and to generate its opposite signal is called *convergence time* (typically, a few seconds). During convergence, the caller hears echo, which should gradually decrease in amplitude to zero when convergence is complete.

Jitter

Jitter is a variable-length delay that can cause a conversation to break and become unintelligible. Jitter is a variation in the delay of received packets. At the sending side, packets are sent in a continuous stream with the packets evenly spaced apart. As a result of network congestion, improper queuing, or configuration errors, this steady stream can become fragmented, causing the delay between each packet to vary instead of remaining constant.

Jitter is not usually a problem with public switched telephone network (PSTN) transmissions because the bandwidth of these calls is fixed. However, in VoIP networks in which existing data traffic might be bursty, jitter can occur. For additional information on jitter, refer to [Understanding Jitter in Packet Voice Networks \(Cisco IOS Platforms\)](#).

Latency

Latency is the amount of time between when a device requests access to a network and when the device is granted permission to send. *End-to-end latency* describes the overall delay associated with a network.

Serialization

Serialization occurs when a multiservice route processor (MRP) or router attempts to send both voice and data packets out of the same interface. In general, voice packets are very small (80 to 256 bytes), while data packets can be very large (1,500 to 18,000 bytes). On relatively slow links, such as WAN connections, large data packets can take a long time to transmit onto the network. When these

large packets are mixed with smaller voice packets, the excessive transmission time can lead to both delay and jitter. The time that it takes to put voice traffic onto a transmission line depends on the data volume and the speed of the line—for instance, it takes about 5 ms to send a 1024-byte packet on a 1.544-Mbps T1 line.

**Tip**

You can use *compression* to reduce the size of voice transmissions. Many different compression algorithms are available, such as conjugate structure algebraic code-excited linear predictive (CSA-CELP). CSA-CELP requires only 8 kbps of bandwidth, which is one-eighth the bandwidth (64 kbps) required by traditional pulse code modulation (PCM).

**Caution**

Use compression carefully. The greater the compression of a digital VoIP packet, the greater the likelihood that voice quality will decrease.

Loss

Loss occurs when networks drop voice packets. Packet loss is most likely to occur where the network connects to the WAN, although it can occur anywhere in the network.

Noise

Noise (or *distortion*) is a problem that users commonly describe as “muffled,” “tinny,” or “scratchy.” Noise is typically a result of compression, decompression, packet loss, or echo cancellation.

Diagnosing and Resolving Voice Quality Problems

You may experience voice quality problems, including lost or distorted audio signal during phone calls, audio breaks (such as broken words), or the presence of odd noise and audio distortion, such as echo, “underwater,” or robotic voice quality.

The following sections describe how to resolve voice quality problems:

- [Diagnosing Common Voice Quality Problems](#), page 9-6
- [Diagnosing Problems Involving Lost or Distorted Audio](#), page 9-7
- [Diagnosing Echo Problems](#), page 9-10
- [Resolving Echo Problems](#), page 9-12
- [Determining DSP Requirements](#), page 9-14
- [Codec Complexity, DSP Groups, and PVDM Guidelines](#), page 9-14
- [Identifying and Resolving One-Way Voice Problems](#), page 9-22
- [Digits Not Recognized Correctly](#), page 9-24

Diagnosing Common Voice Quality Problems

[Table 9-1](#) shows common voice quality problems and their possible causes.

Table 9-1 *Voice Quality Problems and Causes*

Problem	Possible Cause
Clipped voice	<ul style="list-style-type: none"> • Overdriven input • Might sound fuzzy; loss of quality
Echo	<ul style="list-style-type: none"> • Input/output levels • Impedance mismatch
Gaps in speech, intermittent speech, “underwater” voice	<ul style="list-style-type: none"> • Network queues • Playout delay (de jitter) buffers • Voice packet sizes (delay)



Note

Be sure to check your gateway and phone loads to verify that they are at the latest version. Check [Cisco Connection Online](#) (CCO) at <http://www.cisco.com> for the latest software loads, patches, and release notes.

One-way audio—a conversation between two people in which only one person can hear anything—is not actually a voice quality issue, but it may be experienced on a VoIP network.

Voice quality problems may affect one or more of the following:

- Gateways
- Phones
- Networks

**Note**

For guidance on the type of information you should collect for troubleshooting purposes, refer to *AVVID TAC Cases: Collecting Troubleshooting Information*, at http://www.cisco.com/warp/customer/788/AVVID/AVVID_TAC_ts.html.

Diagnosing Problems Involving Lost or Distorted Audio

A problem that you might encounter is broken audio signal (garbled speech, or lost syllables within a word or sentence). There are two common causes for this problem: packet loss and/or jitter.

- With packet loss, audio packets do not arrive at their destination because they were dropped or because they arrived too late to be useful.
- With jitter, there is variation in the arrival times of packets.

There are many sources of variable delay in a network, some of which cannot be controlled. Variable delay cannot be eliminated entirely in a packetized voice network.

Digital signal processors (DSPs) on phones and other voice-capable devices are designed to buffer some of the audio, in anticipation of variable delay. This dejittering can be done only when the audio packet has reached its destination and is ready to be put into a conventional audio stream.

A Cisco IP Phone (such as the Cisco IP Phone 7960) can buffer as much as 1 second of voice samples. The jitter buffer is adaptive, so if a burst of packets is received, the Cisco IP Phone 7960 can play these packets out in an attempt to control the jitter. The variation between packet arrival times can be minimized by applying quality of service (QoS) techniques. For additional information on QoS, refer to *QoS Technical Tips*.

Follow these steps to isolate and resolve problems related to lost or distorted audio:

-
- Step 1** Try to isolate the path of the audio.
- a. Try to identify each network device (switches and routers) in the path of the call's audio stream. Remember that the audio might be between two phones, or might be between a phone and a gateway, and that the audio could have multiple legs (from a phone to a transcoding device and from that device to another phone).
 - b. Try to determine whether the problem occurs only between two sites, through only a certain gateway, on a certain subnet, and so on. This will help narrow down the devices to investigate.
- Step 2** Disable silence suppression (also known as voice activation detection, or VAD) if it is enabled. VAD saves bandwidth by not transmitting any audio when there is silence, but it may cause noticeable or unacceptable clipping at the beginning of words.
- a. To disable VAD, access the Cisco CallManager publisher on the target SPE.
 - b. From Cisco CallManager Administration, choose **Service > Service Parameters**.
 - c. Select the Call Manager publisher and the Cisco CallManager service.
 - d. In the parameters field, navigate to **SilenceSuppressionSystemWide**, and set it to **F**.
 - e. If a network analyzer is available, monitor a call between two phones. It should show 50 packets per second (or 1 packet every 20 ms) with silence suppression disabled.
 - f. Insert the packet analyzer at various points in the network to help determine the source of the delay.
 - g. If a packet analyzer is not available, you can examine the interface statistics of each device in the path of the audio. The diagnostic call detail record (CDR) is a tool that you can use to track calls with poor voice quality. CDRs are written to a Microsoft SQL Server database. They are useful for post-processing activities, such as billing and network analysis. Refer to [Call Detail and Call Management Records](#) for more information about CDRs.
-

Diagnosing Audio Problems from the Cisco IP Phone

The Cisco IP Phone 7960 provides another tool for diagnosing possible audio problems.

On any active call, you can press the “i” button twice quickly, and the phone will display an information screen that contains packet receive and transmit statistics, as well as average and maximum jitter counters. On this screen, the jitter number is the average of the last five packets that arrived, and the maximum jitter is the highest count of the last five packets (high-water mark for the average jitter).

