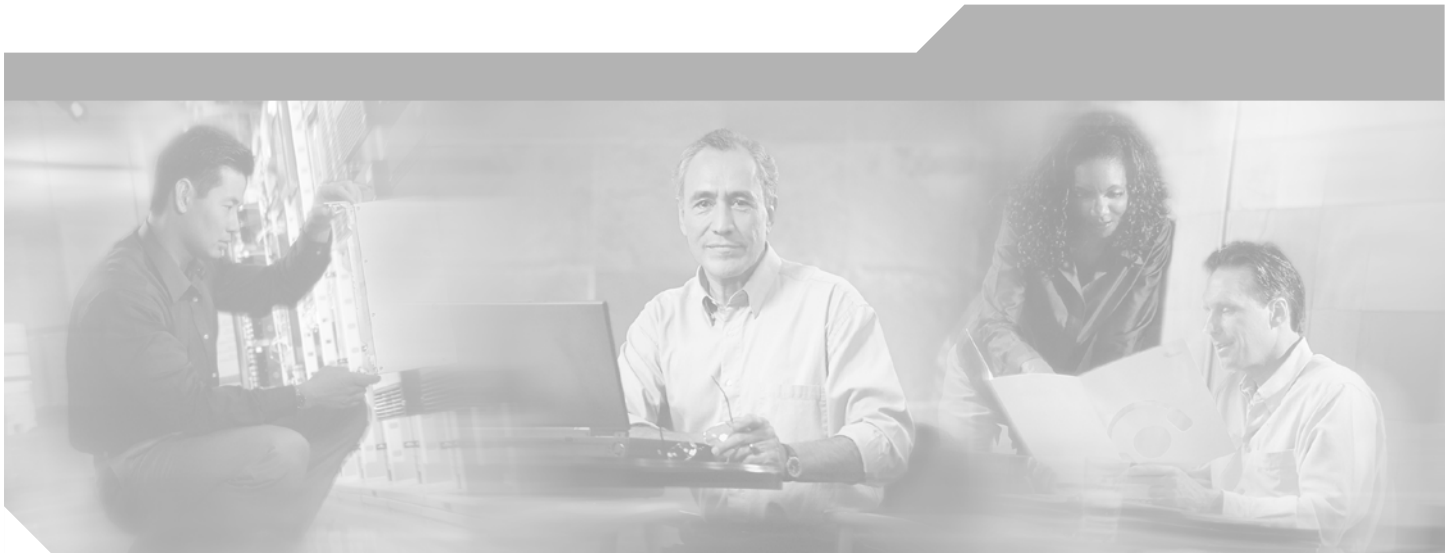


Cisco Land Mobile Radio over IP Solution Reference Network Design

Cisco IOS Software Release 12.4(2)T1
March 2006

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

CONTENTS

Preface

This document provides design considerations and guidelines for implementing Cisco Land Mobile Radio (LMR) over IP solutions

The LMR over IP services described in this guide are based primarily on enhancements made to the signaling operation of the ear and mouth (E&M) digital and analog voice interfaces present on Cisco IOS software-based gateway routers. Cisco IOS software provides a wide array of voice features on gateway routers.

Note This guide describes the results of interoperability testing between the LMR feature and other voice features. Features not mentioned have not been tested, and thus their interoperability with the LMR feature may differ from the intended operation. In addition, the LMR services described here have not been tested on a large scale such as might be seen in typical installations.

DISCLAIMER:

CISCO IOS FEATURES FOR LAND MOBILE RADIO (LMR) OVER IP SHALL BE REFERRED TO HEREINAFTER AS “CISCO LMR FEATURES.”

ALL CISCO CUSTOMERS USING THE CISCO LMR FEATURES, ESPECIALLY CUSTOMERS RESPONSIBLE FOR ENSURING PUBLIC SAFETY, ARE STRONGLY ENCOURAGED TO SEEK TECHNICAL SUPPORT FROM A CISCO CERTIFIED SYSTEM INTEGRATOR PARTNER TO ENSURE PROPER CONFIGURATION AND/OR IMPLEMENTATION OF THE CISCO LMR FEATURES INTO THEIR LAND MOBILE RADIO SYSTEMS.

WITH SOLE RESPECT TO THE CISCO LMR FEATURES THEMSELVES, CISCO WILL PROVIDE TECHNICAL SUPPORT IN ACCORDANCE WITH CISCO'S STANDARD POLICIES AND PROCEDURES FOR PROVIDING SUPPORT FOR ANY OTHER CISCO IOS FEATURES. NOTWITHSTANDING THE FOREGOING, IN NO EVENT SHALL CISCO BE HELD RESPONSIBLE FOR PROVIDING ANY TECHNICAL SUPPORT FOR ANY LAND MOBILE RADIO SYSTEMS.

CISCO MAKES NO WARRANTIES, CONDITIONS, OR REPRESENTATION OF ANY KIND, EITHER EXPRESS OR IMPLIED, WITH RESPECT TO ANY LAND MOBILE RADIO SYSTEMS. CISCO SHALL NOT ACCEPT OR ASSUME ANY RESPONSIBILITY OR LIABILITY WITH REGARDS TO ANY THIRD PARTY PRODUCTS OR SERVICES.

Purpose

The purpose of this document is to equip those responsible for incorporating the LMR over IP services in existing or new networks with the design and implementation tools necessary to complete the tasks. This document contains elements from the following sources to provide a comprehensive resource for implementing LMR services:

- *Land Mobile Radio over IP* feature documentation
- Cisco Architecture for Voice, Video and Integrated Data (AVVID) documents
- Other sources

In addition, protocol flows, packet decodes, state diagrams and other detailed analyses augment the component documentation to assist implementors in designing scalable solutions. The level of detail provided should also help those troubleshooting networks both during and after installation.

The Cisco IP Interoperability and Collaboration System (Cisco IPICS) and the Push-to-Talk Management Center (PMC) application enable integrated communications among disparate LMR systems. For more information about the Cisco IPICS system, see the documentation that is available on the Interoperability Systems Support Resources website at the following link:

http://www.cisco.com/en/US/products/ps6712/tsd_products_support_category_home.html

Audience

This document is intended for use by system integrators, sales engineers, customer support engineers, and anyone else responsible for the design and implementation of LMR over IP services in a network environment. Some readers who have a strong background in the LMR environment, might have limited exposure to data and voice networking. Conversely, some readers with strong data and voice networking backgrounds might have a limited understanding of LMR. This guide bridges the gap between those two realms of knowledge by explaining certain elements of one technology with appropriate reference to the other.

A basic set of knowledge is required to understand each element in the set of LMR over IP services, with additional skills required depending on the service implemented. A successful implementation will require knowledge in the following areas:

- Operational knowledge of the radio systems to be networked, including wired interface characteristics
- Provisioning voice services on Cisco IOS software-based voice gateways

Installations may also require skills in:

- Configuring the Cisco CallManager or Cisco CallManager Express services
- Installation and maintenance of Microsoft Windows 2000 Server
- Secured IP communications (Cisco IOS IPSec, firewall configuration)

Revision History

The following table lists the revision history for this document.

Revision Date	Comments
Spring 2004	Initial release.
Spring 2006	Remove references to Twisted Pair Solutions and WAVE. Add reference to Cisco IPICS.

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a comprehensive library of technical product documentation on a portable medium. The DVD enables you to access multiple versions of installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the same HTML documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .PDF versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Ordering Documentation

Registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

http://www.cisco.com/go/marketplace/

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can submit comments about Cisco documentation by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For Emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- For Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT at the aforementioned e-mail addresses or phone numbers before sending any sensitive material to find other means of encrypting the data.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is down, or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired, while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco offerings. To order and find out more about the Cisco Product Quick Reference Guide, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

LMR over IP Overview

Overview

A Land Mobile Radio (LMR) system is a collection of portable and stationary radio units designed to communicate with each other over predefined frequencies. They are deployed wherever organizations need to have instant communication between geographically dispersed and mobile personnel. Typical LMR system users include public safety organizations such as police departments, fire departments, and medical personnel. However, LMR systems also find use in the private sector for activities like construction, building maintenance, and site security.

In typical LMR systems, a central dispatch console or base station controls communications to the disparate handheld or mobile units in the field. The systems might also employ repeaters to extend the range of communications for the mobile users. LMR systems can be as simple as two handheld units communicating between themselves and a base station over preset channels. Or, they can be quite complex, consisting of hundreds of remote units, multiple dispatch consoles, dynamic channel allocation, and other elements.

Issues

LMR systems have proven a very useful tool to many types of organizations. However, recent events have exposed limitations in the ability of LMR systems to fulfill certain communications needs, particularly system interoperability. By combining LMR systems with the connectivity of IP networks, we can solve many limitation problems.

Interoperability

Within an organization, the radio systems tend to be homogenous, with most elements typically purchased from the same manufacturer. Although the electromagnetic spectrum is rather vendor agnostic, signaling mechanisms and other control aspects of individual radio systems can be quite proprietary. This proprietary factor means that adding equipment generally means purchasing from the same manufacturer or finding compatible equipment, assuming that it still manufactures that particular model of radio. If organizations merge or need to consolidate operations that were previously using different LMR systems, issues with interoperability could require workarounds to bridge the existing systems or ultimately require the purchase of all new equipment.

Interoperability issues within an organization are one aspect of the problem. Consider the situation in which multiple public safety organizations are involved with the same incident. Organizations enjoy the autonomy of using their own radio systems with their own channels. But autonomy implies that the

radios for one group will not be able to communicate with radios used by other groups. So, coordinating the activities of the field personnel from these different groups at one site requires some sort of workaround, either redeploying radios, or some sort of custom cross-patching at dispatch consoles to bring parties together.

Extending Command and Control

Closely associated with interoperability issue is the ability to extend the command and control function of radio systems. Generally, providing someone with the ability to participate in a radio talk group means giving that person a radio. However, if the radio user is out of range of the radio system or is an infrequent user of this capability, that solution might be physically or economically unfeasible. Today, radio systems can be linked through leased lines or over the public telephone network to extend their reach. These lines can be expensive and are often in addition to the communication services run for data purposes.

LMR over IP Service

With the LMR over IP service, standards-based VoIP technology voice gateways are used in combination with additional LMR specific features to address interoperability, extending command and control, and other issues. Base stations, repeaters, and dispatch consoles generally possess a wired interface that can be used to monitor audio received from their air interface, and as input for audio to be transmitted on their air interface. Although this wired interface may contain other control capabilities as well, as long as it has some sort of speaker output and microphone input, it can be connected to a voice port on a router.

The audio received on the voice port is encoded with a standard audio codec, such as G.711 or G.729. Those audio samples are packaged in standards-based Real-Time Transport Protocol (RTP) packets suitable for transport on an IP network. At this point, the communication element is abstracted from the distinctive characteristics of each radio system, thus providing a solution for the interoperability problem. Now, these audio packets can be sent across the network to other LMR gateways with different brands of radio systems either individually (unicast) or as a group (multicast).

The recipient of the audio packets need not be another LMR gateway. It can be any device capable of receiving and decoding the RTP stream, such as an IP telephone or PC with appropriate software. The IP network and IP-enabled devices can be used to allow users to monitor or transmit on a particular radio channel from a desk without issuing another radio. This can be done locally, nationally, or internationally, assuming the IP network has been properly designed.

CHAPTER 2

Services and Components

The variety of radio systems, desired participants, and operational needs of an organization cannot be satisfied by one Land Mobile Radio (LMR) over IP architecture. So, instead of having an omnibus architecture, LMR over IP is broken down into a series of services. Some of these services are implemented by means of the Cisco gateway routers running Cisco IOS software with the LMR over IP feature set. Some services employ Cisco IP telephony equipment such as Cisco IP Phones and Cisco CallManager.

The following sections outline these LMR over IP services, providing a description of how and when they may be used to achieve a more efficient, elegant, or scalable solution for LMR needs. It is important to understand that these tools are not exclusive of each other. In many cases they can be quite complementary. The actual details of configuration, traffic flow, and any caveats for these services are described in Chapter 5, "Enhanced Services."

This chapter describes the following LMR over IP services and components:

Interoperability—The Radio Interface Adaption Layer

The foundation on which all LMR services are built is the interface joining the LMR radio systems to the IP network. The key to implementing all these other services is to adapt the disparate LMR endpoints to a common standard. The radio systems are connected through available wired connection points and not through their air interface. The radios are connected to the LMR-enabled Cisco gateway routers through either an analog ear and mouth (E&M) interface or a digital T1 interface. LMR-specific enhancements to Cisco IOS software provide greater flexibility in controlling audio levels, tuning voice activity detection (VAD), and improving the ability of the router to interact with those radios that employ physical signaling. For those radio systems that utilize in-band tones for signaling, additional hardware such as third-party tone remote units are required to adapt the radio to the IP environment.

With all participants using the same communications structure, any-to-any communication is now possible. Tone controlled systems can communicate with systems using other tone schemes, or systems using physical signaling. Organizations can merge different radio systems onto one common backbone, and they are freed from being tied down to one particular vendor or solution for their radio needs.

Transport

Once the radio system is connected to the network, the audio transmission needs to be sent to and from other endpoints. These three mechanisms for accomplishing this task are discussed in the following sections:

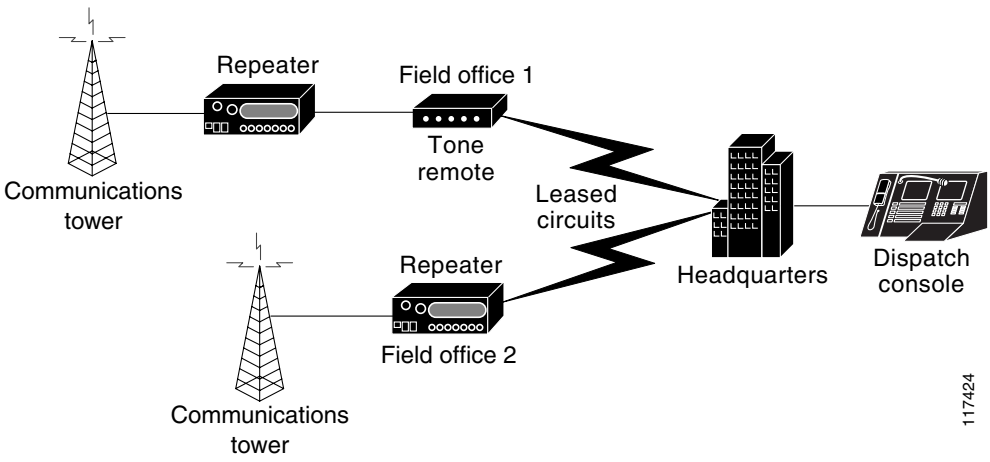
Unicast Connection Trunk (Leased Line Replacement)

In LMR deployments topography, distance or other environmental factors can limit the coverage of the network. In some situations, leased lines or other dedicated point-to-point transmission facilities are used to connect geographically remote devices. By using a unicast connection trunk configuration on the LMR gateway, organizations can leverage standard IP connectivity over either the public Internet, or a private network to backhaul their LMR traffic and provide data connectivity at these remote sites. In this manner, the organization can achieve cost savings through either reduced facility charges or a reduction in the number of required connections at the site.

The unicast connection trunk service on the LMR gateway provides a permanent point-to-point connection between two voice endpoints. It uses standard H.323 signaling to establish the VoIP circuit between the gateways. This circuit is capable of not only sending audio information using standard Real-Time Transport Protocol (RTP) datagrams, but of physical lead state signaling as well.

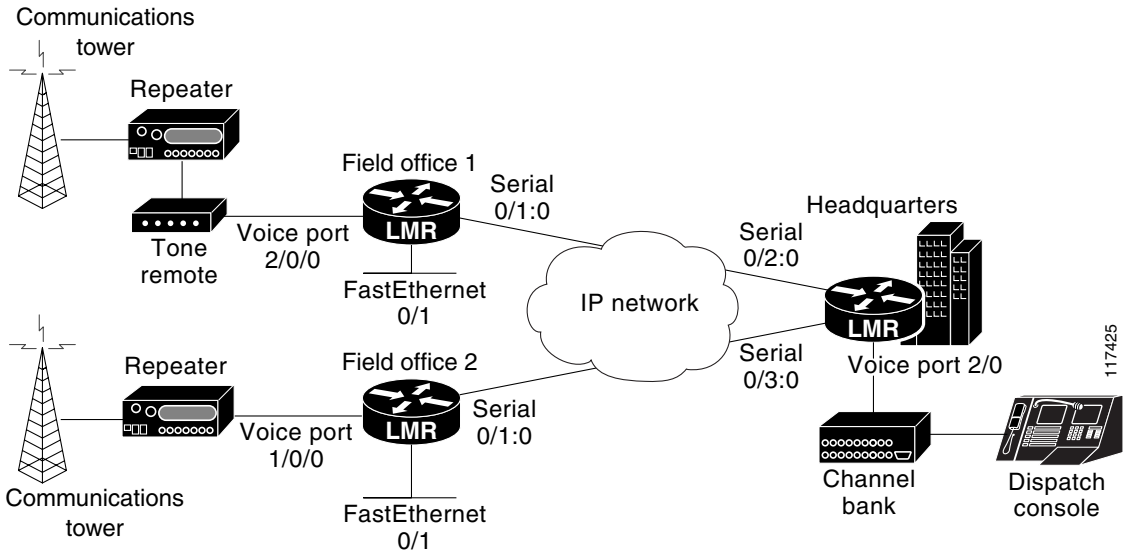
Figure 2-1 shows a representative topology for a traditional configuration with a dispatch console in headquarters connecting to repeaters in the field offices over leased circuits.

Figure 2-1 Traditional Leased Line Implementation



In Figure 2-2, we have connected each of the LMR components to an LMR gateway and connected the gateways through an IP cloud. Again, this IP connectivity could be achieved by leveraging the same leased circuit we saw in Figure 2-1 or through connections to the Internet through a service provider. With the configuration shown in Figure 2-2, we gain the ability to use the same circuits to carry both our LMR audio and any data communications needs we might have. We can also take advantage of higher compression codecs to minimize bandwidth needs.

Figure 2-2 Unicast Connection Trunk Leased Line Replacement



Connection PLAR

The connection private line, automatic ringdown (PLAR) service is a variant of the unicast connection trunk service. PLAR circuits are switched connections between statically configured endpoints. As a switched call, the PLAR connection will be torn down upon certain events such as the calling party going on-hook, or an absence of voice packets for a preconfigured amount of time. Whereas the unicast connection trunk VoIP call is made once at session initialization, with a PLAR connection, we can initiate the VoIP call based on signaling information from the LMR endpoint. The call will stay active while there is audio on the connection and for a configurable amount of time afterward, and then it will get torn down.

Although some bandwidth savings is achieved by only maintaining the connection while voice is present on the circuit, the main benefit of connection PLAR is its ability to connect with other H.323 capable devices. The unicast connection trunk connection uses special signaling packets to pass the signaling end-to-end between devices. Other devices capable of setting up or receiving H.323 calls will not recognize these packets and thus will not be able to establish a connection. Connection PLAR offers a way to connect to these other H.323 devices.

