



## **Solution Reference Network Design (SRND) for Cisco IPICS Release 4.10(2)**

November 10, 2017

**Cisco Systems, Inc.**  
[www.cisco.com](http://www.cisco.com)

Cisco has more than 200 offices worldwide.  
Addresses, phone numbers, and fax numbers  
are listed on the Cisco website at  
[www.cisco.com/go/offices](http://www.cisco.com/go/offices).

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2017 Cisco Systems, Inc. All rights reserved.



<b>Preface</b>	<b>ix</b>
Overview	ix
Organization	ix
Related Documentation	x
Obtaining Documentation, Obtaining Support, and Security Guidelines	x

---

## CHAPTER 1

<b>Introducing Cisco IPICS</b>	<b>1-1</b>
Cisco IPICS Benefits	1-1
Cisco IPICS Components	1-2

---

## CHAPTER 2

<b>Cisco IPICS Component Considerations</b>	<b>2-1</b>
Unified Media Service	2-1
UMS Overview	2-2
When is a UMS Required?	2-3
UMS Instances for Locations	2-3
UMS Scaling	2-3
UMS Resource Allocation	2-4
Remote Users	2-4
UMS Audio Mixing	2-4
Router Media Service	2-5
RMS Overview	2-5
RMS Components for Locations	2-6
When is an RMS Required?	2-10
Allocation of RMS DS0 Resources	2-12
Media Resource Allocation for the Dial Engine	2-15
Virtual Talk Groups	2-15
Cisco IPICS Endpoint Scenarios—Multicast	2-16
VTG Types	2-16
Cisco IPICS Endpoint Scenarios—Multicast	2-16
Cisco IPICS Endpoint Scenarios—Unicast	2-23
Integrating Cisco IPICS with SIP Providers	2-24
Requirements for SIP Sessions	2-24

Default Dial Peer Scenarios	2-25
Cisco IPICS Integration with LDAP	2-29
Cisco Instant Connect for Android Devices	2-29
DNS Configuration	2-30
Point-to-Point Calls	2-31
Using Cisco Jabber with Cisco Instant Connect for Android Devices	2-31
Wireless Network Configurations	2-31
Wireless Controller Configuration Example	2-32
Cisco Unified IP Phones	2-34
Cisco Unified Communications Manager Configuration Overview	2-35
Cisco Unified Communications Manager Express Configuration Overview	2-35
Notification	2-36
Email Notification Action	2-36
IP Phone Text Notification Action	2-36
Dial Notification Action	2-38
Talk Group Notification Action	2-38
Trust Management	2-38
IDC Coexistence with Cisco Safety And Security Desktop	2-39
Port Usage	2-39
Guidelines for Using IP Multicast Addresses with Cisco IPICS	2-41
QOS Policy Considerations	2-41

---

**CHAPTER 3**

<b>Cisco IPICS LMR Gateway Configurations</b>	<b>3-1</b>
Interfacing the Cisco IPICS LMR Gateway with Land Mobile Radios	3-2
Cabling	3-2
Analog E&M Interface	3-4
Analog E&M signaling Types	3-4
Cisco IOS LMR Gateway Configurations	3-7
Determining Correct Cisco IOS Radio Control	3-7
Required Baseline LMR Gateway Configuration	3-8
VAD Operated Signaling Configuration	3-9
COR/COS Operated Signaling Configuration	3-11
DSP Channel Optimization and Allocation	3-12
Important Considerations When Deploying Cisco IPICS with Tone Controlled Radios	3-12
Configuration Examples for Manual Tone Control Operated Signaling Scenarios	3-40
Pooled Radios	3-52
Configuring and Allocating Pooled Resources	3-53

Pooled Resource Allocation	3-53
Determining How many Pooled Radios to Configure	3-54
Optimizing Priorities for Trunked Networks and Wide Area Systems	3-54
Serial Radio Control	3-54
Setting up and Configuring Serial Control for EF Johnson Radios	3-55
Setting up and Configuring Serial Control for Sprint Nextel (iDEN) Handsets	3-59
Trunked Radio Optional Workaround	3-64
Trunked Radio Feedback Tones	3-64
Trunked Radio Hybrid Configuration	3-65
Analog Tap Recording Configuration	3-68
Recording Multicast LMR Traffic	3-69
Recording Tap Cisco IOS Configuration	3-69
Cisco IPICS Integration with ISSI Gateways	3-70
Cisco IPICS Integration with DFSI Gateways	3-71
Feature Support for Radios	3-71