Diagnosing Audio Problems Between the WAN and the LAN

The most common sources for delay and packet loss are devices in which a higher speed interface feeds into a lower speed interface; for example, a router with a 100-megabyte (MB) Fast Ethernet interface, connected to a local area network (LAN), and a slower Frame Relay interface, connected to a WAN.

If poor audio quality occurs only when communicating to a remote site, check the following as the most likely sources of the problem:

- The router has not been properly configured to enable voice traffic priority over data traffic.
- There are too many active calls for the WAN, which means that there is no call admission control to restrict the number of calls that can be placed.
- There are physical port errors.
- There is congestion in the WAN itself.

Follow these steps to test the number of calls that can be supported across your WAN:

-
- Step 1** Disable silence suppression as described in the [“Diagnosing Problems Involving Lost or Distorted Audio”](#) section on page 9-7.
- Step 2** Place calls between your two sites.
- Do not place the calls on hold or on mute, because this will stop packets from being transmitted.
 - With the maximum number of calls across the WAN, the calls should all have acceptable quality.

Step 3 Test to make sure that a fast busy is returned when you try to make one more call.



Note For more information about call admission control and the use of gatekeepers, refer to the [Cisco CallManager System Guide](#).

On the LAN, the most common problems are physical level errors (such as cyclical redundancy check [CRC] errors). LAN problems are usually caused by faulty cables or interfaces, or by incorrectly configured devices (such as a port speed or duplex mismatch). Check all devices in the path, including any shared-media device, such as a hub.

Diagnosing Crackling Sounds

You might also experience a crackling sound, which is another symptom of poor quality. Crackling is sometimes caused by a defective power supply or some kind of strong electrical interference close to the phone. Try changing the power supply and moving the phone to a different location.

Diagnosing Echo Problems

Echo is a problem that you might encounter when you are using a VoIP network. To diagnose echo problems, consider the following:

- Determine whether the echo occurs while using a handset, a headset, or a speaker phone. If it occurs while using a headset, the type of headset is important, as well as whether the headset port on the Cisco IP Phone is being used or whether an external amplifier is connected to the handset. The impedance switch on a headset transformer can cause echo problems.
- Echo cancellation is a function of the remote end of a given connection. That is, if the call is terminated at another Cisco IP Phone, the remote Cisco IP Phone performs the echo cancellation for the caller. If the call goes through the multiservice route processor (MRP) to the central office (CO), both the DSP in the MRP and the CO contribute to echo cancellation. If a CO is

involved, the echo cancellation range on the MRP voice port may need to be tuned. For T1 ports, 16-ms echo cancellation is appropriate. For analog ports, 32-ms echo cancellation can be used.

- When Foreign Exchange Office (FXO) ports on the MRP are used, the input gain might need to be adjusted. Changes to the input gain allow you to increase or decrease the signal at input.

Adjusting Input Gain and Output Attenuation

If you adjusted the input gain to a number greater than 0, you can try to resolve an input gain problem by bringing the input gain back down to 0 (default).



Note

To check the current input gain and output attenuation settings on your system, execute the **show voice port** command. To check settings for a specific voice port, execute the **show voice call** command. This command shows the active signal input and output levels for that voice port.

If the input gain value needs to be adjusted, you can make the adjustment by entering commands similar to the following from the command prompt on the MRP:

```
MRP#configure terminal
MRP(config)#voice-port x/x
MRP(config-voiceport)#input gain value
```

Permitted entries for *value* are from -6 to +14 dBm.

Gain values higher than 12 may cause dual tone multifrequency (DTMF) recognition problems.

If changes to the input gain do not help to improve the situation, try increasing the output attenuation by 2 dB or so.

You can make adjustments to output attenuation by entering commands similar to the following from the command prompt on the MRP:

```
MRP#configure terminal
MRP(config)#voice-port x/x
MRP(config-voiceport)#output attenuation value
```

Permitted entries for *value* are from 0 to 14 dBm. You can decrease the signal only at the output side. Reducing attenuation at the output side raises the output level.

**Note**

You will need to do a **shut/no shut** on the voice port after you make each change.

**Caution**

Use care when adjusting input gain and output attenuation. Adding gain on the input side amplifies noise, so that a large volume increase can actually contribute to echo. Too much attenuation of the signal can make the audio impossible to hear on both sides. It is very important to remember to try small adjustments in small increments.

Follow these general level-adjustment guidelines for input gain and output attenuation:

- Avoid adding gain on the input side; it amplifies noise.
- Try to decrease the attenuation at the output side instead to raise an output level.
- If you are applying 0 dBm of attenuation and the signal is still too soft, go to the input side and increase the gain to avoid overdriving the inputs on your first attempt.
- To lower an output level, adjust the input side first; then adjust the output side.

Resolving Echo Problems

**Note**

You can check the echo on a Cisco IP Phone by generating a test tone. To generate a test tone, call another number and press **3 followed by pressing the **i** button twice. Select a tone from the menu. The tone will provide you with something to hear as you make adjustments for echo on the gateway. The tone will not stop until you hang up.

To help resolve echo problems, try to answer the following questions:

- Where is the echo?
 - Cisco IP Phone to Cisco IP Phone?
 - Cisco IP Phone to PSTN. Which side hears the echo—PSTN or Cisco IP Phone?



Note Make sure that the problem phones are not using the speakerphone and that they have the headset volume set to reasonable levels (start with 50% of the maximum audio level). Most of the time, the problems occur when the phones are connected to the PSTN through a digital or analog gateway.

- What is your gateway type?

If a digital gateway is being used, it may be possible to add additional padding in the transmit direction (toward the PSTN). Lower signal strength yields less reflected energy. Lowering the signal strength may help to clear up the echo.
- What is the frequency of the echo?
- What are the transmit and receive attenuation settings on your gateways?
- Is the echo sustained throughout the entire call?
- Does the echo last for 2 to 3 seconds and then disappear?
- What is the echo return loss (ERL) of the calls that have echo? (ERL is a measurement of echo strength, expressed in dB.)
- What is the echo coverage on the gateway?
- What are the versions and loads of Cisco CallManager, gateway, and phones?
- Has a TAC case been generated?
- Do you have a history of troubleshooting the echo problem?
- Do you have a description of the network?
- Do you have a sniffer trace of the echo?
- Do you have a record of echo cases? It is very important to maintain an echo report with the following information for each situation:
 - The date and time the problem occurred
 - The calling number
 - The called number
 - The gateway used.

Determining DSP Requirements

Voice quality problems might be caused by insufficient DSPs. Voice interface cards (VICs) and voice WAN interface cards (VWICs) installed in the analog station interface (ASI) or MRP might require additional DSPs for processing greater amounts of voice traffic. DSPs are located on the packet voice/data modules (PVDMs) and divided into DSP groups on the ASI and MRP cards. A DSP group is a logical set of DSPs that could be used to handle calls on a set of voice ports. All the DSPs on a PVDM belong to only one group. Each DSP can perform a maximum of 100 million instructions per second, enabling greater processing power on an ASI or MRP. There can be up to five DSPs on a single PVDM, and up to two PVDMs on an ASI or MRP card.

Codec Complexity, DSP Groups, and PVDM Guidelines

This section provides additional information about codec complexity, along with guidelines applicable for use of DSP groups and PVDMs.

Codec Complexity

The number of channels per DSP that can be supported on the MRP card depends on the codec complexity that is configured and on the DSP image (firmware) being used on an individual VIC.

Analog and BRI ports use analog DSP firmware; E1 and T1 ports use Flexi DSP firmware. Each image is capable of handling a different number of voice channels. The number of DSPs that are required on each analog DSP firmware is calculated and loaded on the DSPs, based on the number of analog or BRI ports in the group. The remaining DSPs in the group are loaded with Flexi DSP firmware.