Multicast Connection Trunk (Hoot and Holler)

If multiple participants need access to the same radio channel or talk group, provisioning a full or partial mesh of point-to-point trunk connections will not scale. The multicast connection trunk service leverages the power of IP multicast to provide a one-to-many, and by extension, a many-to-many communication mechanism. Any device on the network capable of listening or sending VoIP packets on these multicast groups can participate in the talk group.

With this connection type, there is no H.323 call set up or special signaling packets. Each participant is either configured with or obtains the particular IP multicast address for the desired talk group. The participants then utilize the underlying multicast routing configuration of the network to broadcast and receive LMR audio to and from specific multicast groups.

Command and Control

LMR is a vital element in an organization's command and control process for maintaining contact between command agents and information resources. In order to extend this facility within a single LMR system to additional resources, an organization would need to incorporate additional radios, repeaters, or base stations into the system. Now that we have our LMR traffic transported over an IP network, we can extend our reach to the limits of our network and to any participant device capable of processing VoIP packets on the network. Thus, a commander with an IP phone or an agent in the field with access to the public switched telephone network (PSTN) or the Internet can now monitor and participate on designated LMR communications channels. The capability can be brought online in an ad-hoc fashion, and in some cases using existing resources.

For the purposes of this document, the additional devices are limited to Cisco IP Phone services using the Cisco CallManager or Cisco CallManager Express software, or PSTN-based phones accessing the IP network through a PSTN gateway. However, once the mechanism through which these new LMR endpoints interact with traditional radio systems is understood, it may become apparent to the reader how other VoIP devices might also participate.

Interconnection

Now that we have the radio systems and other LMR endpoints within an organization effectively communicating over the IP network, we can expand the model to allow different organizations to interconnect their LMR over IP domains. The ability to allow personnel from fire, local police, state police, emergency medical response, utility, and governmental organizations to interconnect between organizations as needed can be invaluable during emergency or disaster situations. The major concerns with joining LMR systems from separate entities are in maintaining system autonomy for each entity and ensuring security for the individual networks

One way to accomplish interconnecting LMR over IP domains is through a protocol firebreak in which each organization dedicates a voice port on an LMR enabled gateway for use as a connect point. Generally, this might be a channel on a digital T1 line, but it could also be an analog E&M port configured for back-to-back operation. These external channels can either be manually enabled, or left in an always-on state and bridged to existing channels.

Hardware Components

This section lists the basic Cisco hardware components necessary to implement the LMR over IP services in a network. Clearly a complete network solution encompasses more than just the edge devices. However, it is not the intent of this document to define a particular architecture for implementing LMR over IP. Instead, the products and their capacities are provided as aids to the designer, whether adding the LMR services to an existing network, or building a complete network from scratch.

Gateways

Table 2-1 shows the Cisco routers that support the LMR over IP feature.

Table 2-1 Supported Platforms

Platform	Maximum Analog Ports	Maximum Digital Channels (T1)
Cisco 2600XM series	4	96
Cisco 2800 series (except Cisco 2801)	10	240
Cisco 3725	8	192
Cisco 3745	16	384
Cisco 3825	16	384
Cisco 3845	24	576

Voice Modules

The LMR systems connect to the gateways using either analog E&M voice interface cards (VICs) or digital T1 voice or WAN interface cards (WICs). These physical interface cards are inserted into voice network modules (NMs) that contain the digital signal processors (DSPs) necessary to encode and decode the audio stream for transmission over the network. Valid interface card and network module configurations are shown in Table 2-2. Note that each E&M VIC supports two voice ports. A T1 WIC supports up to 24 voice ports per T1.

Table 2-2 Supported VICs and NMs

Network Module	Voice Interface Card	Interface Cards/ Module	Voice Channels Supported on NM
NM-1V	VIC-2E/M	1	2
NM-2V	VIC-2E/M	2	4
NM-HDV	VWIC-1MFT-T1 VWIC-2MFT-T1 VWIC-2MFT-T1-DI	1	• 12 medium complexity per PVDM[1]-12 • 6 high complexity per PVDM-12 • The NM-HDV will support up to 5 PVDM-12 DSP cards
NM-HD-1V	VIC2-2E/M	1	4 any complexity
NM-HD-2V	VIC2-2E/M	2	6 any complexity or 8 medium complexity
NM-HD-2VE	VIC2-2E/M VWIC-1MFT-T1 VWIC-2MFT-T1 VWIC-2MFT-T1-DI	2	18 any complexity, 24 medium complexity, or 48 G.711

1. Packet voice/data module (PVDM)

Software Versions

The following sections list the software versions of the components of the LMR over IP network.

Gateways

The LMR feature is supported on Cisco IOS Release 12.3(7)T and later versions in the images shown in Table 2-3.

Table 2-3 Supported Images and Memory Requirements

Platform	Feature Set	Minimum Flash/ DRAM (MB)	Recommended Flash/ DRAM (MB)
Cisco 2610XM, Cisco 2611XM	SP Services	32/128 MB	48/128MB
Cisco 2620XM, Cisco 2621XM	SP Services	32/128 MB	48/128MB
Cisco 2650XM, Cisco 2651XM	Advanced Enterprise Services SP Services	32/128 MB 32/128 MB	48/128MB 48/128 MB
Cisco 2811, Cisco 2821, Cisco 2851	Advanced Enterprise Services SP Services	64/128 MB 64/128 MB	64/128 MB 64/128 MB
Cisco 3725	Advanced Enterprise Services SP Services	64/128 MB 64/128 MB	64/128 MB 64/128 MB
Cisco 3745	Advanced Enterprise Services SP Services	64/194 MB 64/128 MB	128/256 MB 128/256 MB
Cisco 3825	Advanced Enterprise Services SP Services	64/194 MB	128/256 MB
Cisco 3845	Advanced Enterprise Services SP Services	64/194 MB	128/256 MB

Cisco CallManager

Cisco IP Phones using the following versions of Cisco CallManager and Cisco CallManager Express can be added to an LMR over IP network:

- Cisco CallManager Release 3.3(2) and Cisco CallManager Release 3.3(3)
- Cisco CallManager Express Release 3.1 with Cisco IOS Release 12.3(7)T

Interfacing with Radio Systems

The Land Mobile Radio (LMR) devices are attached to the IP network using wired connection points on radio units to link to digital or analog voice ports on the routers. At a minimum, these wired connection points must be able to transmit audio from the LMR device to the voice port and to receive audio from the voice port. They may also pass signaling information to and from the LMR device. The signaling may be in-band in the form of special tones mixed with the audio stream or signaling bits for the digital T1 connections, or it may be out-of-band through the use of dedicated signaling leads for analog connections. In the following sections this chapter explores the mechanics of physically wiring the LMR device to the voice port on the router, and then addresses mechanisms for handling signaling between the two devices:

Cabling

The LMR signaling enhancements in Cisco IOS software are germane to the analog ear and mouth (E&M) interface and a digital interface provisioned for E&M LMR signaling only. For a description of how the leads on the analog E&M interface are implemented on Cisco IOS voice gateways, refer to *Understanding and Troubleshooting Analog E&M Interface Types and Wiring Arrangements*. We recommend reviewing this document before reading further.

Digital T1 Interface

Before an LMR device can be connected to a T1 interface on the router, either the LMR device needs to have its own T1 interface, or a device such as a channel bank needs to be connected between the LMR device and the router. The multiflex trunk (MFT) Voice/WAN Interface Cards (VWICs) listed in Table 2-2 use standard T1 cabling configurations as shown in Figure 3-1 and Table 3-1.

Figure 3-1 T1 Pinouts

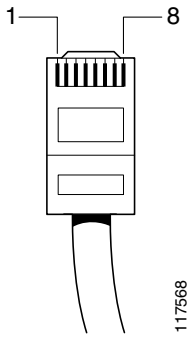


Table 3-1 Digital Voice Port Pinout (RJ-48C)

Pin	Signal
1	RX ring
2	RX tip
3	not used
4	TX ring
5	TX tip
6	not used
7	not used
8	not used

Note The RJ-48C receptacles on the MFT are pinned out as CPE, rather than as central office equipment. Use a T1/E1 crossover cable to connect to other CPE pinned out equipment, for example, PBXs.

The T1 interface on the router has multiple configuration options to match most common framing, line-code, line build-out, and other T1 configurations. From a Cisco IOS software perspective, each DS0 on the T1 is associated with a voice port through the use of the **ds0-group** statement. A signaling type is added to the statement to guide behavior based on the signaling bits for that particular channel. This is a typical LMR configuration:

```
controller T1 2/0
 framing esf
 linecode b8zs
 cablelength short 133
 ds0-group 0 timeslots 1 type e&m-lmr
```

Tip Although it is possible to assign all DS0s from the LMR device to voice ports using one **ds0-group** statement, it is not recommended because the mapping of DS0 to voice port is not deterministic. The only way to guarantee that a certain DS0 gets mapped to a certain voice port is to create a single **ds0-group** statement for each voice channel.

Analog E&M Interface

For analog connections, the E&M interface is the interface card type used to attach the leads from an LMR device. Of all the voice interfaces, only the E&M interfaces can accommodate the variety of different audio and signaling configurations present in the myriad of radio systems out in the field. The E&M port can be configured to transmit and receive audio information using one pair or two pairs of leads. It also has four different configurations for control of the signaling leads. Some radio systems may actually present an E&M interface for their wire-side connections, which obviously simplifies the connection process. However, many others systems will require planning for their connection.

E&M Interface Operation

This section describes the E&M interface leads and the signaling types used on E&M interfaces.

Leads

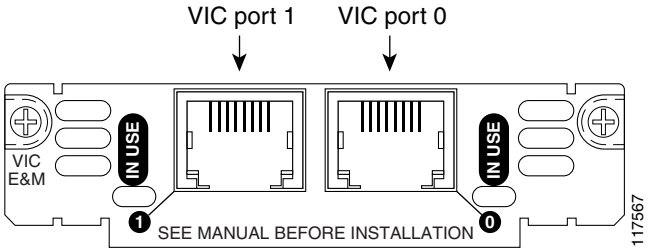
The E&M interface on the router has eight leads for use in connecting to the LMR systems. Four leads are available for the audio path. The other four are available for signaling. Table 3-2 describes the function of the various E&M leads and maps each lead to its corresponding pin on the E&M voice interface cards (VICs). Figure 3-2 shows the physical appearance of an E&M VIC, and Figure 3-1 shows the layout of the pins on a standard RJ-45 connector that would plug in to the receptacles on that VIC.

Table 3-2 E&M VIC Pinouts

Lead Name	Pin	Description
E (Ear or Earth)	Pin 7	Signal wire asserted by the router toward the connected device. Typically mapped to the push-to-talk (PTT) lead on the radio.
M (Mouth or Magnet)	Pin 2	Signal wire asserted by the connected device toward the router. Typically mapped to the Carrier Operated Relay (COR) lead on the radio.
SG (Signal Ground)	Pin 8	Used on E&M signaling Types II, III, and IV. Type IV is not supported on Cisco routers and gateways.
SB (Signal Battery)	Pin 1	Used on E&M signaling Types II, III, and IV. Type IV is not supported on Cisco routers and gateways.
Two-Wire Mode		
T1/R1 (Tip-1/Ring-1)	Pins 5 and 4	In two-wire operation, the T1/R1 leads carry the full-duplex audio path.
Four-Wire Mode		
T/R (Tip/Ring)	Pins 6 and 3	In a four-wire operation configuration, this pair of leads carries the audio in from the radio to the router and would typically be connected to the line out or speaker of the radio.
T1/R1 (Tip-1/Ring-1)	Pins 5 and 4	In a four-wire operation configuration, this pair of leads carries the audio out from the router to the radio and would normally be connected to the line in or microphone on the radio

See Table 3-3 for more information on E&M leads and VICs configured for E&M signaling Types I, II, III, and V.

Figure 3-2 E&M VIC Interface



Signaling Types

Five types of signaling configurations are defined for traditional E&M interfaces. The E&M port on a Cisco router supports four of those types: I, II, III, and V. These signaling types define different mechanisms for asserting signaling on the E-lead or recognizing signals asserted on the M-lead. In general, the Type II configuration is preferred for use with LMR because the absence of DC connectivity between the radio and the router ensures that no ground loops are created. Type V offers the option of connecting E&M ports back-to-back using a simple rollover cable, in 2-wire mode only. However, the devices carrying both E&M ports must be collocated and connected to the same ground or power system.

Figure 3, Figure 4, and Figure 5 illustrate the interface models for each of the E&M types which might be used to connect to an LMR system. Note that Type I is not displayed because that configuration is not conducive to interfacing with LMR system because it requires interconnection of the radio and router ground and power systems.

Note These are generic models. Additional electrical elements may be necessary to adjust the model to fit your specific application.