---

**CHAPTER 4**

<b>Cisco IPICS Infrastructure Considerations</b>	<b>4-1</b>
WAN Considerations	4-1
Multicast Routing	4-2
Bandwidth Planning	4-4
Codecs	4-4
cRTP, Variable-Payload Sizes and Aggressive VAD	4-6
Mixing Voice Streams	4-8
Quality of Service	4-8
QoS Overview	4-8
Cisco IOS Queuing Techniques	4-9
QoS for a LAN	4-10
QoS at the WAN Edge	4-11
Policing	4-11
Queuing	4-11
Trust Boundaries	4-12
VPN in Deployment Scenarios	4-14
Securing the Cisco IPICS Infrastructure	4-14
Secure Socket Layer	4-15
Firewalls and Access Control Lists	4-15
Other Security Recommendations	4-15
Cisco IPICS Network Management System	4-15
Managing the Overall Network	4-16

---

CHAPTER 5

**Understanding Dial Peers 5-1**

- Dial Peer Call Legs 5-1
- Inbound and Outbound Dial Peers 5-2
- Destination Pattern 5-3
- Session Target 5-3
- Configuring Dial Peers for Call Legs 5-3
- Matching Inbound and Outbound Dial Peers 5-3

---

CHAPTER 6

**Cisco IPICS Licensing and Sizing Guidelines 6-1**

- Resource and License Usage 6-1
- UMS Usage 6-1
- Additional Planning and Sizing Guidelines 6-2
- Dial Port Licensing Details 6-2

---

CHAPTER 7

**Cisco IPICS Deployment Models 7-1**

- Single Site Model 7-1
  - Benefits of the Single Site Model 7-2
  - Best Practices for the Single Site Model 7-2
- Multiple Site Model 7-2
  - MPLS with Multicast VPNs 7-3
  - Multicast Islands 7-10
  - VPN Termination for Mobile Clients 7-15

---

GLOSSARY

---

INDEX



## Preface

---

## Overview

This *Solution Reference Network Design (SRND)* document provides design considerations and guidelines for deploying Cisco IPICS release 4.10(2). This document should be used with the related documentation that the “[Related Documentation](#)” section on [page x](#) describes.

For other design documents, go to this URL:

<http://www.cisco.com/go/srnd>

## Organization

This manual is organized as follows:

<a href="#">Chapter 1, “Introducing Cisco IPICS”</a>	Describes the advantages and benefits that Cisco IPICS offers and introduces the primary components that make up a Cisco IPICS deployment
<a href="#">Chapter 2, “Cisco IPICS Component Considerations”</a>	Provides information about various Cisco IPICS components
<a href="#">Chapter 3, “Cisco IPICS LMR Gateway Configurations”</a>	Describes configurations needed to use land mobile radios with Cisco IPICS
<a href="#">Chapter 4, “Cisco IPICS Infrastructure Considerations”</a>	Provides information about network infrastructure considerations that you must be aware of when you deploy Cisco IPICS
<a href="#">Chapter 5, “Understanding Dial Peers”</a>	Provides an overview of dial peers, which will help you understand how Cisco IPICS operates
<a href="#">Chapter 6, “Cisco IPICS Licensing and Sizing Guidelines”</a>	Explains how Cisco IPICS uses licensable features and provides information about resource use and system sizing
<a href="#">Chapter 7, “Cisco IPICS Deployment Models”</a>	Describes the deployment models for Cisco IPICS

## Related Documentation

To access the documentation suite for Cisco IPICS, go to the following URL:

[http://www.cisco.com/en/US/products/ps7026/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps7026/tsd_products_support_series_home.html)

Cisco also provides a wide variety of documentation that provides related information about Cisco IPICS components and the configuration of an infrastructure that supports Cisco IPICS. References to related documentation is provided throughout this manual as appropriate.