When a call is made on a voice port, it uses a DSP from the DSP group to which the voice port belongs. If a DSP serves both analog and E1 or T1 ports, calls originating from the analog ports use only the DSPs that are loaded with analog DSP firmware, and calls originating from the E1 or T1 ports use only the DSPs that are loaded with the Flexi DSP firmware.

The default firmware can be changed using the **codec complexity** command.

The VIC on the MRP3-8FXOM1 card uses a default DSP firmware of medium complexity. Using the Cisco IOS command-line interface (CLI), you can configure the **codec complexity** command to select the DSP image to be applied to the DSPs in the PVDM corresponding to the VIC card slot. This will determine the codecs that are supported. The **[no]** form of the **codec complexity** command restores the medium-complexity default.

The **codec complexity** command can be used on any MRP card installed in the Cisco ICS 7750.

From enable mode on the MRP, execute the following global configuration Cisco IOS CLI command to configure codec complexity:

```
MRP#config term  
MRP(config)#voice-card <slot>
```

where the value of <slot> is 0 or 1 to identify the physical slot on the MRP where the voice card is installed.

```
MRP(config-voicecard)#codec complexity [high | medium]
```

where *high* or *medium* complexity can be chosen as the value (low complexity is not supported). Medium complexity supports G.711, G.729a, G.726, G.723.1 and fax-relay, with a maximum of six channels per DSP (mid-range complexity and call density). High complexity supports G.711, G.726 and G.729a, with a maximum of eight channels per DSP (high complexity with lower call density).

**Note**

The **codec complexity** command is supported only on the 4-port, 8-port, and 16-port analog VICs, such as the VIC-4FXS/DID, MRP3-8FXS, MRP3-16FXS, and MRP3-8FXOM1 cards. Refer to the “Processor Cards Feature Summary” section of the [Cisco ICS 7750 System Description](#) for additional information.

Before you configure codec complexity, you must shut down all voice ports on a T1 or E1 port that shares a PVDM on an analog VIC, and also shut down all voice ports on the analog VIC. This ensures there are no active calls on the DSP group to which the analog VIC belongs.

To ensure that there are no active calls, perform one or more of the following tasks before changing the codec complexity:

- Shut down all analog voice-ports in the DSP group

- Remove all digital channels in the DSP group (DS0, PRI, channel group, transcoding)
- Shut down the BRI interfaces in the DSP group



Tip

The **show voice dsp** command is useful for checking the voice ports belonging to a DSP group and for displaying the number of voice channels that are usable for voice.

Use the **shutdown** command to shut down all the voice ports on an analog VIC with a single command. This command is supported only on analog VICs. The [**no**] form of the **shutdown** command restores the default.

The following example shuts down all the voice ports on the VIC in slot 0:

```
MRP#config term
MRP(config)#voice-card 0
MRP(config-voicecard)#shutdown
```

After this command is run, you can use the **show running-config** command to see that the ports are shut down under the voice-port status in the command output.



Note

For additional information, refer to the “Choosing DSP Firmware” section in Chapter 6, “Configuring the Cisco ICS 7750,” in the [Cisco ICS 7750 Installation and Configuration Guide](#).

DSP Groups

The Cisco IOS software that is packaged with ICS System Software 2.6.0 includes the capability for DSP resources in PVDM0 and PVDM1 to be pooled and shared for use by the FXO ports and digital voice ports (such as T1 ports). Resource sharing enables the most efficient use of DSPs.

With this release, support is provided for 30 voice calls on T1 or E1 controller(s) plus 8 calls through the FXO interface simultaneously. The remaining DSP resources can be used for transcoding, in which one transcoding session is equal to two voice channels. The total number of voice channels cannot exceed 48 on the Flash-based MRP cards.

The number of DSP groups that are created depends on the following two variables:

- Configuration of the **tdm connected** command (see the “[New Cisco IOS CLI Commands](#)” section on page 9-18)
- The number of voice clocking domains

The presence or absence of analog or BRI VICs in the chassis does not affect the number of DSP groups that are created. See [Table 9-2](#) for information about the number of DSP groups that are created under specific conditions.

Table 9-2 *DSP Groups*

Is the tdm connected Command Configured?	Number of Voice Clocking Domains Configured	Number of DSP Groups Created
Yes	1	1
Yes	2	2
No	1	2
No	2	2

Prior to this shared DSP support, two DSP groups were created when analog and digital ports were installed in two different slots in the Cisco ICS 7750 chassis. This system configuration resulted in the use of a single PVDM by the digital ports, with the second PVDM being used for the analog ports and transcoding activity. This did not allow for sharing of PVDMs or for full availability of DSP resources, both of which are now supported in the version of the Cisco IOS software that is included in ICS System Software 2.6.0.



Tip

To configure and use all 24 channels (on a T1) or 30 channels (on an E1) on port 1 of the T1/E1 on the MRP3-8FXOM1 card, the T1 or E1 should not share the PVDM with the PVDM used for the FXO ports. This configuration ensures that all DSPs on the PVDM are available for the T1 or E1 port; the T1 or E1 in port 0 (regardless of the slot number) is allocated a dedicated PVDM, and the T1 or E1 in port 1 is configured to share the PVDM with any FXO, FXS, and/or the VIC-2BRI-NT/TE (2-port BRI VIC) ports installed in the second slot.

**Note**

For detailed information about the configuration modifications that affect the number of supported voice channels on the MRP300 cards, and the caveats associated with that support, refer to the [Release Notes for Cisco IOS Release 12.2\(8\)YN on the Cisco ICS 7750](#).

New Cisco IOS CLI Commands

Two new Cisco IOS CLI commands are available for use on the Flash-based MRP cards beginning with ICS System Software release 2.6.0.

- The **[no] tdm connected** command controls the number of DSP groups that are created when there is only one voice T1 or E1 clocking domain in the system.

**Tip**

It is recommended that you use the **tdm connected** command when there is only one T1 or E1 port configured for voice (or voice and data) installed in the system.

The following guidelines tell how to use the **[no] tdm connected** command:

- If you do not configure **tdm connected**, the default configuration creates two DSP groups if there is a mixture of analog, BRI, and T1 or E1 ports installed.
- If you do configure **tdm connected**, the following DSP groups are created (irrespective of the types of VICs installed):
 - Single voice T1 or E1 clocking domain—One DSP group
 - Two voice T1 or E1 clocking domains—Two DSP groups

When **tdm connected** is configured, a subsequent **tdm clock** command that configures a port for voice (or both voice and data), or a subsequent reload, will result in the creation of a single DSP group (regardless of the number of T1s or E1s, and analog VICs installed), except when there are two voice T1 clocking domains.

- The **[no] tdm multichannel** command enables multichannel support. This command provides support for up to a maximum of eight channel groups, PRI data (PRI-D) channels, or PRI dialer calls on a single T1 or E1 controller on an MRP, with supported speeds on the individual channels of 48 kbps, 56 kbps, and 64 kbps.

If multichannel support is not enabled, speeds of 48 kbps and 56 kbps are not supported.

Use the following command to enable multichannel support (this feature is not enabled by default):

```
tdm multichannel {E1/T1} slot/port number timeslot range
```

where *range* is 1–24 or 1–31. The default is to have all time slots in serial channel controller (SCC) non-multichannel support mode.

If all four SCCs are engaged by multiple channel groups (multichannel and non-multichannel modes) on one controller, all High-Level Data Link Control (HDLC) resources will be allocated and no additional channel groups can be created on the remaining controller. This situation is caused by the fragmentation of channel groups on the controller. To work around this problem, do not interleave SCC and multichannel modes under one controller; instead, use consecutive channels of either SCC or multichannel modes.