Figure 3-3 E&M Type II Interface Model

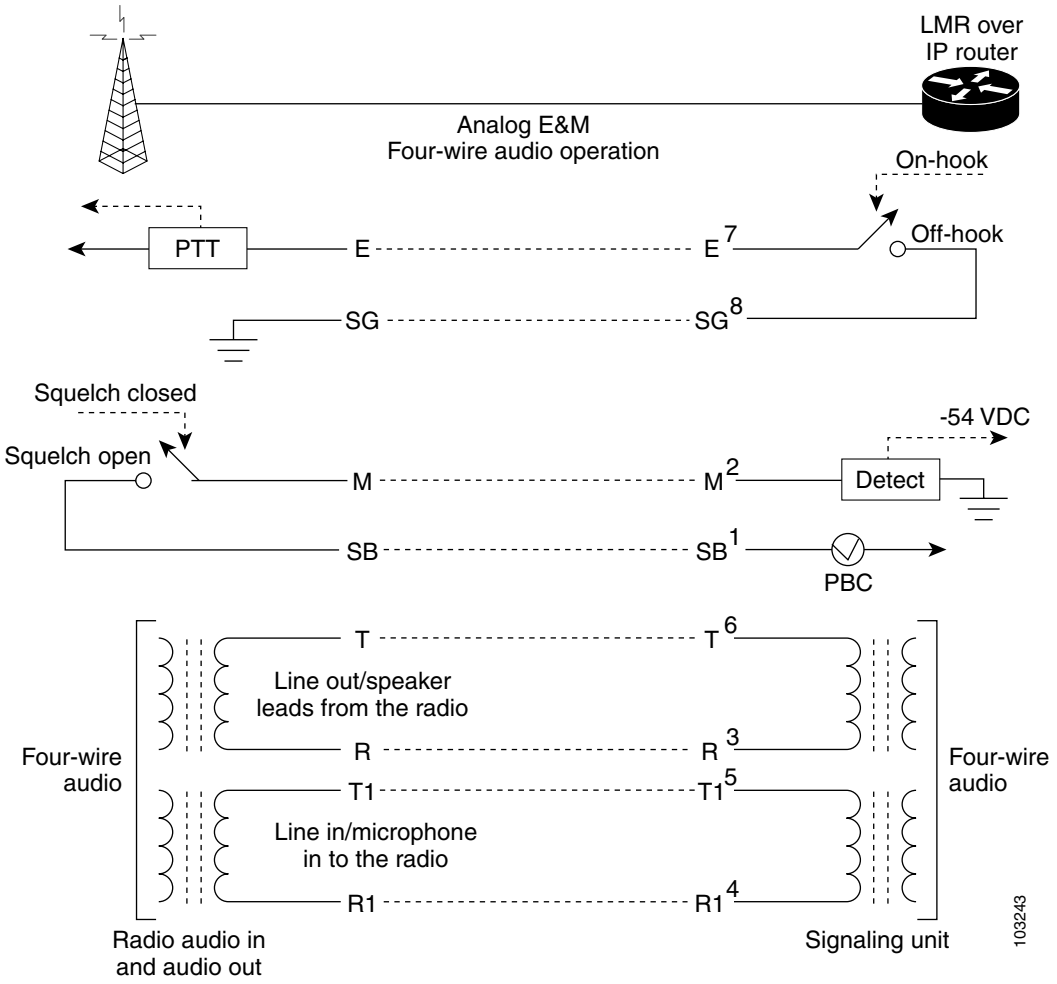


Figure 3-4 E&M Type III Interface Model

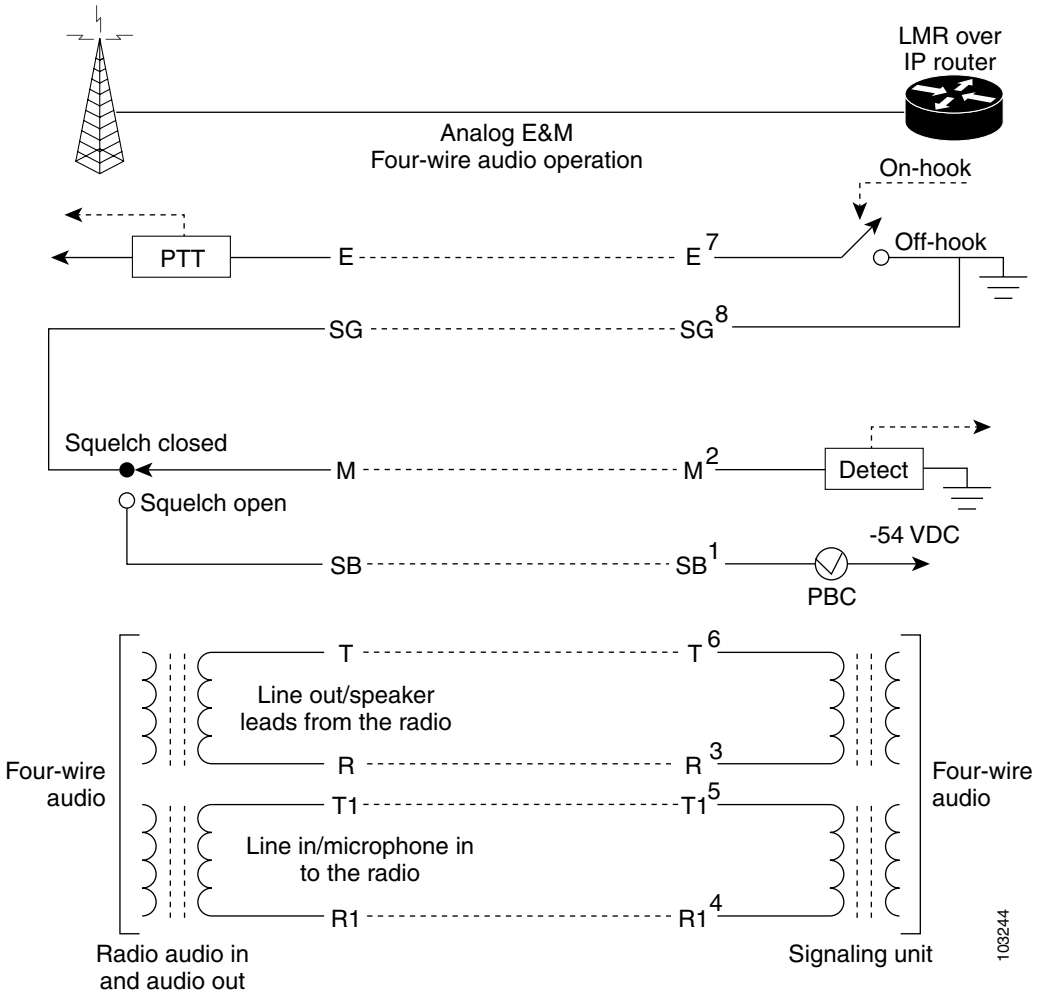
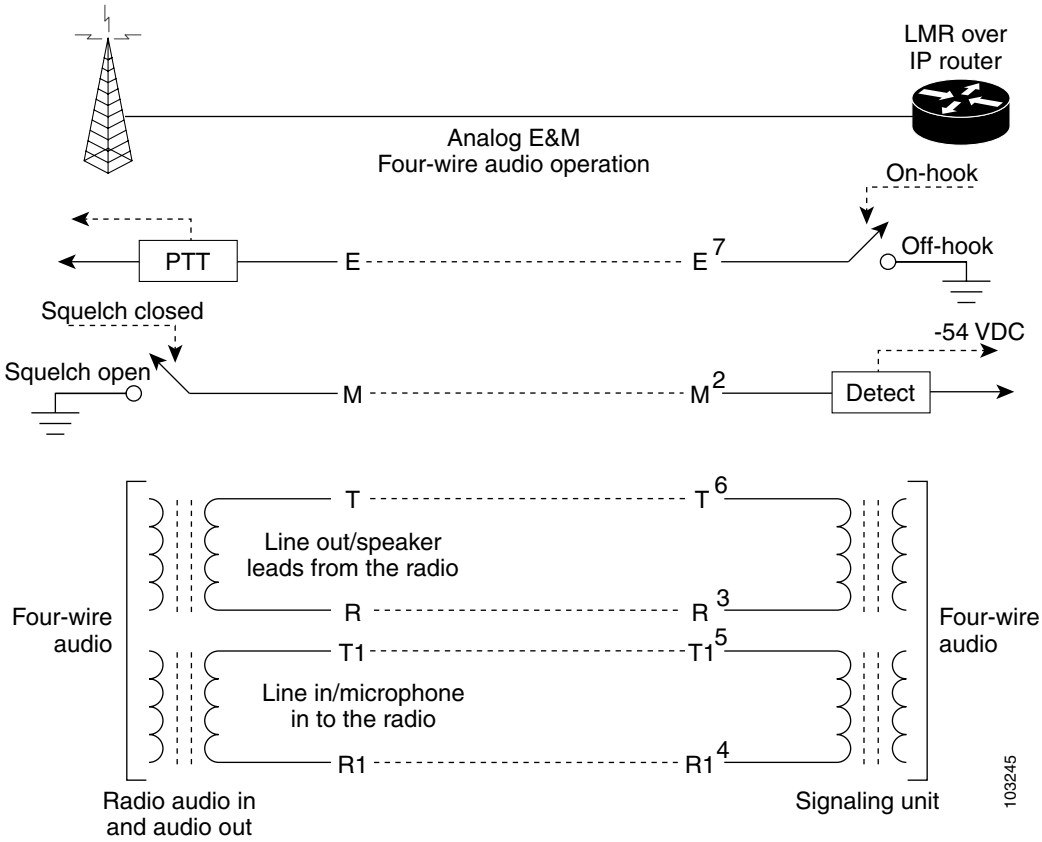


Figure 3-5 E&M Type V Interface Model



E&M Electrical Characteristics

The T1 E&M interface is compliant with the ANSI T1.403 and AT&T Publication 62411 standards for T1. The Analog E&M interface is described in the following section.

General

Table 3-3 provides information about E, M, SG, and SB leads when the E&M VIC is configured for E&M signaling Types I, II, IV, and V.

Table 3-3 Signaling Lead Electrical Characteristics

Lead	Type I	Type II	Type III	Type V
E	Over current protected solid state relay contact to chassis ground	Over current protected solid state relay contact to SG	Over current protected solid state relay contact to chassis ground	Over current protected solid state relay contact to chassis ground
SG	Chassis ground via solid state relay	Over current protected solid state relay contact to E	Chassis ground via solid state relay	Chassis ground via solid state relay
M	Current limited opto coupler input to chassis ground	Current limited opto coupler input to chassis ground	Current limited opto coupler input to chassis ground	Current limited opto coupler input to –54 VDC
SB	Over current protected –54 VDC	Over current protected –54 VDC	Over current protected –54 VDC	Chassis ground

Unless interfacing requirements dictate otherwise, we recommend that you use Type II signaling when directly connecting to a radio to eliminate ground loops. Other signaling types in conjunction with external circuitry can also provide isolation of radio and LMR gateway chassis grounds. We recommend that any components used for external interface circuitry have appropriate agency approvals from Underwriters Laboratories Inc. (UL), Canadian Standards Association (CSA), Verband der Elektrotechnik, Elektronik und Informationstechnik or Association for Electrical, Electronic, and Information Technologies (VDE), British Standards Institution (BSI), or others.

Audio Interface

The E&M VIC presents four audio leads, T and R and T1 and R1, configurable for operation in either two- or four-wire mode. The leads are transformer-isolated with an impedance of 600 ohms across each pair, providing a 600 ohm transformer coupled audio appearance to radios. When the VIC-2E/M is used, these leads are DC blocked. When the VIC2-2E/M is used, these leads are DC over current protected. In two-wire operation, the T1 and R1 leads are used to carry the full-duplex audio. In four-wire operation, the T and R leads are the audio input to the router and the T1 and R1 leads are the audio output from the router.

PTT Interface (E-Lead)

The E&M VIC presents a solid state relay contact in series with a resettable circuit protection device between the E and SG leads when configured for Type II signaling. The built-in current limiting has a maximum of 270 milliamps (mA) or a typical value of 210 mA. In addition, there is a Positive Temperature Coefficient (PTC) device in series with the relay contact that will further limit and protect the circuit. Industry specification says that E-lead current should be limited to a maximum of approximately 250 mA, but with typical operating currents of about 50 mA or less. At currents between 5 mA and 30 mA, this interface exhibits an approximate resistance of 25 ohms. This information, in conjunction with detailed knowledge of radio PTT circuitry, should allow a technician to determine whether a direct connection between radio and VIC can be utilized or if external interface circuitry needs to be added.

E-Lead Operation During Router Reload

When the LMR gateway is reloaded, the VIC-2E/M and VIC2-2E/M interface cards will go off-hook, which will be interpreted as a PTT for those radio systems employing physical signaling. During this interval, the –52 volts from the SB lead is also removed. External circuitry that detects the absence of SB can be used to disable the PTT operation. Patriot Base Stations from Ritron and the Tactical Communications Bridge TCB-1 from Link Communications incorporate this circuitry.

COR Interface (M-Lead)

The E&M VIC presents the input side, that is, LED of an opto isolator in series with a current-limiting resistor and a transistor used to switch between the different E&M configuration types to the COR, also referred to as "squelch open," output from a radio. Opto isolator input is also shunted with a resistor to control its sensitivity. When configured for Type II signaling, the radio COR needs to be able to source about 3 mA into a nominal 7400 ohm resistance with respect to the LMR gateway chassis ground to indicate a squelch open condition to the LMR gateway. This current can be sourced from the radio itself or from the SB lead of the LMR gateway. If the SB lead is used as a current source, the radio must be able to switch about 7 mA of current at an open circuit voltage of 54 V. Because most modern radios typically have an open collector or open drain output, additional external circuitry such as a solid state relay likely will be required between the radio and the E&M VIC.

E&M DC Characterization

This section describes the direct current (DC) characteristics of the E&M interface. Some typical voltages and currents were selected to characterize the E&M VIC DC operational parameters. The information is summarized in the following tables so that a radio technician can use this data in conjunction with knowledge of radio circuitry to perform the necessary integration.

The following testing methodology was used to populate the tables in this section:

- All testing was done in E&M Type II mode.
- Agilent model E3612A power supply was used for all tests in both constant voltage and constant current modes.
- All measurements were made at the end of one foot of 26 American Wire Gauge (AWG) stranded wire connected via an RJ-46 plug to the faceplate of a VIC.
- All E-lead on resistance measurements were made between the E-lead and the SG-lead and included resistance of internal protection device and solid state relay.
- All M-lead measurements were made between M-lead and the chassis ground and included internal M-lead type switching components and the control side of solid state relay.
- Voltages and currents were measured with Fluke Model 73 III VOM verified to have the current calibration sticker.
- All measurements were done at room temperature.
- Voltages of 5, 12, and 24 VDC were picked for testing because these were considered typical of what may be sourced by a radio.

Table 3-4 describes the E-lead (PTT) relay contact resistance for the VIC-2E/M for typical operating conditions.

Table 3-4 E-Lead (PTT) Relay Contact Resistance for VIC-2E/M

Voltage (VDC)	Current (mA)	Vdrop (VDC)	R(ON) ohms	Voltage (VDC)	Current (mA)	Vdrop (VDC)	R(ON) ohms	Voltage (VDC)	Current (mA)	Vdrop (VDC)	R(ON) ohms
5	1	0.033	33.0	12	1	0.030	30.0	24	1	0.030	30.0
5	2	0.054	27.0	12	2	0.055	27.5	24	2	0.060	30.0
5	3	0.081	27.0	12	3	0.076	25.3	24	3	0.081	27.0
5	4	0.097	24.3	12	4	0.104	26.0	24	4	0.102	25.5
5	5	0.130	26.0	12	5	0.128	25.6	24	5	0.127	25.4
5	10	0.264	26.4	12	10	0.245	24.5	24	10	0.261	26.1
5	20	0.504	25.2	12	20	0.503	25.2	24	20	0.495	24.8
5	30	0.740	24.7	12	30	0.747	24.9	24	30	0.747	24.9

Table 3-5 describes the E-lead (PTT) relay contact resistance for the VIC2-2E/M for typical operating conditions.

Table 3-5 E-Lead (PTT) Relay Contact Resistance for VIC2-2E/M

Voltage (VDC)	Current (mA)	Vdrop (VDC)	R(ON) ohms	Voltage (VDC)	Current (mA)	Vdrop (VDC)	R(ON) ohms	Voltage (VDC)	Current (mA)	Vdrop (VDC)	R(ON) ohms
5	1	0.032	32.0	12	1	0.037	37.0	24	1	0.046	46.0
5	2	0.067	33.5	12	2	0.072	36.0	24	2	0.062	31.0
5	3	0.090	30.0	12	3	0.094	31.3	24	3	0.094	31.3
5	4	0.120	30.0	12	4	0.126	31.5	24	4	0.132	33.0
5	5	0.159	31.8	12	5	0.155	31.0	24	5	0.155	31.0
5	10	0.321	32.1	12	10	0.305	30.5	24	10	0.315	31.5
5	20	0.619	31.0	12	20	0.629	31.5	24	20	0.612	30.6
5	30	0.923	30.8	12	30	0.921	30.7	24	30	0.941	31.4

Table 3-6 describes the M-lead detector (COR) detection thresholds for the VIC-2E/M.

Table 3-6 M-Lead Detector (COR) Detection Thresholds for VIC-2E/M

			Vdrop (VDC)	Equivalent Resistance (ohms)
M-Lead Positive	M-Lead Off-Hook Detect (mA)	2.10	15.5	7381
	M-Lead On-hook Detect (mA)	2.04	15.1	7402
M-Lead Negative	M-Lead Off-Hook Detect (mA)	2.08	15.6	7500
	M-Lead On-Hook Detect (mA)	2.06	15.2	7379
			Average	7415

The SB-lead open circuit voltage (VDC) is –53.4.

Table 3-7 describes the M-lead detector (COR) detection thresholds for the VIC2-2E/M.

Table 3-7 M-Lead Detector (COR) Detection Thresholds for VIC2-2E/M

			Vdrop (VDC)	Equivalent Resistance (ohms)
M-Lead Positive	M-Lead Off-Hook Detect (mA)	2.12	15.7	7406
	M-Lead On-Hook Detect (mA)	2.10	15.6	7429
M-Lead Negative	M-Lead Off-Hook Detect (mA)	2.30	16.9	7348
	M-Lead On-Hook Detect (mA)	2.28	16.8	7368
			Average	7388

The SB-lead open circuit voltage (VDC) is –53.1.

Audio Characteristics

This section describes the behavior of the voice ports on the router with respect to audio information passed through the interface. The tests used to obtain the data were performed according to standard voice testing methods for a telephony interface. The results describe how effectively the voice interface on the router can faithfully reproduce audio at different levels and frequencies.

Gain Tracking Characterization

Figure 3-6 and Figure 3-7 show the gain tracking error per Telcordia specification TR-NWT-000507. A 1004-Hz tone was presented to a digital T1 port configured for LMR on one router. The level of the tone was incrementally stepped through various levels starting at –60.0 dBm and proceeding to +3.0 dBm. A VoIP connection was made between the digital interface and an analog E&M interface configured for LMR on another router. The tone was measured at the receiving end and the level was recorded. The Telcordia specification places upper and lower limits for the difference between the level of the received tone and the level sent.

This testing was performed from a T1 interface on an NM-HDV module to an E&M port on an NM-2V module, and from a T1 interface on an NM-HD-2VE module to an E&M port on an NM-HD-2V module. The T1 interfaces were configured for extended superframe (ESF) framing and binary 8-zero substitution (B8ZS) line code and were configured to receive clocking from the attached tone generation device (Sage 930). The E&M interfaces were configured for E& M Type II, 4-wire operation at 600 ohm. Both the E&M and T1 voice ports had input gain and output attenuation set to 0 with echo cancellers disabled. The VoIP dial peers were configured to use the G.711 mu-law codec with voice activity detection (VAD) disabled.

Figure 3-6 Gain Tracking Error for NM-HDV to NM-2V

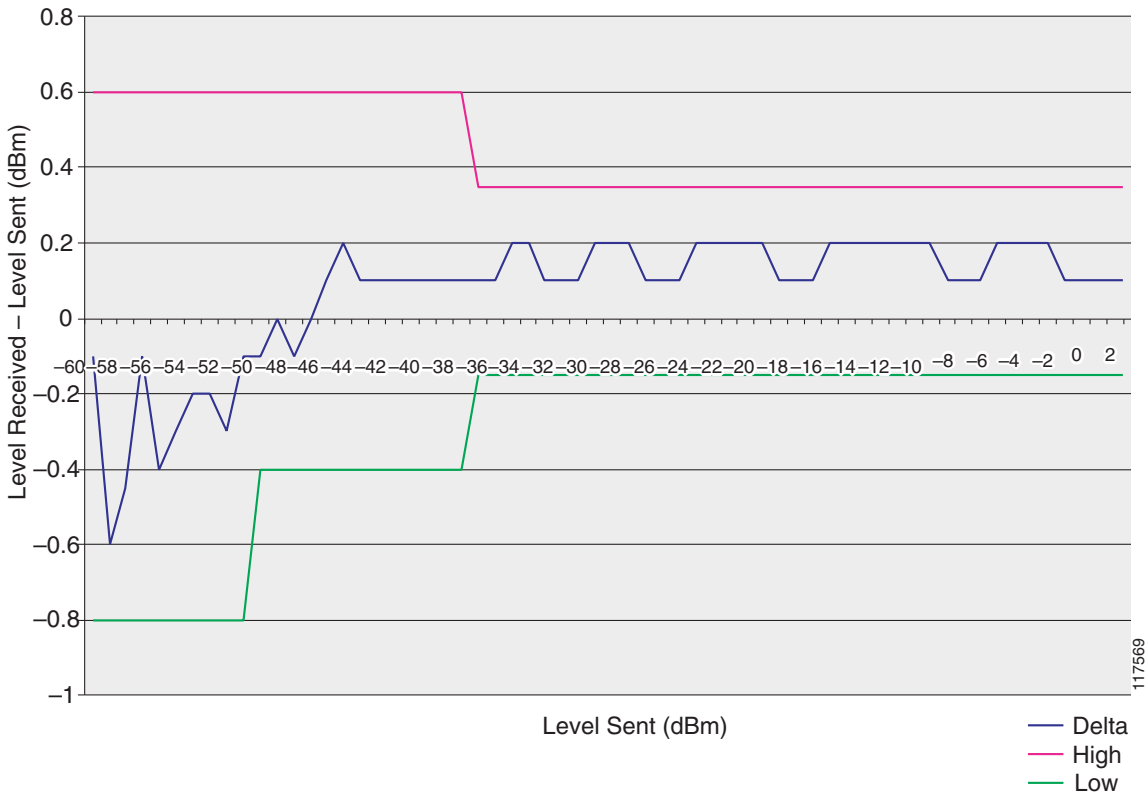
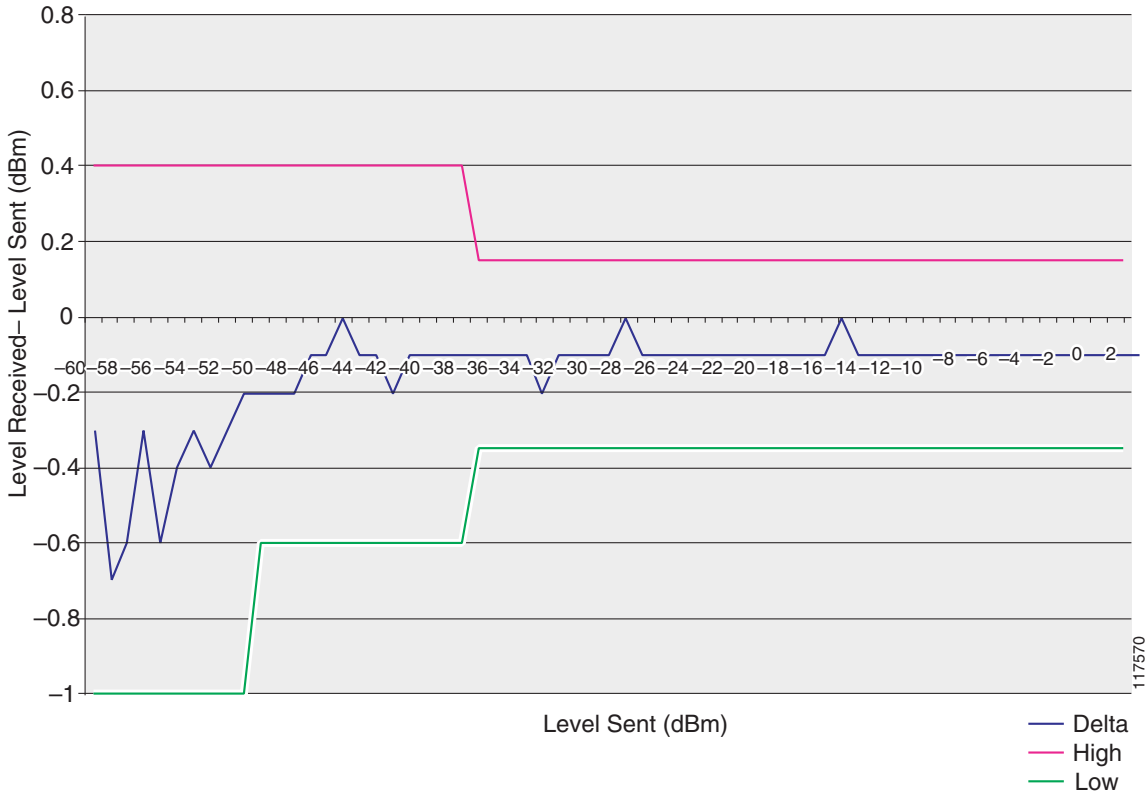


Figure 3-7 Gain Tracking Error for NM-HD-2VE to NM-HD-2V



Frequency Response Characterization

Table 3-8 shows the frequency response rolloff error per Telcordia specification TR-NWT-000507. A VoIP connection was made between a digital interface configured for LMR on one router and an analog E&M interface configured for LMR on another router. Initially, a 1004-Hz tone was presented to one of the ports at 0.0 dBm and the level received at the other end was recorded as a baseline measurement. Then, the frequency of the tone was stepped through various values starting at 60 Hz and ending at 3400 Hz, holding the level constant. The Telcordia specification places upper and lower limits for the level received based on the frequency sent using the 1004 Hz level as the baseline.