## Obtaining Documentation, Obtaining Support, and Security Guidelines

For information about obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*. This document also lists new and revised Cisco technical documentation. It is available at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.





# Introducing Cisco IPICS

---

Cisco IP Interoperability and Collaboration System (Cisco IPICS) is a platform that enables users to bring their own devices into the world of push-to-talk (PTT) communications in Cisco Unified Communications (UC) environments. Cisco IPICS bridges the worlds of land mobile radio (LMR) and UC, providing the ability for communication between disparate devices such as traditional and digital radio, Android, and Apple iOS devices.

This chapter provides an overview of Cisco IPICS. It describes the advantages and benefits that Cisco IPICS offers to various organizations. It also introduces the primary components of a Cisco IPICS deployment.

This chapter includes these topics:

- [Cisco IPICS Benefits, page 1-1](#)
- [Cisco IPICS Components, page 1-2](#)

## Cisco IPICS Benefits

On-premises PTT is an important requirement in many markets, including the following segments:

- Enterprise (operations, safety and security)
- Commercial
- Retail
- Education
- Healthcare
- Government
- Service provider

Organizations in these market segments typically deploy several wired networks and wireless networks to achieve their business and service goals. However, such disparate solutions often do not support interoperability and collaboration, which can affect operational efficiency and customer satisfaction.

Examples of such disparate networks include:

- Legacy push-to-talk (PTT) radio networks (analog or digital at different frequencies) that are used for voice communications within groups. Communication is usually restricted within a specified group or network because of radio frequency (RF) limitations and proprietary protocols.

- Traditional hoot bridges that are connected over time-division multiplexing (TDM) circuits. These deployments cannot provide audit trails and they do not seamlessly integrate with other PTT or Voice over IP (VoIP) networks. In addition, they do not offer the mobility and serviceability that an IP deployment provides.
- VoIP networks that are used to carry packetized voice on wired or wireless IP phones or on other IP clients. These clients do not interact with the PTT services.

For organizations that use disparate networks, Cisco IPICS provides the following benefits:

- Easy-to-use installation, management, and operational features—Enables a migration path to more robust IP applications, devices, and IP-based solutions to achieve greater operational efficiencies.
- Effective solution—Streamlines operations, and command and control while protecting investments in deployed radio networks or legacy hoot bridges and applications.
- Efficient deployment—Leverages current IP infrastructure with minimal upgrades required, decreasing total cost of ownership.
- Resiliency—Eliminates communications silos and single points of failure.

## Cisco IPICS Components

A Cisco IPICS deployment involves several hardware and software components to enable true interoperability and collaboration. Components include the Cisco IPICS server, Cisco Unified Media Service (UMS) server, Cisco IOS and gateways, and LDAP integration. Deployments may also employ integration with devices such as call center turrets, digital radio gateways, messaging gateways, Private Mobile Broadband technologies, and others.

Figure 1-1 illustrates the major components of a Cisco IPICS deployment.