For example, to set up a total of 11 channels in multichannel mode, use the following sample command as a guide:

```
tdm multichannel [T1/E1] 1/0 timeslot 1-11 (multichannel mode)
```

In this example, only one SCC will be used and all remaining time slots on 1/0 will use up the second available SCC. There will be two SCCs available for the second controller. If you fragment the groups by using multiple **tdm multichannel** commands, all four SCCs will be used up under one controller, leaving no available SCCs for the remaining controller.

**Note**

HDLC is a protocol that provides Cisco serial encapsulation. When using non-multichannel mode, only four HDLC resources are available. In multichannel mode, eight HDLC resources are available.

**Note**

For additional information about the new **tdm** commands, refer to Chapter 7, “Cisco ICS 7750 Sample Configurations,” in the *Cisco ICS 7750 Installation and Configuration Guide*.

PVDM Guidelines

The following are general guidelines for using PVDMs. The use of a PVDM-20 module is subject to a limitation on the MRP and ASI motherboard. The general rules are as follows:

- If the PVDMs are shared by the VICs on the MRP or ASI (as one DSP group), only the first four DSPs from each PVDM are accessible.

For example, if only one T1 or E1 port is configured for voice, and there are no other analog or BRI VICs installed in the system, the PVDMs could be shared as long as the **tdm connected** command has been configured. In this situation, only four DSPs on each PVDM can be used, so a PVDM-20 will be treated as a PVDM-16. The recommendation is to use a PVDM-16 instead of a PVDM-20.

**Tip**

You must configure the **tdm connected** command in order for the PVDMs to be shared. The default configuration creates two DSP groups unless **tdm connected** is configured and there is a single voice clocking domain.

- If the PVDMs are not shared, then all five DSPs on a PVDM-20 are usable.
- PVDMs are *not* shared (i.e., two DSP groups are formed) in the following situations:
 - Mixed analog VIC and T1 or E1 VWIC—For example, slot 0 has a VIC-2FXS, slot 1 has a 2MFT-T1, and **tdm connected** is not configured, or **tdm connected** is configured along with two voice T1 or E1 clocking domains.
 - Mixed BRI VIC and T1 or E1 VWIC—For example, slot 0 has a VIC-2BRI-NT/TE, slot 1 has a 1MFT-E1, and **tdm connected** is not configured, or **tdm connected** is configured along with two voice T1 or E1 clocking domains.

**Tip**

In the above situations, if the **tdm connected** command is used and only one voice clocking domain is configured, the PVDMs will be shared. It is recommended that you use the **tdm connected** command when there is only one T1 or E1 port configured for voice (or voice and data) installed in the system.

- Two T1 or E1 ports are configured for voice (or voice and data) using the **tdm clock** commands, defining two voice clock source domains. In this situation, two DSP groups are created regardless of the mixture of VICs installed and regardless of whether the **tdm connected** command is configured.

In the above situations, a PVDM-20 can be fully used.

- If you have only one 1MFT-T1 installed in the MRP and the other WIC slot is empty, the use of PVDM-16 modules is recommended. One PVDM-16 is sufficient for a full voice T1 using G.711 and maximum echo-cancellation (32 ms). Two PVDM-16 modules would suffice for a full voice T1 with G.729a and 32-ms echo-cancellation. A PVDM-20 is required for E1 ports.

You can determine whether the PVDMs are shared by running the **show voice dsp** command from the MRP.

The following documents provide additional information:

- For information about PVDM usage and an analysis output example of the **show voice dsp** command, refer to *Understanding the Use of Codecs, DSPs, and Transcoding on the Cisco ICS 7750*.
- For PVDM installation instructions, refer to *Installing Memory, PVDM, and VPN Modules in ASI Cards, MRP Cards, and SPE Cards in the Cisco ICS 7750*.
- For information about voice compression algorithms and PVDM recommendations for ASI and MRP cards, refer to the *Cisco ICS 7750 Installation and Configuration Guide*.
- For detailed information about the configuration modifications that affect the number of supported voice channels on the MRP300 cards, and the caveats associated with that support, refer to the *Release Notes for Cisco IOS Release 12.2(8)YN on the Cisco ICS 7750*.

Identifying and Resolving One-Way Voice Problems

This section describes some of the possible ways a condition known as *one-way voice* can occur. This is a situation in which Cisco IP Phone users might be able to hear voice traffic in one direction through the Cisco ICS 7750, but not through the other direction.

Some possible causes for one-way voice are an improperly configured Cisco IOS gateway, the use of a firewall (see the [“Other Potential Causes of One-Way Voice Problems”](#) section on page 9-24), or a routing or default gateway problem.

Diagnostic CDRs are useful for determining whether a call is experiencing one-way audio because CDRs log packets that are both transmitted and received. Refer to [Call Detail and Call Management Records](#) for more information about CDRs.



Tip

You can also press the **i** button twice quickly on a Cisco IP Phone 7960 during an active call to view details about transmitted and received packets.



Note

When a call is muted, no packets will be transmitted from the phone on which the mute button is pressed. The Hold button stops the audio stream, so that no packets are sent in either direction. When the Hold button is released, all the packet counters are reset. Remember that Silence Suppression must be disabled on both devices in order for the transmit and receive counters to stay equal.

Gateway Route Not Present

The most common cause of one-way voice is an improperly configured device or gateway.

For example, Cisco CallManager handles the call setup for a Cisco IP Phone. The actual audio stream occurs between the two Cisco IP Phones (or between the Cisco IP Phone and a gateway). Cisco CallManager may be able to signal a destination phone (making it ring) even if the phone originating the call does not have an IP route to the destination phone. A common cause for this problem is an improper configuration of the default gateway in the phone, either statically or dynamically on the DHCP server.

The lack of a properly configured default gateway, whether using dynamic routing or using static routing, is also a common cause of one-way voice issues.

To check the IP routing configuration on the MRP, at the MRP command prompt, enter the command **show ip route**.

An example of the output from **show ip route** is as follows:

```
MRP#show ip route
10.0.0.0/23 is subnetted, 1 subnets
C      10.34.200.0 is directly connected, FastEthernet0/0
S*    0.0.0.0/0 [1/0] via 10.34.200.1 - Required route to default
gateway
```

MRP Configuration Lacking voice rtp send-recv Command

The Cisco IOS command **voice rtp send-recv** is needed in the MRP configuration to allow voice traffic to pass both ways.

The **voice rtp send-recv** command is used to establish a two-way voice path when the Real-Time Transport Protocol (RTP) channel is opened. By default, the voice path is connected in only the backward direction when the RTP channel is opened. Enabling **voice rtp send-recv** allows the voice path to be established in both backward and forward directions and, as a global command, affects all VoIP calls when enabled.

If the **voice rtp send-recv** command is not included as part of the Cisco IOS software that you are running, follow these steps to add the command:

Step 1 Log in to the MRP, and proceed to global configuration mode.

Step 2 Enter these commands:

```
MRP#configure terminal
MRP(config)#voice rtp send-recv
MRP(config)#exit
MRP#copy run start
MRP#end
```

Step 3 View the running configuration. It should now contain the following string:

```
voice rtp send-recv
```

Other Potential Causes of One-Way Voice Problems

Other possible causes of one-way audio problems include the use of a firewall or a packet filter (such as access lists on a router), which might block the audio in one or both directions.

If one-way audio occurs only through a voice-enabled Cisco IOS gateway, check the configuration carefully. Make sure that IP routing is enabled (look at the configuration to verify that the command **no ip routing** is not present in your configuration).

A bad phone load can also create one-way voice problems. It is important to make sure that you are using the latest gateway and phone loads. Be sure to check the versions that you are using to verify that they are current.



Tip

Check [Cisco Connection Online](http://www.cisco.com) (CCO) at <http://www.cisco.com> for the latest software loads, patches, and release notes.