This testing was performed from a T1 interface on an NM-HDV module to an E&M port on an NM-2V module, and from a T1 interface on an NM-HD-2VE module to an E&M port on an NM-HD-2V module. The T1 interfaces were configured for ESF framing and B8ZS line code and were configured to receive clocking from the attached tone generation device (Sage 930). The E&M interfaces were configured for E& M Type II, four-wire operation at 600 ohms. Both the E&M and T1 voice ports had input gain and output attenuation set to 0 with echo cancellers disabled. The VoIP dial peers were configured to use the G.711 mu-law codec with VAD disabled.

Table 3-8 Frequency Response Characteristics for Voice Ports

Frequency (Hz)	Received Level (dBm)				
	Analog to Digital	Digital to Analog	Analog to Digital	Digital to Analog	Digital to Digital
	NM-2V to NM-HDV	NM-HDV to NM-2V	NM-HD-2V to NM-HD-2VE	NM-HD-2VE to NM-HD-2V	NM-HD-2VE to NM-HD-2VE
60	No Value	–2.6	No Value	–2.1	0.0
200	–0.5	–0.1	–0.6	–0.2	0.0
300	0.1	0.1	0.2	–0.1	0.0
400	0.0 to 0.2	0.1	0.1 to 0.4	–0.1	0.0
500	0.1	0.1	0.1 to 0.3	0.0	–0.1
600	0.1	0.2	0.2	–0.1	0.0
700	0.1	0.2	0.2	–0.1	0.0
800	–0.2 to +0.4	0.1	–0.1 to +0.4	–0.1	0.1
900	0.1	0.2	0.2	–0.1	0.0
1004	0.1	0.1	0.2	–0.1	0.0
1100	0.1	0.2	0.2	–0.1	0.0
1200	0.0 to 0.2	0.1	0.1 to 0.3	–0.1	0.0
1300	0.1	0.1	0.2	–0.1	–0.1
1400	0.1	0.2	0.2	–0.1	0.0
1500	0.1	0.1	0.1 to 0.3	–0.2	–0.1
1600	–0.2 to +0.3	–0.1 to +0.3	–0.1 to +0.4	–0.4 to +0.0	0.1
1700	0.1	0.1	0.2	0.0	0.0
1800	0.1	0.1	0.2	0.0	–0.1
1900	0.1	0.1	0.2	0.0	–0.1
2000	–2.0 to +1.1	–0.3 to +0.3	–1.9 to +1.3	–0.7 to –0.1	0.3
2100	0.1	0.1	0.2	0.0	–0.1
2200	0.1	0.1	0.2	0.0	0.0
2300	0.0	0.1	0.2	0.0	0.0
2400	–0.2 to +0.2	0.1	–0.1 to +0.4	0.0	0.1
2500	0.0	0.1	0.1 to 0.3	–0.1	0.0
2600	0.0	0.1	0.2	0.0	–0.1
2700	0.0	0.1	0.2	–0.1	0.0
2800	0.0	0.1	0.1 to 0.3	0.0	0.0
2900	0.0	0.1	0.2	0.0	0.0
3000	–0.4 to +0.2	0.0	–0.2 to +0.5	–0.2	–0.2
3400	–0.3	–0.3	–0.1	–0.4	–0.1

Signaling

LMR endpoints generally need some method to indicate to other endpoints on the wired network that they have received audio from their air interface that they will be sending onto the network. Similarly, the LMR device needs some method to understand these signals from the other devices on the wired network, so it can relay the received audio on its air interface. There are two basic methods to accomplish this task. First, the LMR endpoint can use physical signaling external to the audio stream to communicate its status. Second, the LMR endpoint can mix the signaling in with the audio stream using special tones or some other encoding system.

In addition to the LMR endpoint communicating its status, the gateway to which the LMR device is connected must receive the status, and then be able to effectively transport that status. With point-to-point connections, the signaling transport mechanisms are fairly straightforward. With multicast many-to-many connections, the mechanisms require some adjustments, which are described in the following sections:

Physical Signaling

On an analog E&M interface, physical signaling occurs though electrical changes on the various leads, primarily the E- and M-leads. For digital interfaces, T1 signaling bits are employed. The LMR gateways convert this received physical signaling to an internal representation, which looks strikingly similar to the T1 ABCD signaling bits. For unicast transport mechanisms, the signaling can be passed through the IP network using VoIP signaling packets. When the gateway on the other side of the connection receives these signaling packets, it translates the internal signaling representation back into physical signaling on its interface. In a multicast environment, it would be confusing to the gateway to receive conflicting signaling packets, so none are sent.

Let us consider a general example of this signaling method in operation across a unicast connection. An LMR endpoint recognizes audio on its air interface. It signals this state by applying voltage to its COR lead. The attached gateway interprets this state as a seize on its M-lead. The gateway sends this signal state across the network. The receiving gateway takes the signaling state and grounds its E-lead, indicating seizure. The LMR endpoint attached to the receiving gateway interprets this state as someone pressing the PTT button and transmits received audio on its air interface.

When implementing your LMR over IP network, consider these issues:

- Are the correct leads connected from the LMR endpoint to the E&M interface on the gateway?
- Does the signal state received from the other side of the connection map correctly to the signals the LMR system on this side expects to see?

Tone Signaling (In-Band)

If the LMR endpoint uses tone signaling mixed in the audio stream to communicate its activity states, from the gateway's standpoint, reception of the signaling consists of recognizing the existence of incoming audio information. The gateway accomplishes this function by passing audio samples of a sufficient dB level through its VAD algorithm. Note that reception of the signaling does not imply an

understanding of the signaling. At this point, the gateway does not have the ability to examine the incoming voice stream to determine and characterize any tone signaling that may be present. Thus transport involves merely passing these voice samples untouched along the connection.

When implementing your LMR over IP network, consider whether the signaling will survive transcoding by means of lower bit-rate codecs such that it is recognizable when decoded at the receiver.

LMR Signaling

The previous examples of physical and tone signaling assumed homogenous systems. One LMR endpoint signals another LMR endpoint using substantially similar physical or tone signaling. Although this assumption may reflect the conditions in some installations, it clearly does not provide the interoperability needed in many other installations. The goal is to attach LMR endpoints to the IP network in such a fashion that regardless of whether the endpoint uses physical, tone, or no signaling at all, it can communicate with other LMR endpoints and traditional voice endpoints as well.

Table 3-9 describes the voice port configuration commands introduced to handle signaling differences in the various LMR systems that may be attached to the network. The M-lead options describe the ways in which the gateway can interpret signaling coming from the LMR systems. The E-lead options describe the ways in which the gateways can send signaling to the LMR systems. Although we find real E- and M-leads on analog interfaces only, these commands apply equally to the digital interfaces.

Table 3-9 LMR Signaling Configuration Options

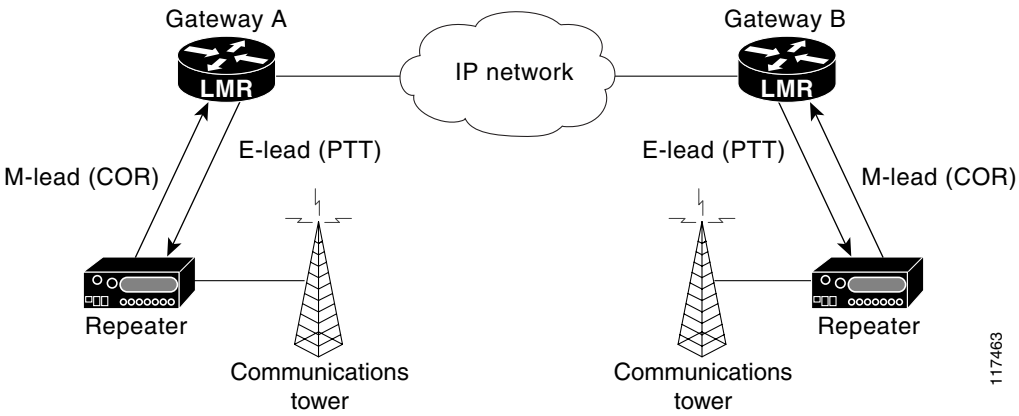
Voice Port Configuration Command	Behavior
lmr m-lead audio-gate-in	The gateway monitors the status of the M-lead. When it registers a seize condition for the M-lead, the incoming voice stream is passed to the digital signal processors (DSPs) for further processing. When the M-lead is idle, any audio arriving on the interface is ignored. If VAD is enabled for the connection, the received audio must still pass the VAD threshold in order for voice packets to appear on the network. Otherwise, voice packets will be constantly generated even if they contain just silence.
lmr m-lead dialin	The command operates exactly the same as the **audio-gate-in** option with the addition of a dial trigger. If the voice port is currently not engaged in a VoIP connection, a seize condition on the M-lead will trigger the voice port to dial a configured connection E.164 address. An idle condition on the M-lead does not by itself cause the connection to get torn down, but it does start the timer that is set with the **timeouts teardown lmr** command. The **lmr m-lead** command with the **dialin** option is designed for private line, automatic ringdown (PLAR) connections.

Table 3-9 LMR Signaling Configuration Options

Voice Port Configuration Command	Behavior
lmr m-lead inactive	The condition of the M-lead is ignored. The incoming audio stream is passed to the DSPs for processing. If VAD is enabled for the connection, the received audio must pass the VAD threshold in order for voice packets to appear on the network. Otherwise, voice packets will be constantly generated even if they contain just silence. Without VAD enabled, there is a great chance for problems with this option.
lmr e-lead seize	The gateway will place the E-lead in a seize or idle state depending on signaling state received on the connection. This command will be employed primarily in those situations where signaling packets can be expected from the other end of the connection, which for the most part means unicast connection trunk connections.
lmr e-lead voice	The gateway will place the E-lead in a seize or idle state depending on presence or absence of voice packets. Note that for this side of the connection, VAD is not triggering the E-lead. The E-lead is triggered by the presence of voice packets from the network. Of course, VAD may be responsible for the presence of the voice packets on the connection, but that is the business of the other side, over which this side has no control. This command is employed in those situations where signaling will not be forthcoming from the network, which generally means multicast connection trunk and connection PLAR connections.
lmr e-lead inactive	It might be supposed that with this command, the gateway would leave the E-lead in its default state. This is true, unless the gateway received signaling packets from the network, in which case it applies a state based on the contents of those packets. This behavior is seen in unicast connection trunk connections, and, this behavior is unavoidable. Therefore, the suggestion for these connections is to alter the way in which the voice port processes the seize and idle packets from the network, so that they both produce the same results. The process for accomplishing this task is described in the "Seize and Idle Bit Patterns" section.

Table 3-10, Table 3-11, and Table 3-12 present the behavior of the voice port E- and M-lead configuration options broken down by connection type, M-lead state, and the presence or absence of audio. The tables refer to Figure 3-8. The M-lead configuration option is what would be configured on the voice port of Gateway A, and the E-lead option is what would be configured on the voice port of Gateway B. The column headings present each of the four possible M-lead and audio permutations that can be expected from the LMR endpoint on Gateway A. The table entries are what the LMR endpoint on Gateway B can expect to see.

Figure 3-8 LMR Signaling from Gateway to Radio



For purposes of these tables, it is assumed that the default values for the voice port seize and idle bit patterns are used. In addition, it is assumed that VAD is enabled for the connection, unless otherwise stated.

Table 3-10 Unicast Connection Trunk

Voice Port Configuration Command		M-Lead Idle		M-Lead Seize	
Gateway A	**Gateway B**	**No Audio Supplied**	**Audio Supplied**	**No Audio Supplied**	**Audio Supplied**
lmr m-lead audio-gate-in	lmr e-lead seize	E-lead idle	E-lead idle	E-lead seize	E-lead seize
		No audio generated	No audio generated	No audio generated	Audio generated
	lmr e-lead inactive	E-lead idle	E-lead idle	E-lead seize	E-lead seize
		No audio generated	No audio generated	No audio generated	Audio generated
	lmr e-lead voice	E-lead idle	E-lead idle	E-lead idle	E-lead seize
		No audio generated	No audio generated	No audio generated	Audio generated
lmr m-lead dialin	lmr e-lead seize	E-lead idle	E-lead idle	E-lead seize	E-lead seize
		No audio generated	No audio generated	No audio generated	Audio generated
	lmr e-lead inactive	E-lead idle	E-lead idle	E-lead seize	E-lead seize
		No audio generated	No audio generated	No audio generated	Audio generated
	lmr e-lead voice	E-lead idle	E-lead idle	E-lead idle	E-lead seize
		No audio generated	No audio generated	No audio generated	Audio generated
lmr m-lead inactive	lmr e-lead seize	E-lead idle	E-lead idle	E-lead seize	E-lead seize
		No audio generated	Audio generated	No audio generated	Audio generated
	lmr e-lead inactive	E-lead idle	E-lead idle	E-lead seize	E-lead seize
		No audio generated	Audio generated	No audio generated	Audio generated
	lmr e-lead voice	E-lead idle	E-lead seize	E-lead idle	E-lead seize
		No audio generated	Audio generated	No audio generated	Audio generated

Table 3-11 Connection PLAR

Voice Port Configuration Command		M-Lead Idle		M-Lead Seize	
Gateway A	**Gateway B**	**No Audio Supplied**	**Audio Supplied**	**No Audio Supplied**	**Audio Supplied**
lmr m-lead audio-gate-in	lmr e-lead seize	No connection established	No connection established	No connection established	No connection established
		E-lead idle	E-lead idle	E-lead idle	E-lead idle
		No audio generated	No audio generated	No audio generated	Audio generated
	lmr e-lead inactive	No connection established	No connection established	No connection established	No connection established
		E-lead idle	E-lead idle	E-lead idle	E-lead idle
		No audio generated	No audio generated	No audio generated	Audio generated
	lmr e-lead voice	No connection established	No connection established	No connection established	No connection established
		E-lead idle	E-lead idle	E-lead idle	E-lead idle
		No audio generated	No audio generated	No audio generated	Audio generated
lmr m-lead dialin	lmr e-lead seize	No connection established	No connection established	Connection established	Connection established
		E-lead idle	E-lead idle	E-lead seized until connection torn down	E-lead seized until connection torn down
		No audio generated	No audio generated	No audio generated	Audio generated
	lmr e-lead inactive	No connection established	No connection established	Connection established	Connection established
		E-lead idle	E-lead idle	E-lead idle	E-lead idle
		No audio generated	No audio generated	No audio generated	Audio generated
	lmr e-lead voice	No connection established	No connection established	Connection established	Connection established
		E-lead idle	E-lead idle	E-lead idle	E-lead seize
		No audio generated	No audio generated	No audio generated	Audio generated
lmr m-lead inactive	lmr e-lead seize	No connection established	No connection established	No connection established	No connection established
		E-lead idle	E-lead idle	E-lead idle	E-lead idle
		No audio generated	No audio generated	No audio generated	Audio generated
	lmr e-lead inactive	No connection established	No connection established	No connection established	No connection established
		E-lead idle	E-lead idle	E-lead idle	E-lead idle
		No audio generated	No audio generated	No audio generated	Audio generated
	lmr e-lead voice	No connection established	No connection established	No connection established	No connection established
		E-lead idle	E-lead idle	E-lead idle	E-lead idle
		No audio generated	No audio generated	No audio generated	Audio generated

Table 3-12 Multicast Connection Trunk

Voice Port Configuration Command		M-Lead Idle		M-Lead Seize	
Gateway A	**Gateway B**	**No Audio Supplied**	**Audio Supplied**	**No Audio Supplied**	**Audio Supplied**
lmr m-lead audio-gate-in	lmr e-lead seize	E-lead idle	E-lead idle	E-lead idle	E-lead idle
		No audio generated	No audio generated	No audio generated	Audio generated
	lmr e-lead inactive	E-lead idle	E-lead idle	E-lead idle	E-lead idle
		No audio generated	No audio generated	No audio generated	Audio generated
	lmr e-lead voice	E-lead idle	E-lead idle	E-lead idle	E-lead seize
		No audio generated	No audio generated	No audio generated	Audio generated
lmr m-lead dialin	lmr e-lead seize	E-lead idle	E-lead idle	E-lead idle	E-lead idle
		No audio generated	No audio generated	No audio generated	Audio generated
	lmr e-lead inactive	E-lead idle	E-lead idle	E-lead idle	E-lead idle
		No audio generated	No audio generated	No audio generated	Audio generated
	lmr e-lead voice	E-lead idle	E-lead idle	E-lead idle	E-lead seize
		No audio generated	No audio generated	No audio generated	Audio generated
lmr m-lead inactive	lmr e-lead seize	E-lead idle	E-lead idle	E-lead idle	E-lead idle
		No audio generated	Audio generated	No audio generated	Audio generated
	lmr e-lead inactive	E-lead idle	E-lead idle	E-lead idle	E-lead idle
		No audio generated	Audio generated	No audio generated	Audio generated
	lmr e-lead voice	E-lead idle	E-lead seize	E-lead idle	E-lead seize
		No audio generated	Audio generated	No audio generated	Audio generated

Seize and Idle Bit Patterns

Generally, the LMR signaling behavior described in the previous section works well. However, in the vast domain of potential end systems, there may be those systems that need the E-lead open to indicate PTT or will ground the M-lead to indicate seizure on the COR lead, a sort of reverse polarity. Fortunately, Cisco IOS software has a mechanism to alter how the received signaling is represented internally and how the internal representation is mapped to the transmitted signaling. For example, if a gateway receives a seize signaling packet, it can map this packet to what the physical interface would interpret as an idle pattern. The interface would thus open the E-lead circuit, which would indicate to the device in this example that someone was pushing the PTT button.

Table 3-13 lists the bit conditioning commands that can be applied to a voice port interface and the general operation of the commands.