*Figure 1-1 Cisco IPICS Components*

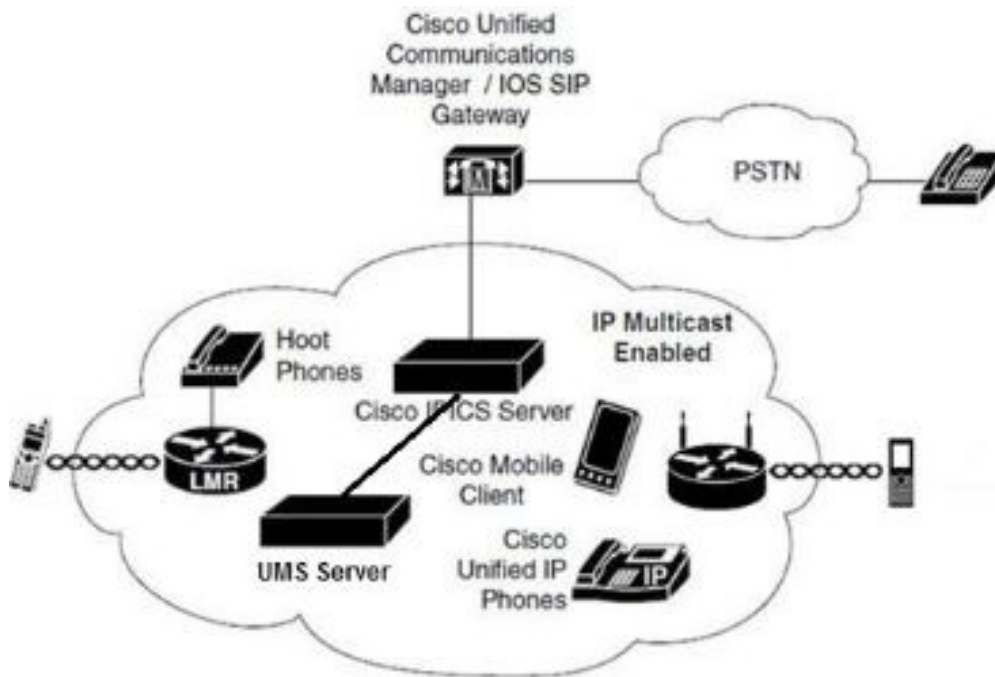


Table 1-1 provides an overview of major Cisco IPICS components. Other chapters in this manual provide more detailed information about using and configuring several of these components. In addition, Cisco provides a wide variety of technical and user documentation that explains in detail Cisco components that are used in the deployment of Cisco IPICS. These documents include information about installing, configuring, operating, managing, maintaining, and troubleshooting components.

For version and compatibility information, see *Cisco IPICS Compatibility Matrix*.

**Table 1-1** Cisco IPICS Component Overview

Component	Description
Cisco IPICS server	<p>Provides the core functionality of the Cisco IPICS system. The Cisco IPICS server software runs on the Cisco Linux operating system (based on Red Hat Linux) on selected Cisco Unified Computing System (UCS) platforms and performs these functions:</p> <ul style="list-style-type: none"> <li>• Hosts the Cisco IPICS Administration Console, an administration GUI that enables dynamic resource management for users, channels, and virtual talk groups (VTGs).</li> <li>• Provides Cisco IPICS authentication and security services</li> <li>• Stores configuration and operational data</li> <li>• Enables integration with various media resources, such as UMS components, Cisco Unified IP Phones, Cisco Unified Communications Manager, and Cisco IOS SIP gateways</li> </ul>
Router media service (RMS)	<p>Provide media stream mixing by looping back DS0 resources on one or more pairs of T1 or E1 interfaces that are connected back to back with a T1 loopback cable. The RMS provides capabilities that include the following:</p> <ul style="list-style-type: none"> <li>• Functions that are required to combine two or more channels.</li> <li>• Multicast channel mixing, using the Cisco Hoot 'n' Holler feature, to support virtual talk groups (VTGs).</li> <li>• PVDM resources are required for DSP resources.</li> <li>• The addition of a single DS0 loopback pair to the RMS when one or more dial-in users or mobile client users joins a channel or VTG</li> </ul>
Unified Media Service (UMS)	<p>Enables media services and provides these capabilities:</p> <ul style="list-style-type: none"> <li>• Functions that are required to combine two or more channels or VTGs.</li> <li>• Multicast channel mixing, using the Cisco Hoot 'n' Holler feature, to support VTGs</li> <li>• PTT media convergence for multicast, unicast, TDM, and SIP endpoints</li> </ul>
Cisco IPICS Dispatch Console (IDC)	<p>A graphical-based application that installs and runs on a client PC and allows Cisco IPICS users to communicate with other users via radio, telephone, mobile device, or PC. Also lets users participate in VTGs and incidents, manage and operate a variety of resource such as channels, radios, incidents, and VTGs, and perform a variety of other activities.</p>
Cisco Instant Connect for Android Devices	<p>Application that allow users of Android devices to use mobile clients and Windows machines to interact with other participants in a Cisco IPICS talkline and perform a variety of other activities.</p>