Digits Not Recognized Correctly

If digits are not being recognized correctly, the **dtmf-relay h245-alphanumeric** command might not have been configured on the dial peers.

For example, a configuration might contain dial peers as follows:

```
dial-peer voice 1 voip
 destination-pattern 2...
 no vad
 codec g711ulaw
 session target ipv4:192.168.1.2
!
```

To configure the dial peers, enter the following commands:

```
MRP#config term
MRP(config)#dial-peer voice 1 voip
MRP(config-dial-peer)#dtmf-relay h245-alphanumeric
MRP(config-dial-peer)#exit
MRP#copy run start
MRP#end
^Z
```

The following is an example of what the dial peer would look like when you execute the command **show running-config** after configuring the **dtmf-relay h245-alphanumeric** command:

```
MRP#show running-config
dial-peer voice 1 voip
 destination-pattern 2...
 no vad
 codec g711ulaw
 dtmf-relay h245-alphanumeric
 session target ipv4:192.168.1.2
!
```

Debugging VoIP Problems

The following are some **debug** commands that are useful when troubleshooting VoIP problems. For additional information about the function and output of each of these commands, refer to [Troubleshoot & Debug VoIP Calls - the Basics](http://www.cisco.com/warp/public/788/voip/voip_debugcalls.html#showcont), at http://www.cisco.com/warp/public/788/voip/voip_debugcalls.html#showcont.



Note

For information about enabling and using **debug** commands, see the “[Enabling debug Commands](#)” section on page 6-20.

- **debug vpm** is used to debug the voice processor module (VPM) telephony interface.
 - **debug vpm all** enables all the debug vpm commands: **debug vpm spi**, **debug vpm signal**, and **debug vpm dsp**.
 - **debug vpm signal** is used to collect debug information for signaling events and can be useful in resolving problems with signaling to a PBX.
 - **debug vpm spi** traces how the voice port module service provider interface (SPI) interfaces with the call control API; displays information about how each network indication and application request is handled.
 - **debug vpm dsp** displays messages from the DSP on the VPM to the MRP and can be useful if the VPM is not functional; checks whether the VPM is responding to off-hook indications and evaluates timing for signaling messages from the interface.

- **debug vpm port** limits the debug output to a particular port; for example, the following shows **debug vpm dsp** messages only for port 1/0:

```
debug vpm port 1/0
```

- **debug vtsp all** enables the following debug voice telephony service provider (VTSP) commands: **debug vtsp session**, **debug vtsp error**, and **debug vtsp dsp**.
 - **debug vtsp dsp** shows messages from the DSP on the V.Fast Class (VFC) modem to the MRP. This command checks whether the VFC is responding to off-hook indications. This is a useful check if you think the VFC may not be functional.
 - **debug vtsp session** traces how the MRP interacts with the DSP, based on the signaling indications from the signaling stack and the requests from the application. This command displays information about how each network indication and application request is processed and provides signaling indications and DSP control messages.
 - **debug vtsp stats** debugs periodic messages sent and received from the DSP requesting statistical information during the call. This command generates a collection of DSP statistics for generating RTP Control Protocol (RTCP) packets.
- **debug voip ccapi inout** traces the call flow through the call control application programming interface (API), which serves as the interface between the call session application and the underlying network-specific software. This command shows call setup and teardown operations performed on both the telephony and network call legs to show how calls are being handled by the MRP.

Debugging H.323 Signaling

Cisco VoIP gateways use H.323 signaling as one method to complete calls. H.323 is made up of three layers of call-negotiation and call-establishment, including the following:

- H.225
- H.245
- H.323

These protocols use a combination of Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) to set up and establish a call.

If you are troubleshooting a call that is failing, and the cause appears to be in the VoIP portion of the call setup, check the H.225 or H.245 TCP portion of the call setup.

Some commands that are useful for debugging the H.225 or H.245 call setup include the following:

- **debug ip tcp transaction** and **debug ip tcp packet** examine the TCP portion of the H.225 and H.245 negotiation. These commands return the IP addresses, TCP ports, and states of the TCP connections.
- **debug cch323 h225** examines the H.225 portion of the call negotiation, that is, the layer 1 portion of the 3-part H.323 call setup. To trace a call to a specific port, you need to know what channel the call is connected to.
- **debug cch323 h245** examines the H.245 portion of the call negotiation, that is, the layer 2 portion of the 3-part H.323 call setup.

To trace a single call, you can run the following **debug** commands:

- **debug h225 event** displays key Q.931 events that occur when placing an H.323 call from one gateway to another. Q.931 events are carried in H.225 messages. This command enables monitoring of Q.931 state changes such as setup, alert, connected, and released.
- **debug h245 event** displays H.245 events.

Solving Problems with Cisco IP Phones

This section describes problems associated with Cisco IP Phones.

For information on how to install, configure, and troubleshoot Cisco IP Phones, refer to the *Cisco IP Phone Administration Guide for Cisco CallManager*.

What to Do First

When problems are reported that might be related to a Cisco IP Phone, the first areas that you should explore for problem determination and resolution include the following:

- If more than one Cisco IP Phone reports a service outage or if there is evidence of degraded service, verify that the Cisco CallManager software is properly configured and otherwise functioning normally.
- Verify that the Cisco IP Phone has power and that it is properly configured.
- Verify that the Cisco IP Phone is properly connected, and inspect the cable for damage.
- If you suspect that there is a problem with the ASI or MRP, see the [“Troubleshooting ASIs, MRPs, and WICs” section on page 3-28](#).

**Note**

For additional information about Cisco CallManager and the Cisco IP Phones, refer to the [Cisco CallManager Troubleshooting Guide](#) and the [Cisco CallManager Serviceability Administration Guide](#).

Troubleshooting IP Phones

Use [Table 9-3](#) to find the possible causes and solutions for problems associated with Cisco IP Phones.

Table 9-3 Cisco IP Phone Problems and Solutions

Symptom	Possible Cause	Solutions
A working Cisco IP Phone stops functioning when it is moved to a new physical location. Status code 04025 is displayed when you press **.	There is a connectivity problem between the Cisco IP Phone and the IP network. The Cisco IP Phone may be using a static address, preventing the network from communicating with it in its new location. (This applies only to the Cisco 30VIP and 12SP+ phones, not to newer models such as the Cisco IP Phone 7960.)	If the Cisco IP Phone is configured to use a static IP address, modify its IP address to reflect the new location. (Refer to the “Configuring and Verifying Network Settings on the Cisco IP Phone” chapter in the <i>Cisco IP Phone Administration Guide for Cisco CallManager</i> .)
A Cisco IP Phone does not accept a new static IP address.	User input error during Cisco IP Phone configuration. (This applies only to the Cisco 30VIP and 12SP+ phones, not to newer models such as the Cisco IP Phone 7960.)	When configuring the Cisco IP Phone, after you enter the last octet of the IP address, make sure to press the asterisk (*) key, not the number sign (#) key. Pressing the * key saves your configuration.
Users of a Cisco IP Phone hear a crackling noise on both the handset and the speakerphone.	Power problem.	Verify that there are no problems with the Catalyst 3524-PWR XL that is powering the Cisco IP Phone. (Refer to the <i>Catalyst 3500 Series XL Hardware Installation Guide</i> .)