Table 3-13 Bit Pattern Options

Voice Port Configuration Command	Default Pattern	Behavior
define rx-bits seize ABCD (where ABCD = 0000 through 1111)	1111	Defines the bit pattern to send to the DSP upon receipt of a seize signal on the interface.
define rx-bits idle ABCD	0000	Bit pattern to send to the DSP upon the receipt of an idle signal on the interface.
define tx-bits seize ABCD	1111	Defines the bit pattern to send out the interface when a seize message is received from the network.
define tx-bits idle ABCD	0000	Defines the bit pattern to send out the interface when an idle message is received from the network.

Let us examine how the various bit pattern options operate in a little more detail. The behavior column references the voice port DSPs. The reason for this is twofold. First, conceptually there are three discrete interfaces in the process of converting physical signaling from the LMR endpoints to Real-Time Transport Protocol (RTP) signaling packets. We have the LMR endpoint to the gateway E&M interface, the E&M to the DSP interface and the DSP to the RTP signaling packets interface. Second, the signaling debug commands reference signaling going to and from the DSPs, so it is good to become familiar with that terminology now.

Table 3-14 and Table 3-15 outline the activities that occur on these interfaces. Table 3-14 describes the behavior when the gateway receives a seize or idle state on its M-lead from the LMR endpoint. Table 3-15 describes how the gateway generates a seize or idle state on its E-lead to the LMR endpoint. The signal translation tables referenced in the table are displayed in the **debug vpm signal** command output.

Table 3-14 Signaling from LMR Endpoint to Network

Action	LMR -> E&M	E&M -> DSP	DSP -> RTP
Seize	The LMR device either applies battery (for E&M signaling Types I, II, and III) or grounds (for Type V) the M-lead on the gateway's E&M interface indicating a squelch open (radio terminology) or off-hook (voice terminology) condition.	The E&M interface converts the seize signal to a digital ABCD bit representation of 1111 (0xF) and passes it the DSP.	The DSP looks up the signal state value at position 0xF in the transmit signal translation table. This state value is set with the **define rx-bits seize** command. The default seize bit pattern is 1111. The state value is placed in a signaling RTP packet for transmission across the network.
Idle	The LMR device either grounds the M-lead (for Type I and Type III) or opens the circuit (for Type II and Type V) on the gateway's E&M interface indicating a squelch closed or on-hook condition.	The E&M interface converts the seize signal to a digital ABCD bit representation of 0000 (0x0) and passes it the DSP.	The DSP looks up the signal state value at position 0x0 in the transmit signal translation table. This state value is set with the **define rx-bits idle** command. The default idle bit pattern is 0000. The state value is placed in a signaling RTP packet for transmission across the network.

Table 3-15 Signaling from Network to LMR Endpoint

Action	RTP -> DSP	DSP -> E&M	E&M -> LMR
Seize	When a signaling RTP packet is received from the network, it is passed to the DSP. The DSP looks up the appropriate ABCD bit pattern based on the received signaling state in the receive signal translation table. The ABCD bit pattern corresponds to the pattern set with the **define tx-bits seize** command. The default bit pattern is 1111.	The DSP passes the ABCD bit pattern to the E&M interface. For a seize, the bit pattern will be 1111.	The gateway grounds the E-lead on its E&M interface indicating to the LMR device that the PTT button is depressed (radio terminology), or we have gone off-hook (voice terminology).

Table 3-15 Signaling from Network to LMR Endpoint

Action	RTP -> DSP	DSP -> E&M	E&M -> LMR
Idle	When a signaling RTP packet is received from the network, it is passed to the DSP. The DSP looks up the appropriate ABCD bit pattern based on the received signaling state in the receive signal translation table. The ABCD bit pattern corresponds to the pattern set with the **define tx-bits idle** command. The default bit pattern is 0000.	The DSP passes the ABCD bit pattern to the E&M interface. For an idle, the bit pattern will be 0000.	The gateway opens the E-lead on its E&M interface indicating to the LMR device that the PTT button is released, or we have gone on-hook.

To take the guesswork out of configuring the bit patterns, Table 3-16 documents the gateway E&M interface behavior for all possible lead states and bit patterns. Table 3-16 applies to both digital and analog interfaces. The debug vpm signal command output columns show the output if the **debug vpm signal** command is enabled on the gateway. The default receive and transmit bit patterns, seize = 1111 and idle = 0000, are in bold.

Table 3-16 Interface Behavior for Lead State and Bit Pattern Combinations

M-Lead	rx-bits seize	rx-bits idle	debug vpm signal command output	tx-bits seize	tx-bits idle	debug vpm signal command output	E-Lead
Idle	**1111**	**0000**	`rcv from dsp sig DCBA state 0x0 encap 1`	**1111**	**0000**	`send RTP to dsp sig DCBA state 0x0`	Idle
Idle	**1111**	**0000**	`rcv from dsp sig DCBA state 0x0 encap 1`	1111	1111	`send RTP to dsp sig DCBA state 0x0`	Seize
Idle	**1111**	**0000**	`rcv from dsp sig DCBA state 0x0 encap 1`	0000	1111	`send RTP to dsp sig DCBA state 0x0`	Seize
Idle	**1111**	**0000**	`rcv from dsp sig DCBA state 0x0 encap 1`	0000	0000	`send RTP to dsp sig DCBA state 0x0`	Idle
Idle	**1111**	**1111**	**`rcv from dsp sig DCBA state 0x0 encap 1`**	**1111**	**0000**	`send RTP to dsp sig DCBA state 0x0`	Idle
Idle	**1111**	**1111**	**`rcv from dsp sig DCBA state 0x0 encap 1`**	1111	1111	`send RTP to dsp sig DCBA state 0x0`	Seize
Idle	**1111**	**1111**	**`rcv from dsp sig DCBA state 0x0 encap 1`**	0000	1111	`send RTP to dsp sig DCBA state 0x0`	Seize
Idle	**1111**	**1111**	**`rcv from dsp sig DCBA state 0x0 encap 1`**	0000	0000	`send RTP to dsp sig DCBA state 0x0`	Idle
Idle	0000	1111	`rcv from dsp sig DCBA state 0xF encap 1`	**1111**	**0000**	`send RTP to dsp sig DCBA state 0xF`	Seize
Idle	0000	1111	`rcv from dsp sig DCBA state 0xF encap 1`	1111	1111	`send RTP to dsp sig DCBA state 0xF`	Seize
Idle	0000	1111	`rcv from dsp sig DCBA state 0xF encap 1`	0000	1111	`send RTP to dsp sig DCBA state 0xF`	Idle
Idle	0000	1111	`rcv from dsp sig DCBA state 0xF encap 1`	0000	0000	`send RTP to dsp sig DCBA state 0xF`	Idle

Table 3-16 Interface Behavior for Lead State and Bit Pattern Combinations (continued)

M-Lead	rx-bits seize	rx-bits idle	debug vpm signal command output	tx-bits seize	tx-bits idle	debug vpm signal command output	E-Lead
Idle	0000	0000	rcv from dsp sig DCBA state 0x0 encap 1	**1111**	**0000**	send RTP to dsp sig DCBA state 0x0	Idle
Idle	0000	0000	rcv from dsp sig DCBA state 0x0 encap 1	1111	1111	send RTP to dsp sig DCBA state 0x0	Seize
Idle	0000	0000	rcv from dsp sig DCBA state 0x0 encap 1	0000	1111	send RTP to dsp sig DCBA state 0x0	Seize
Idle	0000	0000	rcv from dsp sig DCBA state 0x0 encap 1	0000	0000	send RTP to dsp sig DCBA state 0x0	Idle
Seize	**1111**	**0000**	**rcv from dsp sig DCBA state 0xF encap 1**	**1111**	**0000**	send RTP to dsp sig DCBA state 0xF	Seize
Seize	**1111**	**0000**	**rcv from dsp sig DCBA state 0xF encap 1**	1111	1111	send RTP to dsp sig DCBA state 0xF	Seize
Seize	**1111**	**0000**	**rcv from dsp sig DCBA state 0xF encap 1**	0000	1111	send RTP to dsp sig DCBA state 0xF	Idle
Seize	**1111**	**0000**	**rcv from dsp sig DCBA state 0xF encap 1**	0000	0000	send RTP to dsp sig DCBA state 0xF	Idle
Seize	**1111**	**1111**	rcv from dsp sig DCBA state 0x0 encap 1	**1111**	**0000**	send RTP to dsp sig DCBA state 0x0	Idle
Seize	**1111**	**1111**	rcv from dsp sig DCBA state 0x0 encap 1	1111	1111	send RTP to dsp sig DCBA state 0x0	Seize
Seize	**1111**	**1111**	rcv from dsp sig DCBA state 0x0 encap 1	0000	1111	send RTP to dsp sig DCBA state 0x0	Seize
Seize	**1111**	**1111**	rcv from dsp sig DCBA state 0x0 encap 1	0000	0000	send RTP to dsp sig DCBA state 0x0	Idle
Seize	0000	1111	rcv from dsp sig DCBA state 0x0 encap 1	**1111**	**0000**	send RTP to dsp sig DCBA state 0x0	Idle
Seize	0000	1111	rcv from dsp sig DCBA state 0x0 encap 1	1111	1111	send RTP to dsp sig DCBA state 0x0	Seize
Seize	0000	1111	rcv from dsp sig DCBA state 0x0 encap 1	0000	1111	send RTP to dsp sig DCBA state 0x0	Seize
Seize	0000	1111	rcv from dsp sig DCBA state 0x0 encap 1	0000	0000	send RTP to dsp sig DCBA state 0x0	Idle
Seize	0000	0000	**rcv from dsp sig DCBA state 0x0 encap 1**	**1111**	**0000**	send RTP to dsp sig DCBA state 0x0	Idle
Seize	0000	0000	**rcv from dsp sig DCBA state 0x0 encap 1**	1111	1111	send RTP to dsp sig DCBA state 0x0	Seize
Seize	0000	0000	**rcv from dsp sig DCBA state 0x0 encap 1**	0000	1111	send RTP to dsp sig DCBA state 0x0	Seize
Seize	0000	0000	**rcv from dsp sig DCBA state 0x0 encap 1**	0000	0000	send RTP to dsp sig DCBA state 0x0	Idle

The rx-bits patterns where both the seize and idle patterns are set to 1111 are in bold also. The behavior for these permutations differs from what you may expect and represents a departure from normal bit conditioning for LMR interfaces only. As outlined previously, if the M-lead registers an idle state, the rx-bits idle pattern is used as the internal state. So, if the M-lead is idle and the rx-bits idle pattern is 0000, the state is 0x0. When the rx-bits idle pattern is 1111, the state is 0xF. However, for the rx-bits patterns where both the seize and idle patterns are set to 1111, the rx-bits idle pattern is 1111, but the state is 0x0.

This behavior was instituted for the unicast connection trunk configurations. With unicast connection trunks, the signaling packets serve a dual purpose as a way to transmit signaling information and as a keepalive mechanism to monitor the health of the connection. So, even if there is no signaling transition on an interface, we will see a signaling packet from each side of the trunk every five seconds, unless the keepalive timer is changed. See the "Connection Initialization" section on page 4-4 for instructions for changing the keepalive timer. The recipient of these keepalive packets will set the E-lead state based on this signaling, even if the E-lead status is set to inactive on the voice port. If one side of the unicast trunk connection is using physical signaling and the other side is not, then to ensure that the lead states do not change, you can either turn off keepalives, which is not recommended, or alter the bit patterns so that idle is always played out on that other side. So, if both the seize and idle rx-bits patterns have the same value (either both 0000 or both 1111), then idle signaling packets are always sent to the other side. The transmitting gateway can then set the tx-bits patterns to either always play a seize or an idle, depending on what is appropriate.

You can determine current bit patterns for the interface with the **show voice port** command as shown in the following example:

```
lmr-3725e# show voice port 1/0/0 | inc ABCD

Rx Seize ABCD bits = 1111 Default pattern
 Rx Idle ABCD bits = 0000 Default pattern
 Tx Seize ABCD bits = 1111 Default pattern
 Tx Idle ABCD bits = 0000 Default pattern
 Ignored Rx ABCD bits = BCD
```

Codec Selection

Cisco VoIP gateways use coder-decoders (codecs), which are integrated circuit devices that typically use pulse code modulation (PCM) to transform analog signals into a digital bit stream and digital signals back into analog signals.

Some codec compression techniques require more processing power than others. Codec complexity is broken into two categories, medium and high complexity. The difference between medium and high complexity codecs is the amount of CPU utilization necessary to process the codec algorithm, and therefore, the number of voice channels that can be supported by a single DSP. Medium complexity codecs support four channels per DSP. High complexity codecs support two channels per DSP. For this reason, all the medium complexity codecs can also be run in high complexity mode, but fewer (usually half) of the channels are available per DSP.

Connections that require the transport of in-band tones for radio control, modem tones, or dual tone multifrequency (DTMF), should use full rate codecs, like G.711. If transcoding is required, it is recommended that transcoding be done only once for any end-to-end connection to minimize impacts to speech quality. Low bit rate codecs can be used if DTMF transmission is required, provided both ends of the connection support compatible out-of-band schemes like DTMF relay using H.245.

Gateway to Gateway Connections: Transport

This chapter describes three options for connecting LMR gateways:

Connection Trunk (Unicast)

This section describes these aspects of unicast connection trunk connections:

Overview

In general, a trunk, or tie line, is a permanent point-to-point communication link between two voice endpoints. From a Cisco IOS software perspective, the unicast **connection trunk** command creates a permanent VoIP call between two VoIP gateways. It simulates a trunk connection by creating virtual trunk tie lines between two telephony endpoints. To the connected systems, it appears as if a T1 trunk is directly connecting them.

The key features of unicast connection trunk connections are:

- Permanent connection—always up
- Transports signaling end-to-end
- Can be used only with other Cisco IOS software-based devices supporting unicast connection trunk

From an LMR perspective, a typical application for the unicast connection trunk would be as a replacement for leased line connections. Instead of dedicating an entire circuit for LMR traffic, the circuit could be configured for IP transmission with the LMR traffic and other data traffic sharing the same line.

Notice that we continually qualify the connection trunk as either unicast or multicast. To the voice endpoints, both types present the same permanent tie-line style connection. The difference lies in how that connection is implemented across the IP network. The unicast version employs an H.323 connection setup mechanism to establish a channel to another voice gateway and directs the Real-Time Transport Protocol (RTP)/RTP Control Protocol (RTP/RTCP) datastream to that single endpoint. The multicast version directs the RTP/RTCP datastream to an IP multicast address so it can be received by any number of endpoints. Aside from the protocols used for multicast routing, no other telephony connection setup mechanism is used.

Configuration

The relevant format for the **connection trunk** command is as follows:

```
connection trunk digits [answer-mode]
```

The *digits* argument corresponds to the E.164 address used to identify the voice endpoint on the far side of the connection. The optional **answer-mode** keyword identifies this side of the connection as a "slave-side." As a slave-side, the gateway does not attempt to initiate a trunk connection, but instead waits for an incoming call before establishing the trunk. It is recommended that one side of the connection be configured with the **answer-mode** keyword. This configuration scheme minimizes the time routers take to bring up trunks and ensures that trunks go down when connections are lost between two gateways. Otherwise, the gateways might not attempt to reestablish the trunk when the underlying circuit is up again.

Although Cisco IOS software permits a range of voice endpoint options for connection trunk, in an LMR environment, the unicast connection trunk will be set up between two analog E&M ports, between two digital E&M ports, or from an analog E&M port to a digital E&M port. In addition to the physical interfaces, the configuration requires at least two voice dial peers. The VoIP voice dial peer is used to associate the E.164 address specified in the **connection trunk** command to the IP address for the gateway on the other side of the connection. The POTS voice dial peer is used to associate an incoming E.164 address to the physical interface on the gateway that will terminate the connection.

Example 4-1 shows a sample unicast trunk configuration for two routers, lmr-3745c and lmr-3725e. In this configuration, both routers connect through their FastEthernet0/1 interfaces because they are on the same LAN segment. The parts of the configurations in Example 4-1 that are referred to in the following sections are in bold.

Example 4-1 Sample Unicast Connection Trunk Configuration

Master Gateway lmr-3745c	Slave Gateway lmr-3725e
!	!
hostname lmr-3745c	hostname lmr-3725e
!	!
controller T1 1/0	!
framing esf	!
crc-threshold 320	!
linecode b8zs	!
cablelength short 133	!
! This line creates a digital LMR voice	!
! port. We use one time slot per voice	!
! port to ensure a 1:1 mapping between	!
! voice ports on the trunk connection.	!
ds0-group 0 timeslots 1 type e&m-lmr	!
!	!
interface FastEthernet0/1	interface FastEthernet0/1
ip address 10.40.0.2 255.255.255.0	ip address 10.40.0.1 255.255.255.0
duplex auto	duplex auto
speed auto	speed auto
!	!
voice-port 1/0:0	voice-port 1/0/0
! With this line, we control the flow of	lmr m-lead audio-gate-in
! voice frames onto the network based on	lmr e-lead seize
! the state of the M-lead from the LMR	operation 4-wire
! device. If the M-lead is raised, then	type 3
! we send voice frames on the connection.	signal lmr
lmr m-lead audio-gate-in	no echo-cancel enable
lmr e-lead seize	**connection trunk 40002 answer-mode**
no echo-cancel enable	!
connection trunk 40001	!
!	!
!	!
!	!
!	!
dial-peer voice 10400001 voip	dial-peer voice 10400002 voip
destination-pattern 4...1	destination-pattern 4...2
session target ipv4:10.40.0.1	session target ipv4:10.40.0.2
codec g711ulaw	codec g711ulaw
vad aggressive	vad aggressive
!	!
dial-peer voice 374540002 pots	**dial-peer voice 372540001 pots**
destination-pattern 40002	destination-pattern 40001
port 1/0:0	port 1/0/1
!	!
end	end

Operation

The stages in the life of a unicast trunk connection between two voice interfaces are as follows:

Connection Initialization

In this stage, we actually build the permanent connection between the endpoints. The gateway routers:

- Establish an H.323 connection.

- Perform H.225.0 session negotiation.
- Synchronize the endpoints.

Data transfer

Once the connection is established, the endpoints sit in an inactive state sending connection maintenance frames, until either end decides to send data, which is the active state.

- Inactive state:
  - RTCP sender and receiver reports are sent.
  - Signaling keepalives are sent.
- Active state:
  - RTCP sender and receiver reports are sent.
  - Signaling transitions are sent.
  - RTP voice frames are sent.

Disconnect

Because this is a permanent connection, it will stay up as long as the gateways, their respective voice interfaces, and the IP connection between them stay up.

Connection Initialization

From a Cisco IOS software perspective, when the voice interface on the master side of the connection, router lmr-3745c, enters the up state, both administratively and operationally, the gateway places a call to the E.164 address specified in the **connection trunk** command. In this case, the number dialed is 40001. This address matches the destination pattern address configured on the VoIP dial peer with tag 10400001. Thus, the target IP address for the H.323 connection for the device on the slave side of the connection, router lmr-3725e, is 10.40.0.1.

Looking at the frames on the wire, an H.323 connection is established from the master to the slave gateways as seen in Table 4-1.