Table 1-1 Cisco IPICS Component Overview

Component	Description
Cisco Instant Connect for Microsoft Windows	Allows Microsoft Windows users to participate in talklines and mobile clients activities on Microsoft Windows machines.
Cisco IPICS ISSI Gateway (ISSIG)	An ISSI Gateway allows multiple RF subsystems (RFSSs) to be connected together into wide area networks that extends area coverage for P25 compliant digital radios
Cisco Digital Fixed Station Interface Gateway (DFSIG)	Serves as a gateway between Cisco IPICS and P25 DFSI capable fixed stations (FS). It is a proxy for all non-P25 clients within Cisco IPICS and is responsible for transcoding between multicast RTP streams (G.711) and SIP based P25 CAI frames (IMBE codec for digital communications and PCM for analog communications). It also is responsible for encryption and decryption the audio stream when necessary.
Cisco Instant Connect MIDlet	<p>An application for certain Cisco Unified Wireless IP Phone models that lets you communicate with other Cisco IPICS users via a point-to-point or standard telephone call, and communicate via channels, VTGs, and incidents by using the IP phone as a PTT device.</p> <p>For a list of Cisco Unified Wireless IP Phone models and minimum firmware version that support the Cisco Instant Connect MIDlet, see <i>Cisco IPICS Compatibility Matrix</i>.</p> <p>For detailed information about installing and using the MIDlet, see <i>Cisco Instant Connect MIDlet Reference Guide</i>.</p>
Unified media service (UMS)	<p>Enables media services and provides these capabilities:</p> <ul style="list-style-type: none"> <li>Provides the functions that are required to combine two or more VTGs.</li> <li>Multicast channel mixing, using the Cisco Hoot ‘n’ Holler feature, to support VTGs.</li> <li>Enables PTT media convergence for multicast, unicast, TDM, and SIP endpoints.</li> </ul>
SIP provider	Handles calls to and from the Cisco IPICS policy engine.
LMR gateway	<p>LMR gateways provide voice interoperability between radio and non-radio networks by bridging radio channels and talk groups to IP multicast streams.</p> <p>The LMR gateway functionality is available in certain versions of Cisco IOS software.</p>
Networking components	Include switches, routers, firewalls, mobile access routers, and wireless access points and bridges.
Cisco Unified IP Phone	Cisco IPICS integrates selected models of the Cisco Unified IP Phone. Users of these phones can select a channel from a list of channels on which to participate when Cisco IPICS is configured as a phone service for Cisco Unified Communications Manager or for Cisco Unified Communications Manager Express when it is bundled with supported versions of Cisco IOS software.



## Cisco IPICS Component Considerations

---

This chapter provides information about various components and features that can be part of a Cisco IPICS solution. This information will help you to understand how these items interoperate in a Cisco IPICS deployment.

This chapter includes these topics:

- [Unified Media Service, page 2-1](#)
- [Router Media Service, page 2-5](#)
- [Media Resource Allocation for the Dial Engine, page 2-15](#)
- [Virtual Talk Groups, page 2-15](#)
- [Integrating Cisco IPICS with SIP Providers, page 2-24](#)
- [Cisco IPICS Integration with LDAP, page 2-29](#)
- [Cisco Instant Connect for Android Devices, page 2-29](#)
- [Wireless Network Configurations, page 2-31](#)
- [Cisco Unified IP Phones, page 2-34](#)
- [Notification, page 2-36](#)
- [Trust Management, page 2-38](#)
- [IDC Coexistence with Cisco Safety And Security Desktop, page 2-39](#)
- [Port Usage, page 2-39](#)

### Unified Media Service

A Cisco IPICS deployment includes or more Cisco Unified Computing System (UCS) components that host virtual instances of the Unified Media Service (UMS).

For information about UMS system requirements and capacity, see *Cisco IPICS Compatibility Matrix*.

For information about the ports and transport protocols that the UMS uses, see [Table 2-4 on page 2-39](#).