Table 9-3 Cisco IP Phone Problems and Solutions (continued)

Symptom	Possible Cause	Solutions
Users of a Cisco IP Phone hear echo.	<ul style="list-style-type: none"> • Speakerphone use, or headset volume too high. • A noisy line is causing reflection. • The type of gateway being used. 	<ul style="list-style-type: none"> • Check the volume level on the speakerphone, and check the headset level (start at 50% of the maximum audio level). • Adjust the receive level so that any reflected audio is reduced further. Make adjustments in small increments. • Contact your carrier, and request to have the lines checked. On a typical T1/PRI circuit, the input signal should be -15 dB. • Verify your gateway and phone loads to ensure that they are at the most current levels. • If the listener on the opposite end of the connection hears echo, contact your telephone service provider to determine the type of gateway being used and the level of echo cancellation.

Cisco IP Phone Connections to the Cisco ICS 7750

This section describes situations in which Cisco IP Phones might not be able to connect successfully to the Cisco ICS 7750.

Cisco IP Phones attached to the Cisco ICS 7750 are not updated with the IP address of a new or replacement SPE under the following circumstances:

- If you replace an SPE that is running Cisco CallManager



Note

When you replace an SPE, it is assigned an IP address that is different from the IP address of the SPE that was in the same chassis slot.

- If you change the IP address of an SPE that is running Cisco CallManager, using ICSCconfig

Because Cisco CallManager acts as a TFTP server, if Cisco IP Phones cannot contact an SPE on which Cisco CallManager is running, you might need to update the affected Cisco IP Phones with the new SPE IP address.

To solve this problem, complete the following steps:

Step 1 Access Cisco CallManager

Step 2 Choose **System > Cisco CallManager Group**.

The Cisco CallManager Group Configuration page opens.

Step 3 In the pane on the left side of the window, click **Default**.

The screen refreshes, displaying the Default Cisco CallManager Group.



Caution

Restarting devices causes them to drop calls. Be sure to alert users, if possible

Step 4 Click **Reset Devices**.

Configuring the Cisco IP Phone 7960

The Cisco IP Phone 7960 is a network device and has many configurable network settings. Certain options must be configured before the phone is accessible and usable.

By default, network configuration options are locked to prevent unauthorized changes that could impact network connectivity.

To unlock the network configuration options, follow these steps:

-
- Step 1** Press the **Settings** button
 - Step 2** Press ****#**.
The network configuration options are unlocked.
 - Step 3** To verify the unlocked state, select **Network Configuration**.
 - Step 4** Examine the upper-right portion of the Cisco IP Phone LCD display. The padlock icon shows as unlocked.
-

To change network configuration settings, follow these steps:

-
- Step 1** Press the **Settings** button.
 - Step 2** Scroll to Network Configuration.
 - Step 3** Press the **Select** soft key.
 - Step 4** Scroll through the options to display the information as shown in [Table 9-4](#).
-

Table 9-4 Cisco IP Phone 7960 Network Settings

Network Setting	Description	Usage Notes
DHCP Server (Dynamic Host Configuration Protocol)	IP address of the DHCP server the phone used to obtain its IP address	Cannot be configured locally
BOOTP Server (Bootstrap Protocol)	Indicates whether the phone obtained its IP configuration from a BOOTP server	Displays Yes or No; cannot be configured
MAC Address (Media Access Control)	MAC address of the phone	Cannot be configured
Host Name	Host name assigned to phone	Cannot be configured locally
Domain Name	Name of the DNS domain in which the phone resides	
IP Address	IP address of the phone	
Subnet Mask	Subnet mask used by the phone	
TFTP Server (Trivial File Transfer Protocol)	TFTP server used by the phone to obtain config files	
Default Routers 1–5	Default gateway used by the phone	
DNS Servers 1–5	DNS server used by the phone to resolve host names of the TFTP server and Cisco CallManager	
Operational VLAN (Virtual Local Area Network)	VLAN in which the phone is a member; obtained through Cisco Discovery Protocol (CDP)	Cannot be configured locally
Administrative VLAN	Assigns the phone to an auxiliary VLAN; used in non-Cisco switched networks	
CallManager 1–5	CallManagers available for this phone's call processing	Cannot be configured locally
DHCP Enabled	Indicates whether DHCP is being used by the phone	

Table 9-4 Cisco IP Phone 7960 Network Settings (continued)

Network Setting	Description	Usage Notes
DHCP Address Released	Allows release of the IP address assigned by DHCP	
Alternate TFTP	Indicates the phone is using an alternate TFTP server	
Erase configuration	Allows locally assigned settings on the phone to be erased and values reset to default settings	

Disabling DHCP and Configuring a Static Network Address

If DHCP is not being used for the Cisco IP Phone 7960, follow the procedures listed in the following sections to configure a static network address:

- [Disabling DHCP, page 9-34](#)
- [Assigning a Static IP Address, page 9-35](#)
- [Assigning the Default Gateway, page 9-36](#)
- [Assigning the Subnet Mask, page 9-36](#)
- [Assigning a TFTP Server, page 9-37](#)

Disabling DHCP

Follow these steps to disable DHCP on a Cisco IP Phone 7960:

-
- Step 1** Press the **Settings** button.
 - Step 2** Scroll to Network Configuration.
 - Step 3** Press the **Select** soft key.
 - Step 4** Scroll to DHCP Enabled.

If DHCP is enabled, the screen displays as follows:

```
DHCP Enabled YES
```

Step 5 Press the **No** soft key to disable DHCP.

Continue with the [“Assigning a Static IP Address”](#) section on page 9-35.

Assigning a Static IP Address

When you assign static IP addresses on a Cisco IP Phone 7960, note the following:

- You can use 0.0.0.0 for the subnet mask only if the default gateway is also 0.0.0.0.
- The TFTP server must have an IP address.
- The default gateway IP address must be on the same subnet as the host IP address.

Follow these steps to assign a static IP address:

Step 1 Press the **Settings** button.

Step 2 Scroll to Network Configuration.

Step 3 Press the **Select** soft key.

Step 4 Scroll to IP Address.

Step 5 Press the **Edit** soft key.

Step 6 Use the buttons on the dial pad to enter a new IP address, using the asterisk (*) key on the dial pad or the period (.) soft key to enter periods (or dots).

Step 7 Press the << soft key to delete any mistakes.

Step 8 Press the **Validate** soft key.

Continue with [Assigning the Default Gateway](#).

Assigning the Default Gateway

If an IP address is manually defined for the Cisco IP Phone 7960, the default gateway must also be defined. Follow these steps:

-
- Step 1** Press the **Settings** button.
 - Step 2** Scroll to Network Configuration.
 - Step 3** Press the **Select** soft key.
 - Step 4** Scroll to Default Router 1.
 - Step 5** Press the **Edit** soft key.
 - Step 6** Use the buttons on the dial pad to enter the new router IP address.
 - Step 7** Press the **Validate** soft key.
 - Step 8** Repeat Step 3 through Step 7 to add Default Router 2-5 as backup gateways.
-

Continue with the [“Assigning the Subnet Mask”](#) section on page 9-36.

Assigning the Subnet Mask

To assign a subnet mask for the Cisco IP Phone 7960, follow these steps:

-
- Step 1** Press the **Settings** button.
 - Step 2** Scroll to Network Configuration.
 - Step 3** Press the **Select** soft key.
 - Step 4** Scroll to Subnet Mask.
 - Step 5** Press the **Edit** soft key.
 - Step 6** Use the buttons on the dial pad to enter a new subnet mask
 - Step 7** Press the **Validate** soft key.
-

Continue with the [“Assigning a TFTP Sever”](#) section on page 9-37.