Table 4-1 Unicast Connection Trunk Connection Initialization Frames

Frame	Time (sec)	Source	Destination	Protocol	Src Port	Dest Port	Length	Information
1	0	10.40.0.2	Broadcast	ARP[1]	—	—	60	Who has 10.40.0.1? Tell 10.40.0.2
2	0.000298	10.40.0.1	10.40.0.2	ARP	—	—	60	10.40.0.1 is at 00:07:b3:5d:0a:91
3	1.99729	10.40.0.2	10.40.0.1	TCP	11000	1720	60	11000 > 1720 [SYN] Seq=2509514642 Ack=0 Win=4128 Len=0
4	1.997989	10.40.0.1	10.40.0.2	TCP	1720	11000	60	1720 > 11000 [SYN, ACK] Seq=3049137647 Ack=2509514643 Win=4128 Len=0
5	1.998175	10.40.0.2	10.40.0.1	TCP	11000	1720	60	11000 > 1720 [ACK] Seq=2509514643 Ack=3049137648 Win=4128 Len=0

Table 4-1 Unicast Connection Trunk Connection Initialization Frames (continued)

Frame	Time (sec)	Source	Destination	Protocol	Src Port	Dest Port	Length	Information
6	1.999282	10.40.0.2	10.40.0.1	H.255.0	11000	1720	361	CS: setup OpenLogicalChannel [Unreassembled Packet]
7	2.009371	10.40.0.1	10.40.0.2	H.255.0	1720	11000	177	CS: callProceeding OpenLogicalChannel
8	2.011518	10.40.0.1	10.40.0.2	H.255.0	1720	11000	124	CS: alerting
9	2.013301	10.40.0.1	10.40.0.2	H.255.0	1720	11000	165	CS: connect

1. Address Resolution Protocol

After establishing the MAC-layer address for the slave gateway in frames 1 and 2, the master gateway opens a TCP connection to the H.323 port (1720) on the slave in frames 3 through 5. The master issues an H.225 call setup message containing the calling number (40002), the called number (40001), the media channel (RTP/18654), and the media control channel (RTCP/18655). The slave responds with an H.225 call proceeding message that contains its media channel (RTP/16664) and media control channel (RTCP/16665).

The called number in the call setup message matches the destination pattern configured on the POTS dial peer with tag 372541001 on the slave gateway in Example 4-1. Under that dial peer, the destination pattern is associated with voice port 1/0/0. Voice port 1/0/0 also has a connection trunk configured. The E.164 address on that connection trunk command (40002) matches the calling number contained in the call setup. The slave gateway responds again to the master with an alerting message. If the calling and called addresses on the slave gateway did not correspond to the called and calling addresses on the master, the slave would have responded with a release complete message after the call proceeding message and the trunk would not be created.

Immediately following the alerting message, the slave gateway sends out a connect message indicating everything is set up on its end. So, at this point, both gateways have presumably set up all the structures on their respective ends to handle the data stream. They also know each other's RTP and RTCP ports to use in sending the data. However, before the real voice traffic commences, the gateways send synchronization frames as shown in Table 4-2.

Table 4-2 Unicast Connection Trunk Synchronization Frames

Frame	Time (sec)	Source	Destination	Protocol	Src Port	Dest Port	Length	Information
14	2.07382	10.40.0.2	10.40.0.1	RTP	18654	16664	214	Payload type=ITU-T G.711 PCMU, SSRC=199491586, Seq=8120, Time=40347
15	2.078833	10.40.0.2	10.40.0.1	RTP	18654	16664	70	Payload type=Unknown (123), SSRC=186122242, Seq=0, Time=0, Mark
16	2.0897	10.40.0.1	10.40.0.2	RTP	18654	16664	70	Payload type=Unknown (123), SSRC=482017281, Seq=0, Time=0
17	2.093819	10.40.0.2	10.40.0.1	RTP	18654	16664	214	Payload type=ITU-T G.711 PCMU, SSRC=199491586, Seq=8121, Time=40507

Table 4-2 Unicast Connection Trunk Synchronization Frames (continued)

Frame	Time (sec)	Source	Destination	Protocol	Src Port	Dest Port	Length	Information
18	2.098826	10.40.0.2	10.40.0.1	RTP	18654	16664	70	Payload type=Unknown (123), SSRC=186122242, Seq=0, Time=0, Mark
19	2.109381	10.40.0.1	10.40.0.2	RTP	18654	16664	70	Payload type=Unknown (123), SSRC=482017281, Seq=0, Time=0

The master side of the connection sends an RTP voice frame containing 20 ms of voice in frames 14 and 17, and a channel-associated signaling (CAS) signaling frame in frames 15 and 18 every 20 ms. The slave side responds with a CAS signaling frame in frames 16 and 19. This three-frame handshake occurs 24 times over the next half-second as shown in Table 4-3.

Table 4-3 Three-Frame Handshake Frames

Frame	Time (sec)	Source	Destination	Protocol	Src Port	Dest Port	Length	Information
89	7.520661	10.40.0.2	10.40.0.1	RTP	18654	16664	70	Payload type=Unknown (123), SSRC=186122242, Seq=0, Time=0
90	7.571345	10.40.0.1	10.40.0.2	RTP	16664	18654	70	Payload type=Unknown (123), SSRC=482017281, Seq=0, Time=0
91	10.98381	10.40.0.2	10.40.0.1	RTCP	18655	16665	146	Sender Report
92	11.25979	10.40.0.1	10.40.0.2	RTCP	16665	18655	146	Sender Report
93	12.52268	10.40.0.2	10.40.0.1	RTP	18654	16664	70	Payload type=Unknown (123), SSRC=186122242, Seq=0, Time=0
94	12.57333	10.40.0.1	10.40.0.2	RTP	16664	18654	70	Payload type=Unknown (123), SSRC=482017281, Seq=0, Time=0
95	13.76831	10.40.0.1	10.40.0.2	RTCP	16665	18655	146	Sender Report
96	14.15189	10.40.0.2	10.40.0.1	RTCP	18655	16665	146	Sender Report
97	17.52471	10.40.0.2	10.40.0.1	RTP	18654	16664	70	Payload type=Unknown (123), SSRC=186122242, Seq=0, Time=0
98	17.57529	10.40.0.1	10.40.0.2	RTP	16664	18654	70	Payload type=Unknown (123), SSRC=482017281, Seq=0, Time=0
99	18.73985	10.40.0.1	10.40.0.2	RTCP	16665	18655	146	Sender Report
100	20.94287	10.40.0.2	10.40.0.1	RTCP	18655	16665	146	Sender Report
101	22.52673	10.40.0.2	10.40.0.1	RTP	18654	16664	70	Payload type=Unknown (123), SSRC=186122242, Seq=0, Time=0
102	22.57727	10.40.0.1	10.40.0.2	RTP	16664	18654	70	Payload type=Unknown (123), SSRC=482017281, Seq=0, Time=0

After the synchronization period, in the absence of any voice or signaling frames traversing the connection, each side of the connection issues a keepalive frame. The default period of these keepalive messages is five seconds. The rate can be adjusted using the following configuration command:

signal keepalive {*seconds* | **disabled**}

Although it is possible to turn off the keepalive messages altogether, it is not advisable because their presence helps the gateways know when there is a problem with the connection.

These keepalive frames use the CAS signaling payload type (123). They reflect the current state of the signaling across the connection. For instance, if the LMR device connected to the slave side has its E-lead high, then the keepalive frames will carry the 0xF (1111) signaling bits across to the master side of the connection to be played out.

Included in the mix of frames for the connection are the RTCP media control channel frames. Each side of the connection will issue a sender report or receiver report about every five seconds. See *RFC 1889 - RTP: A Transport Protocol for Real-Time Applications* for more information on the contents of these frames. Sender reports are sent when the sender has sent any RTP frames since the last report. In the quiescent state, because the default is to send keepalive CAS signaling frames every five seconds, sender reports are usually seen from each side as shown in Table 4-4.

Table 4-4 Sender Report Frames

Frame	Time (sec)	Source	Destination	Protocol	Src Port	Dest Port	Length	Information
121	47.53689	10.40.0.2	10.40.0.1	RTP	18654	16664	70	Payload type=Unknown (123), SSRC=186122242, Seq=0, Time=0
122	47.58715	10.40.0.1	10.40.0.2	RTP	16664	18654	70	Payload type=Unknown (123), SSRC=482017281, Seq=0, Time=0
123	47.8469	10.40.0.2	10.40.0.1	RTCP	18655	16665	146	Sender Report
124	50.42424	10.40.0.1	10.40.0.2	RTCP	16665	18655	146	Sender Report
125	50.84008	10.40.0.2	10.40.0.1	RTCP	18655	16665	126	Receiver Report
126	52.53889	10.40.0.2	10.40.0.1	RTP	18654	16664	70	Payload type=Unknown (123), SSRC=186122242, Seq=0, Time=0
127	52.5891	10.40.0.1	10.40.0.2	RTP	16664	18654	70	Payload type=Unknown (123), SSRC=482017281, Seq=0, Time=0
128	55.1975	10.40.0.2	10.40.0.1	RTCP	18655	16665	146	Sender Report
129	56.31227	10.40.0.1	10.40.0.2	RTCP	16665	18655	146	Sender Report
130	57.54097	10.40.0.2	10.40.0.1	RTP	18654	16664	70	Payload type=Unknown (123), SSRC=186122242, Seq=0, Time=0
131	57.59106	10.40.0.1	10.40.0.2	RTP	16664	18654	70	Payload type=Unknown (123), SSRC=482017281, Seq=0, Time=0

However, RFC 1889 provides for a jitter factor on the frames of between 0.5 and 1.5 times the nominal arrival rate, so it is possible for one side of the connection to send two RTCP frames within the keepalive time. In this case, the first RTCP frame after the keepalive will be a sender report, and the next RTCP frame will be a receiver report as shown in frames 123 through 125 of Table 4-4.

Finally, the TCP stack sends periodic keepalives for the H.323 connection during the life of the connection trunk as shown in Table 4-5. The master gateway initiates this messaging every 60 seconds.

Table 4-5 Periodic TCP Keepalive Frames

Frame	Time (sec)	Source	Destination	Protocol	Src Port	Dest Port	Length	Information
134	62.00001	10.40.0.2	10.40.0.1	TCP	11000	1720	60	11000 > 1720 [ACK] Seq=2509514949 Ack=3049137951 Win=3824 Len=0
135	62.00027	10.40.0.1	10.40.0.2	TCP	1720	11000	60	1720 > 11000 [ACK] Seq=3049137952 Ack=2509514950 Win=3821 Len=0
186	121.9868	10.40.0.2	10.40.0.1	TCP	11000	1720	60	11000 > 1720 [ACK] Seq=2509514949 Ack=3049137951 Win=3824 Len=0
187	121.9871	10.40.0.1	10.40.0.2	TCP	1720	11000	60	1720 > 11000 [ACK] Seq=3049137952 Ack=2509514950 Win=3821 Len=0
234	181.9736	10.40.0.2	10.40.0.1	TCP	11000	1720	60	11000 > 1720 [ACK] Seq=2509514949 Ack=3049137951 Win=3824 Len=0
235	181.9738	10.40.0.1	10.40.0.2	TCP	1720	11000	60	1720 > 11000 [ACK] Seq=3049137952 Ack=2509514950 Win=3821 Len=0

Caveats

- A single **ds0-group** command can be defined to handle all the DS0s on a digital interface, and a single **connection trunk** command can be defined on the associated voice port. This would reduce the amount of manual configuration required to 1 voice port and 1 POTS dial peer, instead of 24 voice ports and 24 POTS dial peers for a fully loaded T1. However, there is no guarantee of one-to-one mapping of DS0s on either end of the trunk. In addition, each time the router reloads, the mapping can be different from last time. This configuration complicates troubleshooting because you are not able to isolate the problem to a single, or even a few, time slots without taking down the entire trunk group. This configuration may also not be practical given the configuration of the LMR units that will attach to the digital interfaces.
- The only way to guarantee that a particular DS0 on one router maps through connection trunk to a particular DS0 on another router is to create a DS0 group for each DS0 on the T1.

Connection PLAR

This section describes these aspects of PLAR connections:

Overview

Private line automatic ringdown (PLAR) circuits are switched connections between statically configured voice endpoints. The endpoints have the destination address of the connection preconfigured and so do not require user dialing to connect calls. PLAR connections are those in which a phone goes off-hook and a remote phone rings without digits being dialed. As switched calls, the connections will be torn down on certain events; for example, the calling party goes on-hook, and the resources made available for other connections.

The following are the main similarities and differences between connection PLAR mode and connection trunk (unicast) mode:

- Connection trunk mode is a permanent connection; the VoIP call is always connected independently of the associated voice port being on-hook or off-hook.
- Connection PLAR mode is a switched VoIP call; the call is set up on an as-needed basis. With connection PLAR, no bandwidth is consumed while the device connected to the associated voice port is on-hook. When a device is taken off-hook, the call is automatically connected, and the remote device is signaled to go off-hook.
- Both connection trunk (unicast) and connection PLAR modes have statically configured endpoints and do not require user dialing to connect calls.
- Connection trunk (unicast) mode allows supplemental call signaling to be passed over the IP network between the two telephony devices. Connection PLAR transports only limited types of signaling.
- Connection PLAR does not use a proprietary keepalive mechanism and is thus can establish connections to other H.323 capable endpoints.

From an LMR standpoint, PLAR connections would be employed in those leased line replacement scenarios in which the overhead of a connection trunk (unicast) connection was not needed or desired. PLAR connections would also be useful for connecting to non-Cisco IOS software-based devices that support H.323 call setup mechanisms.

Configuration

The relevant format for the **connection trunk** command is as follows:

```
connection plar digits
```

The *digits* argument corresponds to the E.164 address used to identify the voice endpoint on the far side of the connection. Although Cisco IOS software permits a range of voice endpoint options for connection PLAR, in an LMR environment a PLAR connection may be established only between two analog E&M ports, between two digital E&M ports, or between an analog E&M port and a digital E&M port. In addition to the physical interfaces, the configuration requires at least two voice dial peers. The VoIP voice dial peer is used to associate the E.164 address specified in the **connection plar** command to the IP address for the gateway on the other side of the connection. The POTS voice dial peer is used to associate an incoming E.164 address to the physical interface on the gateway that will terminate the connection.

Table 4-5 shows a sample connection PLAR configuration for two routers, lmr-3745c and lmr-3725e. In this configuration, both routers connect via their FastEthernet0/1 interfaces because they are on the same LAN segment. The parts of the configurations in Table 4-5 that are referred to in the following sections are in bold.

Example 4-2 Sample Connection PLAR Configuration

lmr-3745c	lmr-3725e
!	!
hostname lmr-3745c	hostname lmr-3725e
!	!
controller T1 1/0	!
framing esf	!
crc-threshold 320	!
linecode b8zs	!
cablelength short 133	!
!	!
interface FastEthernet0/1	interface FastEthernet0/1
ip address 10.40.0.2 255.255.255.0	**ip address 10.40.0.1 255.255.255.0**
duplex auto	duplex auto
speed auto	speed auto
!	!
voice-port 1/0:0	voice-port 1/0/0
lmr m-lead dialin	lmr m-lead dialin
lmr e-lead voice	lmr e-lead voice
no echo-cancel enable	operation 4-wire
timeouts call-disconnect 3	type 3
timeouts teardown lmr 30	signal lmr
timing hookflash-in 0	no echo-cancel enable
connection plar 41001	timeouts call-disconnect 3
!	**timeouts teardown lmr 25**
!	timing hookflash-in 0
!	connection plar
!	!
!	!
dial-peer voice 10400001 voip	dial-peer voice 10400002 voip
destination-pattern 4...1	destination-pattern 4...2
session target ipv4:10.40.0.1	session target ipv4:10.40.0.2
codec g711ulaw	codec g711ulaw
vad aggressive	vad aggressive
!	!
!	!
dial-peer voice 374541002 pots	**dial-peer voice 372541001 pots**
destination-pattern 41002	destination-pattern 41001
port 1/0:0	port 1/0/0
!	!
!	!
end	end

Operation

The stages in the life of a PLAR connection between two voice interfaces are as follows:

Connection Initialization

In this stage, we actually build the permanent connection between the endpoints. The gateway routers:

- Establish an H.323 connection.
- Perform H.225.0 session negotiation.
- Synchronize the endpoints.

Data Transfer

Once the connection is established, the endpoints sit in an inactive state sending connection maintenance frames, until either end decides to send data, which is the active state.

- Inactive state. RTCP sender and receiver reports are sent.
- Active state:
  - RTCP sender and receiver reports are sent.
  - RTP voice frames are sent.

Disconnect

For Cisco IOS software-based LMR gateways, when the party initiating the call goes on-hook, which is the M-lead idle state, it starts the call teardown timer on that gateway. For the LMR gateway receiving the call, as soon as it stops receiving voice frames, it starts its call teardown timer. The gateway whose timer expires first initiates the actual call teardown.

Connection Initialization

In this section, we examine the PLAR connection initialization process in detail. The examples will use two Cisco IOS software-based gateways running software containing the LMR feature. Although technically either side can initiate the call that brings up the connection, we will refer to the gateway making the call as the "calling" gateway and the one on the receiving end of the call as the "called" gateway.

From a Cisco IOS software perspective, the voice interfaces associated with the PLAR connection on both the calling and called gateways must be in an up state, both administratively and operationally. In order to initiate the call, the calling gateway (lmr-3745c) must have its voice interface configured with the **lmr m-lead** command with the **dialin** option as shown in Table 4-5. The other two M-lead options, **inactive** and **audio-gate-in**, will not trigger the H.323 connection process. With the **lmr m-lead dialin** command configured, when the M-lead enters a seize state, the gateway places a call to the E.164 address specified in the **connection plar** command. In this case, the number dialed is 41001. This address matches the destination pattern address configured on the VoIP dial peer with tag 10400001. Thus, the target IP address for the H.323 connection to the called gateway (lmr-3725e) is 10.40.0.1.

Looking at the frames on the wire, an H.323 connection is established from the calling to called gateways as seen in Table 4-6.

Table 4-6 Connection PLAR Connection Initialization Frames

Frame	Time (sec)	Source	Destination	Protocol	Src Port	Dest Port	Length	Information
4	10.75153	10.40.0.2	Broadcast	ARP	—	—	60	Who has 10.40.0.1? Tell 10.40.0.2
5	10.75184	10.40.0.1	10.40.0.2	ARP	—	—	60	10.40.0.1 is at 00:07:b3:5d:0a:91
6	12.74956	10.40.0.2	10.40.0.1	TCP	11000	1720	60	11000 > 1720 [SYN] Seq=4291627303 Ack=0 Win=4128 Len=0
7	12.75026	10.40.0.1	10.40.0.2	TCP	1720	11000	60	1720 > 11000 [SYN, ACK] Seq=1500783035 Ack=4291627304 Win=4128 Len=0

Table 4-6 Connection PLAR Connection Initialization Frames (continued)

Frame	Time (sec)	Source	Destination	Protocol	Src Port	Dest Port	Length	Information
8	12.75047	10.40.0.2	10.40.0.1	TCP	11000	1720	60	11000 > 1720 [ACK] Seq=4291627304 Ack=1500783036 Win=4128 Len=0
9	12.75153	10.40.0.2	10.40.0.1	H.225.0	11000	1720	361	CS: setup OpenLogicalChannel [Unreassembled Packet]
10	12.76163	10.40.0.1	10.40.0.2	H.225.0	1720	11000	177	CS: callProceeding OpenLogicalChannel
11	12.76367	10.40.0.1	10.40.0.2	H.225.0	1720	11000	142	CS: progress
12	12.82407	10.40.0.1	10.40.0.2	H.225.0	1720	11000	165	CS: connect

After establishing the MAC-layer address for the called gateway in frames 4 and 5, the calling gateway opens a TCP connection to the H.323 port (1720) on the called gateway in frames 6 through 8. The calling gateway issues an H.225 call setup message (frame 9) containing the calling number (40002), the called number (40001), the media channel (RTP 19508), and the media control channel (RTCP 19509).