The following sections provide additional information about the UMS:

- [UMS Overview, page 2-2](#)
- [When is a UMS Required?, page 2-3](#)
- [UMS Instances for Locations, page 2-3](#)
- [UMS Scaling, page 2-3](#)

- [UMS Resource Allocation, page 2-4](#)
- [Remote Users, page 2-4](#)
- [UMS Audio Mixing, page 2-4](#)

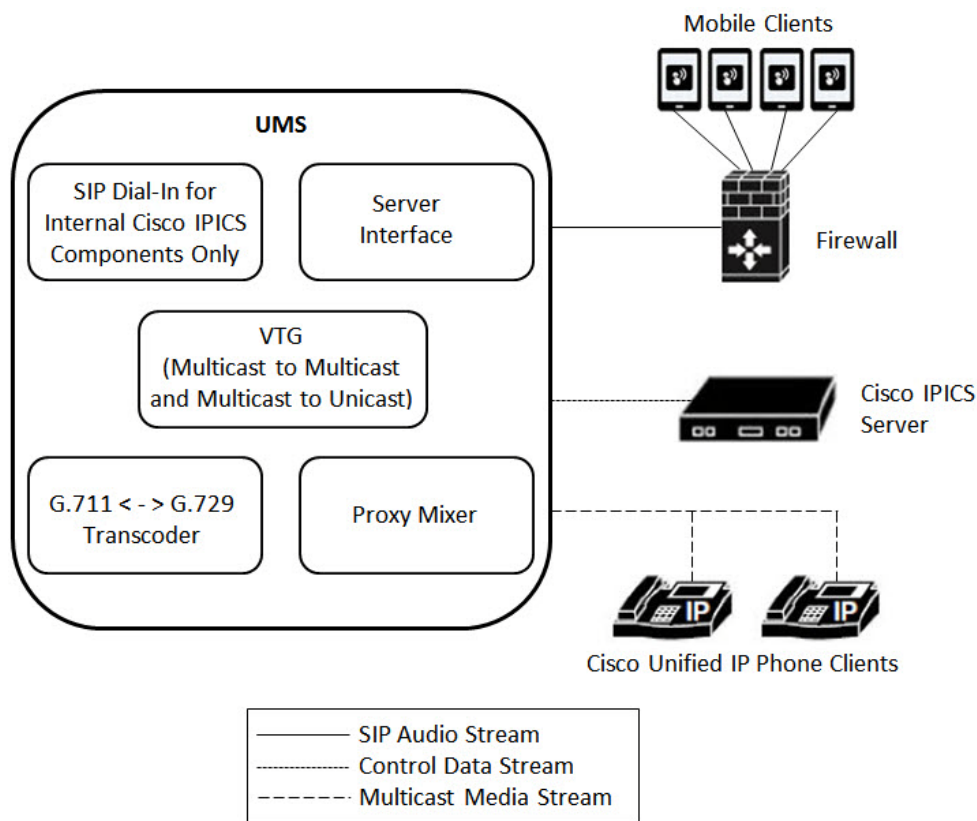
## UMS Overview

The UMS is a highly available, software-based media engine that performs several core functions in a Cisco IPICS deployment including:

- Media transcoding between G.711 and G.729 media streams
- Media stream mixing and floor control
- Talker ID for P25 and SIP based endpoints
- SIP termination
- SIP to multicast, SIP to SIP, multicast to SIP, and multicast to multicast media connectivity
- Floor control for mobile clients and Cisco Unified IP Phone clients

Figure 2-1 illustrates the use of a UMS in a Cisco IPICS deployment.

*Figure 2-1 UMS in a Cisco IPICS Deployment*



## When is a UMS Required?

A UMS is required for any Cisco IPICS deployment in which unicast and multicast endpoints are joined or channels are combined.

Examples include:

- Using VTGs
- Using Cisco IPICS incidents
- Having dial-in users
- Dial-in users joining VTGs or channels
- Having a Land Mobile Radio (LMR) connected to a multicast channel the communicates with a Cisco IPICS SIP client via a unicast channel

## UMS Instances for Locations

Cisco IPICS relies upon the concept of resource *locations* to effectively manage network traffic. A location is a multicast enabled domain within a network. A domain can comprise multiple geographic locations. Some networks may be fully multicast enabled across the entire network while others may not route multicast traffic beyond a geographic boundary or a single subnet. Cisco IPICS considers each separate multicast domain to be a different location. Any resources (channels, radios, endpoints, and so on) that are not in the same multicast domain as the Cisco IPICS server are considered to be in the *Remote* location.

A UMS is assigned to a location when it is configured. All IPICS servers and components that are in the same multicast domain should be assigned to the same location. While a single IPICS server can administer UMS resources in multiple locations, multicast media is confined to its originating location. Media can move between locations via a Multicast–Unicast–Multicast (MUM) trunk configured on a T1 or E1 loopback or via a GRE tunnel. Only baseband audio data is carried across the MUM trunk; talker ID, control data and supplemental services are not distributed between locations.