Assigning a TFTP Sever

The default TFTP Server on the Cisco IP Phone 7960 is set to CiscoCM1. When not using DHCP, you must manually assign the TFTP server to the Cisco IP Phone. To assign the TFTP server, follow these steps:

-
- Step 1** Press the **Settings** button.
 - Step 2** Scroll to Network Configuration.
 - Step 3** Press the **Select** soft key.
 - Step 4** Scroll to TFTP Server.
 - Step 5** Press the **Edit** soft key.
 - Step 6** Use the buttons on the dial pad to enter a new TFTP server.
 - Step 7** Press the **Validate** soft key.
 - Step 8** Press the **Save** soft key to save all changes.
-

The following message sequence appears on the Cisco IP Phone 7960 as it comes up after a power recycle:

```
Configuring VLAN
Configuring IP
Configuring CM List
Connecting
Registering
Requesting Template
```

Obtaining Status and Version Information

Status information about a current call and the network can be obtained directly from the Cisco IP Phone 7960. Information on the installed firmware version can also be obtained directly from the Cisco IP Phone.

To display statistics for an active call, press the **i** button twice rapidly. The following information displays:

- RxType—Type of voice stream received (G.729, G.711 U-law, or G.711 a-law).

- RxSize—Size of the voice packets (in milliseconds) in the receiving voice stream.
- RxCnt—Number of RTP voice packets received since the voice stream was opened (this number may not be the same as the number received since the call began, because calls can be put on hold).
- TxType—Type of voice stream transmitted (G.729, G.711 U-law, or G.711 a-law).
- TxSize—Size of the voice packets (in milliseconds) in the transmitting voice stream.
- TxCnt—Number of RTP voice packets transmitted since the voice stream was opened (this number may not be the same as the number received since the call began, because calls can be put on hold).
- Avg Jtr—Estimated average jitter (dynamic delay that a packet encounters when going through the network) observed since the receiving voice stream was opened.
- Max Jtr—Maximum jitter observed since the receiving voice stream was opened.
- RxDiscard—Number of RTP packets in the receiving voice stream that have been discarded.

Status Messages

You can use status messages to diagnose network configuration problems. To view status messages, follow these steps:

-
- Step 1** During a call, press the **Settings** button.
 - Step 2** Scroll to Status, and press the **Select** soft key.
 - Step 3** Scroll to Status Messages, and press the **Select** soft key again.

Any of the following messages might be displayed:

- DHCP timeout—DHCP server did not respond.
- TFTP timeout—TFTP server did not respond.
- TFTP file not found—Requested file was not found in the TFTP Path directory.
- TFTP access error—TFTP server is pointing to a directory that does not exist.

- TFTP general error—All other TFTP failures.
 - DNS unknown host—DNS could not resolve the name of the TFTP server or Cisco CallManager.
 - DNS timeout—DNS server did not respond.
 - No DNS server IP—Name was specified, but DHCP or static IP configuration did not specify a DNS server address.
 - Load ID incorrect—Load ID of the software file is of the wrong type.
 - Checksum Error—Downloaded software file is corrupted.
 - SEPDefault.cnf or SEPMacaddress—Name of the configuration file.
 - No default router—DHCP or static configuration did not specify a default router.
 - Duplicate IP—Another device is using the IP address assigned to the phone.
-

Displaying Network Statistics

Network statistics provide information about the phone and network performance. To view network statistics, follow these steps:

-
- Step 1** Press the **Settings** button.
 - Step 2** Scroll to Status, and press the **Select** soft key.
 - Step 3** Scroll to Network Statistics, and press the **Select** soft key.

The following lists text messages that might display on the phone's LCD screen:

- RCV—Number of packets received at the phone.
- XMT—Number of packets transmitted from the phone.
- REr—Number of receive errors at the phone.
- Bcast—Number of broadcast packets received.
- TCP-timeout—Connection closed due to exceeding the allowed retry time.
- TCP-Bad-ACK—Connection was cleaned up because an unacceptable ACK was received.
- CM-reset-TCP—Cisco CallManager closed and initiated the closing of connection.

- CM-closed-TCP—Cisco CallManager closed and initiated the closing of connection.
 - CM-aborted-TCP—Cisco CallManager closed and initiated the closing of connection.
 - CM-NAKed—Cisco CallManager refused the connection attempt.
 - KeepaliveTO—Phone closed because of a Keepalive Timeout.
 - Failback—Phone closed to failback to a higher priority Cisco CallManager.
 - Phone-Loading—Phone closed to upgrade software. This text message appears only if TFTP fails during software upgrade.
 - Phone-Keypad—Phone closed due to a **** reset.
 - Phone-Re-IP—Phone closed due to a duplicate IP address condition.
 - Reset-Reset—Phone closed due to receiving a Reset/Reset from web admin.
 - Reset-Restart—Phone closed due to receiving a Reset/Restart from web admin.
 - All-CMs-Bad—Phone detected a state in which all Cisco CallManagers failed their keepalives and were marked bad.
 - Phone-Reg-Rej—Phone closed due to receiving a Registration Reject.
 - Phone-Initialized—Phone has not experienced a connection close since the hardware reset or since it was powered on.
 - Elapsed time—The amount of time that has elapsed since the phone connected to Cisco CallManager.
 - Port 0 Full, 100—Network port is in a link-up state and has auto-negotiated a full-duplex 100 Mbps connection.
 - Port 0 Half, 10—The network port is in a link-up state and has auto-negotiated a half-duplex, 10-Mbps connection.
 - Port 1 Full, 100—The PC port is in a link-up state and has auto-negotiated a full-duplex 100-Mbps connection.
 - Port 2 Down—PC port is in a link-down state.
-



Note For additional information about Cisco IP Phone administration, refer to the [*Cisco IP Phone Administration Guide for Cisco CallManager*](#).

Verifying Firmware Version

The firmware version loaded on the Cisco IP Phone 7960 can be verified by following these steps:

-
- Step 1** Press the **Settings** button.
 - Step 2** Scroll to Status.
 - Step 3** Press the **Select** soft key.
 - Step 4** Choose **Firmware Revisions**.

Firmware Revisions information is displayed that includes

- Application Load—firmware load specified by the Cisco CallManager database
- Boot Load—firmware load installed on phone during manufacturing



Note The firmware version on the phone can be updated only through Cisco CallManager.

Resetting the Cisco IP Phone 7960 and Erasing the Configuration

The Cisco IP Phone 7960 can be reset at any time by pressing ****#****, which will cause the phone to cycle through its normal startup procedures. To erase locally stored configuration options and user-defined changes on the Cisco IP Phone 7960, follow these steps:

-
- Step 1** Press the **Settings** button.
 - Step 2** Scroll to Network Configuration.
 - Step 3** Press the **Select** soft key.

- Step 4** Scroll to Erase Configuration.
If the configuration is not set to be erased, the option displays as follows:
Erase Configuration No
- Step 5** Press the **Yes** soft key to erase the configuration.
- Step 6** Press the **Save** soft key.
- Step 7** You may reset options as described in the “[Disabling DHCP and Configuring a Static Network Address](#)” section on page 9-34.

Solving Problems with VICs, VWICs, and Trunks

This section describes problems associated with VICs and VWICs installed in ASI81s and MRPs and the trunks connected to VICs and VWICs.



Note

For additional information on VICs, WAN interface cards (WICs), VWICs, and LED information, refer to the [Cisco Interface Cards Installation Guide](#).

Troubleshooting VICs and VWICs

[Table 9-5](#) lists symptoms for problems associated with DSPs. DSPs are microprocessors that MRPs use to handle voice-processing tasks such as compression.

Table 9-5 VIC/VWIC Problems and Causes

Syslog Message	MRP LED Status Change	Possible Cause
DSPALARM, VTSP (All calls through affected VIC are dropped)	ALARM: on (amber)	DSP VTSP error
DSPALARM, HTSP (All calls through affected VIC are dropped)	None	DSP HTSP error

To resolve either of these problems:

- Verify that the DSP is functioning properly by placing a call through the affected voice interface.
- Copy the error message exactly as it appears. Also collect information from the **show version** and **show running-configuration** commands. Then contact your technical support representative.