The called number in the call setup message matches the destination pattern configured on the POTS dial peer with tag 372541001 on the called gateway. Thus, the called gateway responds with an H.225 call proceeding message in frame 10 that contains its media channel (RTP/16454) and media control channel (RTCP/16455). If the called gateway had been unable to match the called number to any voice port, it would have responded with a release complete message (unassigned number) and that would have been the end of the call. But, because the called number is assigned to a voice port, the called gateway responds again to the calling gateway with a progress message in frame 11.

Note that if the E.164 address configured on the **connection plar** command on the called gateway voice port did not match the calling number, the connection would still be established. The called gateway need only find a match on its POTS dial peer destination patterns for the called number to accept the call. Of course, because the calling gateway obtained the calling number from its associated POTS dial peer, if the called gateway tried to make a return call, it would not match the voice port on the calling router.

Immediately following the progress message, the called gateway sends out a connect message in frame 12 indicating everything is set up on its end. So, at this point, both gateways have presumably set up all the structures on their respective ends to handle the data stream. They also know each other's RTP and RTCP ports to use in sending the data. However, before the real voice traffic commences, the calling gateway sends about 2 seconds-worth of voice frames to the called gateway as shown in Table 4-7.

Table 4-7 Connection PLAR Synchronization Frames

Frame	Time (sec)	Source	Destination	Protocol	Src Port	Dest Port	Length	Information
13	12.82995	10.40.0.2	10.40.0.1	RTP	19508	16454	214	Payload type=ITU-T G.711 PCMU, SSRC=287375362, Seq=6698, Time=40347
14	12.84971	10.40.0.2	10.40.0.1	RTP	19508	16454	214	Payload type=ITU-T G.711 PCMU, SSRC=287375362, Seq=6699, Time=40507
15	12.8697	10.40.0.2	10.40.0.1	RTP	19508	16454	214	Payload type=ITU-T G.711 PCMU, SSRC=287375362, Seq=6700, Time=40667

Table 4-7 Connection PLAR Synchronization Frames (continued)

Frame	Time (sec)	Source	Destination	Protocol	Src Port	Dest Port	Length	Information
110	14.72861	10.40.0.2	10.40.0.1	RTP	19508	16454	214	Payload type=ITU-T G.711 PCMU, SSRC=287375362, Seq=6793, Time=55547
111	14.74859	10.40.0.2	10.40.0.1	RTP	19508	16454	214	Payload type=ITU-T G.711 PCMU, SSRC=287375362, Seq=6794, Time=55707
112	14.76859	10.40.0.2	10.40.0.1	RTP	19508	16454	134	Payload type=ITU-T G.711 PCMU, SSRC=287375362, Seq=6795, Time=55867
113	14.76861	10.40.0.2	10.40.0.1	RTP	19508	16454	60	Payload type=Unknown (19), SSRC=287375362, Seq=6796, Time=55947
114	14.98875	10.40.0.2	10.40.0.1	RTCP	19509	16455	146	Sender Report
115	16.30351	10.40.0.2	10.40.0.2	LOOP			60	Loopback
116	16.51785	10.40.0.2	10.40.0.1	RTCP	19509	16455	126	Receiver Report
117	16.93295	10.40.0.1	10.40.0.2	RTCP	16455	19509	150	Receiver Report
118	20.00043	10.40.0.1	10.40.0.1	LOOP			60	Loopback

The called side of the connection sends a series of RTP voice frame containing 20 ms of voice in frames 13 through 112. When the voice transmission ceases, the calling party sends an RTP type 19 (comfort noise) frame in frame 113. At that point each side of the connection will issue a sender report or receiver report about every 5 seconds. See *RFC 1889 - RTP: A Transport Protocol for Real-Time Applications* for more information on the contents of these frames. Sender reports are sent when a gateway has sent any RTP frames since it last issued a report. In the quiescent state, there will not be any keepalive or other RTP frames, so we should see only receiver reports.

Connection Teardown

Unlike the unicast connection trunk mode in which the connection stays up as long as the voice ports and underlying IP circuit are up, with connection PLAR, the voice call can be torn down from either side. Each gateway participating in the connection maintains a teardown timer. If there is an active connection, the teardown timer begins running whenever the interface M-lead is in an idle state and whenever no voice frames are received from the network. The length of this timer (in seconds) is set using the following command on the voice port:

```
timeouts teardown lmr {<5-60000> | infinity}
```

We will illustrate the operation of the teardown timer using the output of the **debug vpm signal** command. First, we examine the behavior on the calling router. When the M-lead is raised, we see the following debug messages:

```
lmr-3745c#
Jan 29 16:42:34.566 EST: htsp_process_event: [1/0:0(1), LMR_ONHOOK, E_DSP_SIG_1100]
lmr_onhook_offhook
Jan 29 16:42:34.566 EST: htsp_timer_stop htsp_setup_ind
```

```
Jan 29 16:42:34.566 EST: [1/0:0(1)] get_local_station_id calling num= calling name=
calling time=01/29 16:42  orig called=
Jan 29 16:42:34.566 EST: htsp_timer - 3000 msec
Jan 29 16:42:34.570 EST: htsp_process_event: [1/0:0(1), LMR_WAIT_SETUP_ACK,
E_HTSP_SETUP_ACK] lmr_wait_setup_ack_get_ack
Jan 29 16:42:34.570 EST: htsp_timer_stop
Jan 29 16:42:34.570 EST: htsp_process_event: [1/0:0(1), LMR_OFFHOOK, E_HTSP_PROCEEDING]
htsp_progress_notifyhtsp_call_bridged
Jan 29 16:42:34.582 EST: htsp_process_event: [1/0:0(1), LMR_OFFHOOK,
E_HTSP_VOICE_CUT_THROUGH] lmr_offhook_voice_cut
Jan 29 16:42:34.582 EST: htsp_timer_stop
Jan 29 16:42:34.582 EST: htsp_process_event: [1/0:0(1), LMR_OFFHOOK, E_HTSP_CONNECT]
lmr_offhook_connect
Jan 29 16:42:34.582 EST: htsp_timer_stop
Jan 29 16:42:34.582 EST: htsp_timer_stop2
```

The last line in bold indicates that the teardown timer has stopped running. As long as the calling gateway keeps the M-lead raised, the timer will not start. On the called side, the debug output from the same call appears as follows:

```
Jan 29 16:42:34.576 EST: htsp_timer_stop3 htsp_setup_req
Jan 29 16:42:34.576 EST: htsp_process_event: [1/0/0, LMR_ONHOOK, E_HTSP_SETUP_REQ]
lmr_onhook_setup
Jan 29 16:42:34.576 EST: htsp_timer_stop htsp_progress
Jan 29 16:42:34.576 EST: lmr_start_timer: 2000 ms
Jan 29 16:42:34.576 EST: htsp_timer - 2000 msechtsp_call_bridged
Jan 29 16:42:34.580 EST: htsp_process_event: [1/0/0, LMR_WAIT_CUT_THRU,
E_HTSP_VOICE_CUT_THROUGH] lmr_cut_thru
Jan 29 16:42:34.580 EST: htsp_timer_stop
Jan 29 16:42:34.580 EST: lmr_pak_suppress_enable FALSE
Jan 29 16:42:34.580 EST: lmr_start_timer2: 25 second
Jan 29 16:42:34.580 EST: htsp_timer2 - 25000 msec
Jan 29 16:42:34.580 EST: htsp_process_event: [1/0/0, LMR_CONNECT, E_DSP_SIG_0000]
lmr_conn_onhook
Jan 29 16:42:34.580 EST: htsp_timer_stop
Jan 29 16:42:34.580 EST: lmr_pak_suppress_enable TRUE
Jan 29 16:42:34.580 EST: lmr_start_timer2: 25 second
Jan 29 16:42:34.580 EST: htsp_timer2 - 25000 msec
Jan 29 16:42:34.604 EST: htsp_process_event: [1/0/0, LMR_CONNECT, E_HTSP_V_PAK_RCVD]
lmr_conn_pkt_rcvd
Jan 29 16:42:34.604 EST: htsp_timer_stop2 lmr_offhook (0)
Jan 29 16:42:34.604 EST: [1/0/0] set signal state = 0x8 timestamp = 0
Jan 29 16:42:36.888 EST: htsp_process_event: [1/0/0, LMR_CONNECT, E_HTSP_V_PAK_STOP]
lmr_conn_pkt_stoplmr_onhook (0)
Jan 29 16:42:36.888 EST: [1/0/0] set signal state = 0x0 timestamp = 0
Jan 29 16:42:36.888 EST: lmr_start_timer2: 25 second
Jan 29 16:42:36.888 EST: htsp_timer2 - 25000 msec
```

In the previous lines in bold, we actually see the timer start three times. The timeout value for this voice port is set at 25 seconds. Because we have not raised the M-lead on this side of the connection, we wholly depend on the presence of voice frames to stop the timer from running. We see this timer transition from start to stop and to start again during the two-second voice spurt sent when the call is made. When the called gateway gets another talk spurt a few seconds later, the following debug messages appear:

```
Jan 29 16:42:56.421 EST: htsp_process_event: [1/0/0, LMR_CONNECT, E_HTSP_V_PAK_RCVD]
lmr_conn_pkt_rcvd
Jan 29 16:42:56.421 EST: htsp_timer_stop2 lmr_offhook (0)
Jan 29 16:42:56.421 EST: [1/0/0] set signal state = 0x8 timestamp = 0
```

When the called gateway gets the voice frames and goes off-hook, the teardown timer stops counting as shown in the bold line of the previous debug messages. When the talk spurt ends and the called gateway goes on-hook, we see the following:

```
Jan 29 16:43:30.890 EST: htsp_process_event: [1/0/0, LMR_CONNECT, E_HTSP_V_PAK_STOP]
lmr_conn_pkt_stoplmr_onhook (0)
Jan 29 16:43:30.890 EST: [1/0/0] set signal state = 0x0 timestamp = 0
Jan 29 16:43:30.890 EST: lmr_start_timer2: 25 second
Jan 29 16:43:30.890 EST: htsp_timer2 - 25000 msec
```

If 25 seconds elapse since the called gateway went on-hook, the timer expires, and the call is torn down. On the called gateway, the following debug messages appear:

```
Jan 29 16:44:18.888 EST: htsp_process_event: [1/0/0, LMR_CONNECT, E_HTSP_V_PAK_STOP]
lmr_conn_pkt_stoplmr_onhook (0)
Jan 29 16:44:18.888 EST: [1/0/0] set signal state = 0x0 timestamp = 0
Jan 29 16:44:18.888 EST: lmr_start_timer2: 25 second
Jan 29 16:44:18.888 EST: htsp_timer2 - 25000 msec
lmr-3725e#
lmr-3725e#
lmr-3725e#
Jan 29 16:44:43.889 EST: htsp_process_event: [1/0/0, LMR_CONNECT, E_HTSP_EVENT_TIMER2]
lmr_offhook_timer
Jan 29 16:44:43.889 EST: htsp_timer_stop2
Jan 29 16:44:43.889 EST: htsp_timer_stop3
Jan 29 16:44:43.889 EST: htsp_process_event: [1/0/0, LMR_CONNECT, E_HTSP_RELEASE_REQ]
lmr_conn_release
Jan 29 16:44:43.889 EST: htsp_timer_stop
Jan 29 16:44:43.889 EST: htsp_timer_stop2 lmr_onhook (0)
Jan 29 16:44:43.889 EST: [1/0/0] set signal state = 0x0 timestamp = 0
```

On the calling gateway, the following debug messages appears:

```
lmr-3745c#
Jan 29 16:44:43.888 EST: htsp_timer_stop3
Jan 29 16:44:43.892 EST: htsp_process_event: [1/0:0(1), LMR_CONNECT, E_HTSP_RELEASE_REQ]
lmr_conn_release
Jan 29 16:44:43.892 EST: htsp_timer_stop
Jan 29 16:44:43.892 EST: htsp_timer_stop2 lmr_onhook (0)vnm_dsp_set_sig_state:[recEive and
transMit1/0:0(1)] set signal state = 0x0
```

If the called side had raised its M-lead at any time during the call, we would have seen messages similar to the bold lines in the previous debug messages indicating that timer had stopped.

Table 4-8 shows the disconnect mechanism from a frame trace perspective.

Table 4-8 Connection PLAR Disconnect Frames

Frame	Time (sec)	Source	Destination	Protocol	Src Port	Dest Port	Length	Information
119	21.02002	10.40.0.2	10.40.0.1	RTP	19508	16454	214	Payload type=ITU-T G.711 PCMU, SSRC=287375362, Seq=6797, Time=105867, Mark
120	21.03996	10.40.0.2	10.40.0.1	RTP	19508	16454	214	Payload type=ITU-T G.711 PCMU, SSRC=287375362, Seq=6798, Time=106027
121	21.0599	10.40.0.2	10.40.0.1	RTP	19508	16454	214	Payload type=ITU-T G.711 PCMU, SSRC=287375362, Seq=6799, Time=106187
122	21.07991	10.40.0.2	10.40.0.1	RTP	19508	16454	214	Payload type=ITU-T G.711 PCMU, SSRC=287375362, Seq=6800, Time=106347

Table 4-8 Connection PLAR Disconnect Frames (continued)

Frame	Time (sec)	Source	Destination	Protocol	Src Port	Dest Port	Length	Information
600	30.51938	10.40.0.2	10.40.0.1	RTP	19508	16454	214	Payload type=ITU-T G.711 PCMU, SSRC=287375362, Seq=7272, Time=181867
601	30.53936	10.40.0.2	10.40.0.1	RTP	19508	16454	214	Payload type=ITU-T G.711 PCMU, SSRC=287375362, Seq=7273, Time=182027
602	30.55936	10.40.0.2	10.40.0.1	RTP	19508	16454	214	Payload type=ITU-T G.711 PCMU, SSRC=287375362, Seq=7274, Time=182187
603	30.57934	10.40.0.2	10.40.0.1	RTP	19508	16454	214	Payload type=ITU-T G.711 PCMU, SSRC=287375362, Seq=7275, Time=182347
604	30.59933	10.40.0.2	10.40.0.1	RTP	19508	16454	214	Payload type=ITU-T G.711 PCMU, SSRC=287375362, Seq=7276, Time=182507
605	30.6093	10.40.0.2	10.40.0.1	RTP	19508	16454	60	Payload type=Unknown (19), SSRC=287375362, Seq=7277, Time=182667
607	34.88555	10.40.0.1	10.40.0.2	RTCP	16455	19509	150	Receiver Report
608	34.95209	10.40.0.2	10.40.0.1	RTCP	19509	16455	146	Sender Report
611	38.12519	10.40.0.2	10.40.0.1	RTCP	19509	16455	126	Receiver Report
613	40.49343	10.40.0.1	10.40.0.2	RTCP	16455	19509	126	Receiver Report
614	43.53205	10.40.0.2	10.40.0.1	RTCP	19509	16455	126	Receiver Report
615	43.90542	10.40.0.1	10.40.0.2	RTCP	16455	19509	126	Receiver Report
617	46.89014	10.40.0.1	10.40.0.2	RTCP	16455	19509	126	Receiver Report
618	49.03379	10.40.0.2	10.40.0.1	RTCP	19509	16455	126	Receiver Report
619	49.85	10.40.0.1	10.40.0.2	RTCP	16455	19509	126	Receiver Report
621	54.71046	10.40.0.2	10.40.0.1	RTCP	19509	16455	126	Receiver Report
622	55.89928	10.40.0.1	10.40.0.2	H.225.0	1720	11000	104	CS: releaseComplete
623	55.90063	10.40.0.2	10.40.0.1	H.225.0	11000	1720	104	CS: releaseComplete
624	55.90117	10.40.0.2	10.40.0.1	RTCP	19509	16455	86	Receiver Report
625	55.90234	10.40.0.1	10.40.0.2	RTCP	16455	19509	86	Receiver Report
626	55.90255	10.40.0.2	10.40.0.1	ICMP			70	Destination unreachable
627	56.09722	10.40.0.1	10.40.0.2	TCP	1720	11000	60	1720 > 11000 [ACK] Seq=1500783408 Ack=4291627661 Win=3771 Len=0

Either side may send voice traffic over the connection. In Table 4-8, note that there are no signaling frames sent advising the other side of lead status changes. In frames 119 through 604, the calling gateway sends out a stream of voice frames. Again, when the stream is finished, we see the RTP type 19 (comfort noise) frame in frame 605. For the next 25 seconds we see the expected handshake of RTCP sender and receiver report frames in frames 607 through 621.

Recall from the configuration in Example 4-2 that the called gateway (lmr-3725e) has the **timeouts teardown lmr 25** command configured on its voice port. The teardown timer starts after frame 605 in Table 4-8, and thus we see at frame 622 the called party sending a release complete message on the H.225 part of the connection. The calling party acknowledges the release by sending its own release complete message in frame 623.

Both sides send final RTCP receiver report messages in frames 624 and 625. It is interesting to note that the calling gateway has closed out its connection by the time it gets the receiver report from the called gateway. Thus, the calling gateway sends an Internet Control Message Protocol (ICMP) destination/port unreachable message to the called gateway. Finally, the TCP stack on both gateways send periodic acknowledgments on the H.323 connection every minute for the next 10 minutes until the TCP connection itself is finally torn down.

Connection Trunk (Multicast)

This section describes these aspects of multicast connection trunk connections:

Overview

The operation of a unicast connection trunk is described in the "Connection Trunk (Unicast)" section. As mentioned in that section, the other alternative to unicast operation was to send the audio traffic using a multicast connection trunk. The multicast connection trunk differs from the unicast version in the following key aspects:

- One-to-many transmission for the multicast trunk instead of one-to-one.
- No H.323 call setup between endpoints with the multicast trunk.
- No lead state signaling frames passed in the RTP stream with the multicast trunk.

With a multicast configuration, an endpoint joins a multicast group based on its configured destination multicast IP address. By joining this group, the endpoint sends its audio stream to all other members of the group. The endpoint also receives audio streams from all other members of the multicast group. So, by extension, the one-to-many transmission capability ends up serving as a many-to-many communications vehicle. It is worth noting that the endpoints need not be standard radio or telephony devices. Any application capable of decoding RTP audio streams can join the multicast group to receive and send audio.