The following guidelines apply to locations:

- A channel is associated to a location
- A VTG is a global resource and can be used to span a channel to another channel in another location
- Cisco Mobile Client users are always considered to be remote

## UMS Scaling

Each instance of the UMS supports up to 100 simultaneous audio streams. A Cisco IPICS deployment can be scaled to support many hundreds of users by adding UMS resources. The number of UMS resources that are required is based on sum of the streams. Cisco The IPICS server maintains a list of available UMSs and locations and distributes media streams on a round-robin basis.

Clients consume resources differently; the UMS sends one audio stream to a registered mobile client regardless of how many channels are displayed on the client. When deploying Cisco IPICS to support more than 1,000 simultaneous audio streams, server and media streams must be distributed across multiple physical servers. Additional virtual cores and memory may be required for optimized performance. Consult your Cisco representative for assistance with large scale installations.

## UMS Resource Allocation

UMS resources are dynamically allocated in the following situations:

- Activating or deactivating a VTG—When a VTG is activated by a Cisco IPICS user or triggered by a Cisco IPICS policy, one UMS resource is allocated for each channel in the VTG. The UMS resource is released when the user deactivates the VTG
- Activating or changing an incident—An incident is a special case of a VTG in which media other than voice can be associated with an event. Each channel or VTG in an incident consumes one UMS resource.
- Authenticating a mobile client—Mobile clients connect to Cisco IPICS via a SIP session between the client and the UMS, which consumes one UMS resource.
- Authenticating a Cisco video surveillance IP camera—Cisco video surveillance cameras that run the SIP client create a SIP session between the camera and the UMS, which consumes one UMS resource.
- A dial-in user joining a channel or VTG—Each Channel or VTG that the Cisco IPICS dial engine accesses consumes one UMS resource. (This UMS resource can service multiple users simultaneously.)

## Remote Users

A Cisco IPICS mobile client user is, by definition, a remote user. A remote user accesses Cisco IPICS through a SIP-based (unicast) connection and obtains a media connection to the Cisco IPICS server. When the user joins a channel or VTG, Cisco IPICS configures a resource on the UMS to enable a multicast connection from the UMS to the user.

This multicast connection is made one time for a channel or VTG, regardless of the number of users who select the channel or VTG. When the last remote user disconnects from the channel or VTG, the resource is released in the UMS and becomes available.

When a remote user obtains a media connection on the Cisco IPICS server, the UMS sends and receives multicast streams as follows:

1. After the user selects a resource, Cisco IPICS allocates a UMS resource for the user and allocates a multicast address from the multicast pool. Cisco IPICS then performs an IGMP join operation on the multicast address so that when additional users select the same resource, the Cisco IPICS server can continue to use same the multicast address.
2. When the user begins to talk, Cisco IPICS transmits the audio to the multicast address of the selected resources.
3. When the UMS receives the multicast packets, it forwards the packets to the multicast address that has been allocated from the multicast pool. Cisco IPICS receives that multicast audio stream and forwards it as a unicast stream to all remote users who have selected that resource.

## UMS Audio Mixing

With the Cisco IPICS talk priority feature, when a higher priority user transmits from and IDC while a lower priority user is transmitting, the system stops streaming (preempts) the lower priority call in a unicast environment. If two users with same priority transmit, the first user to transmit receives precedence. Talk priority values can be 1 (highest talk priority) through 7 (lowest talk priority).



For example, assume that User 1 and User 2 are transmitting on a channel. If User 1 has a talk priority of 5 and User 2 has a talk priority of 1, the audio streams of User 2 receive precedence.

## Router Media Service

The Cisco IPICS solution uses one or more of the supported Cisco IOS routers to provide the router media service (RMS) functionality.

The following sections provide additional information about the RMS:

- [RMS Overview, page 2-5](#)
- [RMS Components for Locations, page 2-6](#)
- [When is an RMS Required?, page 2-10](#)
- [Allocation of RMS DS0 Resources, page 2-12](#)

For detailed information about configuring an RMS for Cisco IPICS, see the “Configuring the Cisco IPICS RMS Component” appendix in *Cisco IPICS Server Administration Guide* for this release.