Troubleshooting Unrecognized VICs

This section describes how to troubleshoot an MRP that does not recognize VICs.

Cisco voice-enabled routers, including the MRP in the Cisco ICS 7750, require the installation of a packet voice data module (PVDM) to support VICs. The PVDM contains the DSPs that make the card fully functional.



Note

For information about supported VICs, refer to the [Cisco ICS 7750 Installation and Configuration Guide](#).

The MRP may not recognize a VIC as a result of one or more of the following:

- Incorrect Cisco IOS version
- Absence of a PVDM (or sufficient PVDMs)
- Faulty VIC, or VIC not properly seated in the chassis

Follow these steps to troubleshoot an unrecognized VIC:

- Step 1** Verify that the correct Cisco IOS software is installed on the MRP.
- The Cisco IOS “IP Plus Voice” feature set is required for voice. Check the version of MRP software that was included with your Cisco ICS 7750 package to verify that you are running the appropriate version.
- Step 2** Verify that the MRP recognizes the VIC. At the MRP command prompt, enter the **show hardware** or **show diag** command. The following example output is from the **show hardware** command (the VIC is highlighted):

```
MRP2#show hardware
Cisco Internetwork Operating System Software
IOS (tm) ICS7700 Software (ICS7700-SV3Y-M), Version 12.2(4)XL1, EARLY
DEPLOYMENT RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
```

```

Copyright (c) 1986-2001 by cisco Systems, Inc.
Compiled Thu 22-Nov-01 01:05 by ealyon
Image text-base: 0x80008124, data-base: 0x80D73708

ROM: System Bootstrap, Version 12.0(20000705:170114)
[mtluong-ics7750-MRP200-ROM102], DEVELOPMENT SOFTWARE
ROM: ICS7700 Software (ICS7700-SV3Y-M), Version 12.2(4)XL1, EARLY
DEPLOYMENT RELEASE SOFTWARE (fc1)

MRP2 uptime is 6 weeks, 1 day, 3 hours, 25 minutes
System returned to ROM by power-on
Running default software
cisco ICS7750-MRP200 (MPC860T) processor (revision 0x602) with
52429K/13107K bytes of memory.
Processor board ID JAD0440057B (2956515537), with hardware revision
0000
MPC860T processor: part number 0, mask 32
Bridging software.
X.25 software, Version 3.0.0.
Primary Rate ISDN software, Version 1.1.
1 FastEthernet/IEEE 802.3 interface(s)
24 Serial network interface(s)
2 Channelized T1/PRI port(s)
2 Voice FXS interface(s)
32K bytes of non-volatile configuration memory.

Configuration register is 0x1

```

**Note**

You can also see voice ports in the output of the **show running-config** command.

Step 3

If the VIC is not recognized, verify that there are sufficient PVDMS installed. Use the **show diag** command to display information about the hardware interfaces. The following output shows the portion of this command that shows an installed PVDM-20 (5 DSPs):

```

MRP2#show diag
Slot 0:
ICS7750-MRP200 Mainboard Port adapter, 5 ports
  Port adapter is analyzed
  Port adapter insertion time unknown
  EEPROM contents at hardware discovery:
  Hardware Revision       : 6.2
  PCB Serial Number       : JAD0440057B
  Part Number             : 73-4341-08
  Board Revision          : A0
  Fab Version             : 06

```

```

        EEPROM format version 4
        EEPROM contents (hex):
Packet Voice DSP Module Slot 0:
    Hardware Revision      : 2.2
    Part Number           : 73-4793-02
    Board Revision        : 01
    Deviation Number      : 0-0
    Fab Version           : 02
    PCB Serial Number     : ICP0442007M
    RMA Test History      : 00
    RMA Number            : 0-0-0-0
    RMA History           : 00
    Processor type        : D2
    Number of DSP's       : 5
    DSP memory size(in kwords): 256
    Type of DSP           : Unknown (210)
        EEPROM format version 4
        EEPROM contents (hex):

```

If you see the following output, it means that the PVDM is not being recognized by the MRP:

```

MRP2#show diag
...Packet Voice DSP Module Slot0:
Not populated...

```

- Step 4** If the MRP still does not recognize the VIC, reseal the VIC to make sure it is properly installed in the chassis. If that does not resolve the problem, then replace the VIC.
-

Trunk Guidelines

Trunks connect the Cisco ICS 7750 to other private branch exchanges (PBXs) (or similar equipment) or to the CO at the telephone service provider. A trunk may go down temporarily and come back up shortly without intervention. However, if the trunk remains down or if it transitions constantly in and out of service, you must find and correct the problem. Use the loopback tests described in this section to isolate the faulty component. A loopback test is a software or hardware test that alters the flow of data so that an electronic signal is returned to its sender.

Trunks can be directly connected, or they can be connected with data service unit/channel service unit (DSU/CSU) devices through telephone lines. A trunk interface loop occurs in the circuitry within the Cisco ICS 7750 and does not involve components external to the system.

Most trunk failures are temporary; they are caused by problems on the telephone company line. A trunk is usually returned to service within 3 minutes without any intervention on your part and before the telephone company finds anything wrong. If a trunk is reported down, you should wait at least 10 minutes to make sure that the problem is not temporary.

If the trunk does not come up within 10 minutes, identify the failed portion of the trunk. To do this, run a series of loopback tests to segment the trunk from end to end, starting at the ASI or MRP connected to it and progressing outward from the Cisco ICS 7750. This process tests each segment in sequence to find the exact location of the failure.



Note

For information about loopback tests over serial lines, see the [“Using Loopback Tests” section on page 6-31](#). For information about solving problems with VICs, see the [“Troubleshooting ASIs, MRPs, and WICs” section on page 3-28](#).

Troubleshooting T1 Trunk Problems

[Table 9-6](#) lists symptoms and possible solutions for problems associated with T1 trunks and the VICs or VWICs connected to them.

Table 9-6 T1 Trunk Problems and Solutions

Symptom or Syslog Message	MRP LED Status Change	Possible Cause
INITFAILURE, E1T1_MODULE	ALARM: on (amber)	Error detected by T1 driver during initialization
T1:HWIDBFAILED	ALARM: on (amber)	No HWIDB registered for serial T1 interface

To solve either of these problems, copy the error message exactly as it appears. Also, collect information from the **show version** and **show running-config** commands. Then contact your technical support representative.

Troubleshooting ISDN Problems

Table 9-7 lists symptoms and possible solutions for problems associated with Integrated Services Digital Network (ISDN) and ISDN VICs.

Table 9-7 ISDN Problems and Solutions

Symptom or Syslog Message	MRP LED Status Change	Possible Cause	Solutions
INITFAIL, BRI	ALARM: on (amber)	BRI initialization error	Copy the error message exactly as it appears. Also collect information from the show version and show running-configuration commands. Then contact your technical support representative.
REPEATEDRESET, SERVICE_MODULE	ALARM: on (amber)	BRI VIC not responding	Copy the error message exactly as it appears. Also collect information from the show version and show running-configuration commands. Then contact your technical support representative.
UNSUPPORTED_CONFIG, PQUICC	ALARM: on (amber)	Invalid BRI VIC combination installed in MRP	<ul style="list-style-type: none"> Determine which VICs are installed. Replace one of the BRI VICs with a different type of VIC.
NOMEMORY, BRI	None	Insufficient memory for BRI operations	<ul style="list-style-type: none"> Reduce other system activity to decrease memory demands. Install a memory upgrade in the MRP (refer to <i>Installing Memory, PVDM, and VPN Modules in ASI Cards, MRP Cards, and SPE Cards in the Cisco ICS 7750</i>).