Because the endpoints have no knowledge of how many, or if any, endpoints have joined the group, they have no way to perform a standard H.323 call setup with other endpoints. Instead, the endpoints perform the equivalent of a call setup by using the IP multicast join mechanism to make their multicast-enabled

neighbors aware that they want to communicate on a particular multicast address. The multicast-enabled neighbors connecting the various endpoints will perform the routing necessary to deliver RTP/RTCP frames transmitted by one endpoint to all the other subscribed endpoints. When an endpoint no longer wants to participate in that multicast group, it is pruned from the distribution tree and no longer factors into distribution decisions made by other multicast-enabled devices.

Similarly, because each endpoint can receive multicast frames from multiple endpoints simultaneously, lead state signaling information is not sent between the endpoints because of the potential confusion it would cause the receiver. The multicast endpoints terminate lead states from the connected devices and just present the audio RTP frames, and associated RTCP frames, to the multicast group. Endpoints that rely on physical, as opposed to in-band, signaling need to recognize the presence of audio frames on that multicast group and initiate the lead controls necessary to signal the end device that audio is present. This can be accomplished through the use of the various voice port LMR commands. However, for those endpoints that rely on in-band or tone signaling, either all endpoints on the network will have to participate in the same tone scheme, or other equipment will be necessary to allow different units to interoperate.

Configuration

Note Designing networks for multicast routing is a subject unto itself. The myriad of configuration and design options for a multicast network are dealt with extensively by other documents and guides. In this document we will present the information necessary to configure an LMR gateway to participate in a multicast network. We will also present traffic flow, addressing, and other information useful in integrating multicast LMR ports into a multicast network. However, the multicast routing scheme chosen in the following examples may or may not work effectively with the scheme employed in your network.

A successful LMR multicast trunk connection involves four elements:

- A voice-port configured for LMR and connection trunk.
- A VoIP dial peer configured for multicast operation.
- A voice class to control keepalive signaling.
- A virtual interface and multicast enabled network interfaces.

From a voice port perspective, the Cisco IOS software configuration necessary for a connection trunk is nearly the same for both the unicast and multicast versions. The only difference is that the **answer-mode** option is not used because technically there will never be a call set up message to answer. Thus, the command to configure the multicast connection trunk is as follows:

```
connection trunk digits
```

The *digits* argument corresponds to the E.164 address used to identify the connection. The address has local significance only because no call setup message is sent to communicate that address to any other party. This E.164 address needs to match a destination pattern in a VoIP dial peer elsewhere in the router's configuration. The VoIP dial peer is configured to use the multicast session protocol and a destination address of the multicast IP address and port number for that specific multicast group.

As we learned in the "Connection Trunk (Unicast)" section, the unicast trunks send periodic keepalives to maintain the status of the connection. If a device stops receiving those keepalives, it tears down the connection and, depending on whether it is the master or the slave, attempts to restart the connection. In a point-to-point environment, this mechanism works well to maintain the integrity of the trunk. However, in a point-to-multipoint environment where each endpoint is responsible only for building its leg of the connection, this mechanism provides no useful service, thus no keepalives are sent. However, the dial

peers still look for the presence of the keepalives to determine the status of the connection. Therefore, to prevent the trunks from going down due to lack of keepalives, we need to create a voice class with the following options:

```
voice class permanent 1
 signal timing oos timeout disabled
 signal keepalive disabled
```

This voice class should be assigned to each multicast voice port.

Finally, we need to enable the LMR gateway to participate in the multicast routing set up for the network. The first step is to create a virtual host interface with the **interface vif1** command. This is a virtual interface that is similar to a loopback interface, a logical IP interface that is always up when the router is active. The virtual interface requires its own subnet with at least two addresses (that is, a 30-bit mask for IPv4 addressing). The LMR gateway uses an address on the virtual interface subnet other than the one configured to source the multicast frames generated by the voice port. For example, if the virtual interface is configured with the IP address 10.52.0.5/30, multicast frames will use 10.52.0.6 as their source IP address. In addition, the virtual interface subnet needs to be included in routing update. The subnet needs to be reachable by other multicast participants so they can trace their reverse path back to this source.

The codec configured in the dial peer with the **codec** command must be the same as the codec configured on other applications that use these LMR gateway ports. Codecs must also be the same between all parties to a connection in order for speech to be recognizable. The default code for VoIP is G.729r8.

The **ip qos dscp** command assigns all of the RTP packets with a Differentiated Services Code Point (DSCP) value of 5, giving priority to VoIP packets. If this statement is not present, speech quality may suffer. The **ip qos dscp** command implements part of Quality of Service (QoS) for the entire VoIP network by identifying the packets that require special processing. Policing and traffic shaping must be implemented also by defining the special processing for the identified packets.

Example 4-3 shows a sample multicast trunk configuration for two routers, lmr-3725e and lmr-3745c. In this configuration, both routers connect through their FastEthernet0/1 interfaces because they are on the same LAN segment. The parts of the configurations in Example 4-3 that are referred to in the following sections are in bold.

Example 4-3 Sample Multicast Connection Trunk Configuration

lmr-3725e

```
!
hostname lmr-3725e
!
ip multicast-routing
!
voice class permanent 1
 signal timing oos timeout disabled
 signal keepalive disabled
!
!
!
!
!
!
!
interface Vif1
 ip address 10.52.0.5 255.255.255.252
 ip pim sparse-dense-mode
!
interface FastEthernet0/1
 ip address 10.50.0.2 255.255.255.0
 ip pim sparse-dense-mode
 load-interval 30
 duplex auto
 speed auto
!
router ospf 50
 log-adjacency-changes
 network 10.50.0.0 0.0.0.255 area 0.0.0.0
 network 10.52.0.4 0.0.0.3 area 0.52.0.4
!
ip pim bidir-enable
!
voice-port 2/0/0
 voice-class permanent 1
 operation 4-wire
 type 3
 signal lmr
 lmr m-lead audio-gate-in
 lmr e-lead voice
 no echo-cancel enable
 no comfort-noise
 timeouts call-disconnect 3
 timing hookflash-in 0
 connection trunk 500001
!
dial-peer voice 239500001 voip
 destination-pattern 500001
 session protocol multicast
 session target ipv4:239.50.00.01:20000
 codec g711ulaw
 ip qos dscp 5 media
 vad aggressive
!
end
```

lmr-3745c

```
!
hostname lmr-3745c
!
ip multicast-routing
!
voice class permanent 1
 signal timing oos timeout disabled
 signal keepalive disabled
!
controller T1 2/0
 framing esf
 linecode b8zs
 cablelength short 133
 ds0-group 0 timeslots 1 type e&m-lmr
!
interface Vif1
 ip address 10.52.0.1 255.255.255.252
 ip pim sparse-dense-mode
!
interface FastEthernet0/1
 ip address 10.50.0.1 255.255.255.0
 ip pim sparse-dense-mode
 load-interval 30
 duplex auto
 speed auto
!
router ospf 50
 log-adjacency-changes
 network 10.50.0.0 0.0.0.255 area 0.0.0.0
 network 10.52.0.0 0.0.0.3 area 0.52.0.0
!
ip pim bidir-enable
!
voice-port 2/0:0
 voice-class permanent 1
 lmr m-lead audio-gate-in
 lmr e-lead voice
 no echo-cancel enable
 no comfort-noise
 timeouts call-disconnect 3
 timing hookflash-in 0
 connection trunk 500001
!
!
!
!
dial-peer voice 239500001 voip
 destination-pattern 500001
 session protocol multicast
 session target ipv4:239.50.00.01:20000
 codec g711ulaw
 ip qos dscp 5 media
 vad aggressive
!
end
```

Operation

The stages in the life of a multicast trunk connection are as follows:

Connection Initialization

The connection initialization process for a multicast connection trunk consists of the LMR gateway joining the multicast group identified by the multicast address configured on the associated dial peer. There is no H.323 or similar call set up mechanism.

Data Transfer

Once the connection is established, the endpoints will sit in an in-active state sending connection maintenance frames, until either end decides to send data (the active state).

- In-active state: RTCP sender and receiver reports are sent.
- Active state:

  RTCP sender and receiver reports are sent.

  RTP voice frames are sent.

Disconnect

The trunk will remain up until such time as the port is shut down.

Data Transfer

Table 4-9 shows the multicast connection trunk traffic during inactive and active states between the routers with the configurations listed in Example 4-3. Because the routers are configured to use Protocol Independent Multicast (PIM) as their multicast routing protocol, we see PIM hello frames from each LMR gateway every 30 seconds. We also see the RTCP receiver reports generated from each gateway on average of every 5 seconds. Note that the source address of the RTCP frames is the IP address of that gateway's virtual interface plus one. When the lmr-3725c router begins audio transmission at frame 188, it simply starts streaming frames out to the configured multicast IP address and port number. The default codec on the dial peer is G.729, so the RTP frames are only 74 bytes long, including Ethernet header.

Table 4-9 Multicast Connection Trunk Frames

Frame	Time (sec)	Source	Destination	Protocol	Src Port	Dest Port	Length	Information
119	21.02002	10.40.0.2	10.40.0.1	RTP	19508	16454	214	Payload type=ITU-T G.711 PCMU, SSRC=287375362, Seq=6797, Time=105867, Mark
136	141.2141	10.50.0.2	224.0.0.13	PIMv2	—	—	72	Hello
137	141.5193	10.52.0.2	239.50.0.1	RTCP	22969	20001	166	Receiver Report
140	143.5913	10.52.0.2	239.50.0.1	RTCP	22969	20001	166	Receiver Report
143	145.787	10.50.0.1	224.0.0.13	PIMv2	—	—	72	Hello
145	146.8313	10.52.0.2	239.50.0.1	RTCP	22969	20001	166	Receiver Report

Table 4-9 Multicast Connection Trunk Frames (continued)

Frame	Time (sec)	Source	Destination	Protocol	Src Port	Dest Port	Length	Information
146	147.0996	10.52.0.6	239.50.0.1	RTCP	17005	20001	166	Receiver Report
171	167.801	10.52.0.2	239.50.0.1	RTCP	22969	20001	166	Receiver Report
175	170.4909	10.52.0.2	239.50.0.1	RTCP	22969	20001	166	Receiver Report
176	170.6267	10.50.0.2	224.0.0.13	PIMv2			72	Hello
178	172.3691	10.52.0.6	239.50.0.1	RTCP	17005	20001	166	Receiver Report
181	174.8909	10.52.0.2	239.50.0.1	RTCP	22969	20001	166	Receiver Report
182	175.1609	10.50.0.1	224.0.0.13	PIMv2			72	Hello
186	178.2789	10.52.0.6	239.50.0.1	RTCP	17005	20001	166	Receiver Report
188	179.4989	10.52.0.6	239.50.0.1	RTP	17004	20000	74	Payload type=ITU-T G.729, SSRC=268632070, Seq=5467, Time=213741899, Mark
189	179.5189	10.52.0.6	239.50.0.1	RTP	17004	20000	74	Payload type=ITU-T G.729, SSRC=268632070, Seq=5468, Time=213742059
190	179.5389	10.52.0.6	239.50.0.1	RTP	17004	20000	74	Payload type=ITU-T G.729, SSRC=268632070, Seq=5469, Time=213742219
191	179.5589	10.52.0.6	239.50.0.1	RTP	17004	20000	74	Payload type=ITU-T G.729, SSRC=268632070, Seq=5470, Time=213742379
192	179.5789	10.52.0.6	239.50.0.1	RTP	17004	20000	74	Payload type=ITU-T G.729, SSRC=268632070, Seq=5471, Time=213742539
193	179.5989	10.52.0.6	239.50.0.1	RTP	17004	20000	74	Payload type=ITU-T G.729, SSRC=268632070, Seq=5472, Time=213742699

Caveats

One of the main configuration mistakes made when configuring multicast connection trunks is forgetting to assign the appropriate voice class to the voice port in order to disable keepalive activity. In many cases, the global voice class gets created with the correct options, but it never gets assigned to the voice port. The result is that the voice port will enjoy two-way communication for about 15 seconds after it comes up, and then it will receive only audio. Using most of the display commands, the trunk will appear operational. However, if we look at the trunk signaling, it will show us that the trunk recognizes a lack of keepalives.

The following output shows the signaling and supervisory status of a multicast trunk with the voice class assigned to the voice port:

```
lmr-3725e# show voice trunk-conditioning signaling

2/0/0 :
hardware-state IDLE signal type is NorthamericanCAS
```

```
status : IDLE
forced playout pattern = 0x0
last-TX-ABCD=0000, last-RX-ABCD=0000
idle monitoring : tx
tx_idle = TRUE, rx_idle = FALSE, tx_oos = FALSE, lost_keepalive = FALSE
trunk_down_timer = 0, rx_ais_duration = 0, idle_timer = 0,tx_oos_timer = 0

lmr-3725e# show voice trunk-conditioning supervisory

SLOW SCAN, SCAN LMR
2/0/0 : state : TRUNK_SC_CONNECT, voice : off , signal : on ,master
        status: rcv IDLE, trunk connected
        sequence oos : idle-only
        pattern :rx_idle = 0000 tx_idle = 0000
        timing : idle = 0, restart = 0, standby = 0, timeout = 0
        supp_all = 0, supp_voice = 0, keep_alive = 0
        timer: oos_ais_timer = 0, timer = 0
        voice packet detection enable
```

Now look at the output for the same commands when the voice class is omitted from the voice port configuration. The first thing to notice are the words "lost keepalive" in bold in the status line for both commands. If your multicast trunk connection is not working and you see these words, then you need to check the configuration for your voice port and ensure that the voice class is properly configured for that port as in the configurations in Example 4-3.

```
lmr-3725e# show voice trunk-conditioning signaling

2/0/0 :
hardware-state IDLE signal type is NorthamericanCAS
status : lost keepalive, IDLE
forced playout pattern = 0x0
last-TX-ABCD=0000, last-RX-ABCD=0000
idle monitoring : tx
tx_idle = TRUE, rx_idle = FALSE, tx_oos = FALSE, lost_keepalive = TRUE
trunk_down_timer = 0, rx_ais_duration = 0, idle_timer = 0,tx_oos_timer = 0

lmr-3725e# show voice trunk-conditioning supervisory

SLOW SCAN, SCAN LMR
2/0/0 : state : TRUNK_SC_CONN_DEFAULT_IDLE, voice : off , signal : on ,master
        status: rcv IDLE, lost keepalive, trunk connected
        sequence oos : no-action
        pattern :tx_idle = 0000
        timing : idle = 0, restart = 0, standby = 0, timeout = 30
        supp_all = 0, supp_voice = 0, keep_alive = 5
        timer: oos_ais_timer = 93, timer = 93
        voice packet detection enable
```

B

bandwidth The difference between the highest and lowest frequencies available for network signals. The term also is used to describe the rated throughput capacity of a given network medium or protocol. The frequency range necessary to convey a signal measured in units of hertz (Hz). For example, voice signals typically require approximately 7 kHz of bandwidth and data traffic typically requires approximately 50 kHz of bandwidth.

C

CAS channel associated signaling. The transmission of signaling information within the voice channel. CAS signaling often is referred to as robbed-bit signaling because user bandwidth is being robbed by the network for other purposes.

channel 1. Communication path wide enough to permit a single RF transmission. Multiple channels can be multiplexed over a single cable in certain environments.

2. Specific frequency allocation and bandwidth. Downstream channels are used for television in the United States are 6 MHz wide.

codec coder-decoder.

1. Integrated circuit device that typically uses pulse code modulation to transform analog signals into a digital bit stream and digital signals back into analog signals.

2. In Voice over IP, Voice over Frame Relay, and Voice over ATM, a DSP software algorithm used to compress/decompress speech or audio signals.

D

dial peer Addressable call endpoint. In Voice over IP, there are two kinds of dial peers: POTS and VoIP.

DS0 digital service zero (0). Single timeslot on a DS1 (also known as T1) digital interface—that is, a 64-kbps, synchronous, full-duplex data channel, typically used for a single voice connection on a PBX.

E

E.164 ITU-T recommendation for international telecommunication numbering, especially in ISDN, BISDN, and SMDS. An evolution of standard telephone numbers.

F

frame Logical grouping of information sent as a data link layer unit over a transmission medium. Often refers to the header and the trailer, used for synchronization and error control, that surround the user data contained in the unit. The terms cell, datagram, message, packet, and segment also are used to describe logical information groupings at various layers of the OSI reference model and in various technology circles.

H

H.323 H.323 allows dissimilar communication devices to communicate with each other by using a standardized communication protocol. H.323 defines a common set of codecs, call setup and negotiating procedures, and basic data transport methods.

I

interoperability Capability of equipment manufactured by different vendors to communicate with one another successfully over a network.

IPSec IP Security. A framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses IKE to handle the negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

K

keepalive Message sent by one network device to inform another network device that the virtual circuit between the two is still active

M

multicast Single packets copied by the network and sent to a specific subset of network addresses. These addresses are specified in the Destination Address Field. Compare with unicast.

multicast address Single address that refers to multiple network devices. Synonymous with group address. Compare with broadcast address and unicast address. See also multicast

N

NAT Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space. Also known as Network Address Translator.

P

packet Logical grouping of information that includes a header containing control information and (usually) user data. Packets most often are used to refer to network layer units of data. The terms datagram, frame, message, and segment also are used to describe logical information groupings at various layers of the OSI reference model and in various technology circles.

PTC Positive Temperature Coefficient. A device that increases its internal resistance as it get hotter, thus limiting the current flow and additional heating.

Q

QoS quality of service. Measure of performance for a transmission system that reflects its transmission quality and service availability.

R

radio frequency (RF) Generally refers to wireless communications with frequencies below 300 GHz.

repeater Device that regenerates and propagates electrical signals between two network segments.

RTP Real-Time Transport Protocol. Commonly used with IP networks. RTP is designed to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services. RTP provides such services as payload type identification, sequence numbering, timestamping, and delivery monitoring to real-time applications.

RTCP RTP Control Protocol. Protocol that monitors the QoS of an IPv6 RTP connection and conveys information about the on-going session.

T

TCP Transmission Control Protocol. Connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.

trunk 1. Physical and logical connection between two switches across which network traffic travels. A backbone is composed of a number of trunks.

2. In telephony, a phone line between two COs or between a CO and a PBX.

U

unicast Message sent to a single network destination. Compare with multicast.

V

VAD voice activity detection. When enabled on a voice port or a dial peer, silence is not transmitted over the network, only audible speech. When VAD is enabled, the sound quality is slightly degraded but the connection monopolizes much less bandwidth.

VoIP Voice over IP. The capability to carry normal telephony-style voice over an IP-based internet with POTS-like functionality, reliability, and voice quality. VoIP enables a router to carry voice traffic (for example, telephone calls and faxes) over an IP network. In VoIP, the DSP segments the voice signal into frames, which then are coupled in groups of two and stored in voice packets. These voice packets are transported using IP in compliance with ITU-T specification H.323.

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V