For a list of Cisco IOS releases that Cisco IPICS supports for use as an RMS, see *Cisco IPICS Compatibility Matrix*. Each supported Cisco IOS release includes the Cisco Hoot ‘n’ Holler feature.

## RMS Overview

The primary role of the RMS is to provide media stream mixing by looping back DS0 resources. When an RMS is installed, it must have one or more pairs of T1 or E1 interfaces that are connected back to back with a T1 loopback cable. These loopback interface pairs are manually configured in the RMS by adding the DS0-Group to timeslot mapping. (For related information, see the “Configuring the Cisco IPICS RMS Component” appendix in *Cisco IPICS Server Administration Guide* for this release.) When you use the Cisco IPICS Administration Console to add an RMS, the loopback pairs become available for assignment. A properly configured RMS will make a list of DS0 loopback channels available for dynamic allocation by the Cisco IPICS server.

The RMS can be installed as a stand-alone component (RMS router) or as an additional feature that is installed in the LMR gateway.

The Cisco IPICS server dynamically allocates a DS0 loopback pair (two DS0 channels) in the following scenarios:

- Successful Authentication of an IPICS Dispatch Console (IDC) from the remote location—When a remote IDC connection is started, the IDC authenticates to the Cisco IPICS server. The Cisco IPICS server then configures the RMS to allocate a DS0 loopback pair for each channel or virtual talk group (VTG) that is assigned to the IDC user. The IDC retrieves configuration information that contains the IP address of the RMS and the channel details with the Plain Old Telephone Service (POTS) dial-peer information that the Cisco IPICS server configured in the RMS. Then, when the IDC user activates a channel or VTG, the IDC places a SIP call to the POTS dial-peer in the RMS and connects to that channel or VTG.
- Activation or change of a VTG—When a Cisco IPICS dispatcher performs VTG operations that affects an RMS, the Cisco IPICS server updates the RMS as needed. For example, if a VTG with two channels is activated, the Cisco IPICS server configures two DS0 loopback pairs, one for each channel. This configuration will include assigning each side of corresponding voice-port for the allocated DS0 loopback pair to a connection trunk.

- A dial-in user joins a channel or VTG—A single DS0 loopback pair is added per channel or VTG regardless of the number of dial-in users who join the channel or VTG.
- A mobile client user log in to the Cisco IPICS server—A single DS0 loopback pair is used for each incident.

## RMS Components for Locations

An RMS supports one Cisco IPICS *location*, which is defined as a multicast domain. If a Cisco IPICS deployment requires RMS functionality in more than one location, there must be an RMS configured for each of those locations. The multicast address pool contains a list of multicast addresses and their respective port assignments. The addresses in the pool are allocated, as needed, by the Cisco IPICS server when it configures an RMS. The Cisco IPICS server keeps track of the in-use and the available addresses.

The multicast address pool is a global resource that is shared across all RMS components that are configured in that Cisco IPICS server. Therefore the network configuration must be able to support all of the configured addresses in all of the configured RMS components. The IPICS server attempts to load balance across all RMS components that are in the same location. For this reason, it is important that you configure each RMS according to the instructions that are documented in the “Configuring the Cisco IPICS RMS Component” appendix in *Cisco IPICS Server Administration Guide* for this release if you have more than one RMS configured in the server.

The following information applies to locations:

- A channel is associated to a location.
- A VTG is a global resource that can span multiple locations.
- A user may be assigned channels from multiple locations, but when the user authenticates, the user must select the desired location. Channel resources are allocated based on the selected location.

## Multiple Location Example

As an example of how Cisco IPICS and RMS components function in multiple locations, consider the following scenario:

- User A is in the Site 1 location and is assigned the Emergency VTG
- User B is in the Site 2 location and is assigned the Emergency VTG
- Channel EMT1 is in the Site 1 location
- Channel EMT2 is in the Site 2 location
- The Emergency VTG is assigned both channel EMT1 and channel EMT2
- RMS 1 is in the Site 1 location
- RMS 2 is in the Site 2 location

When the Cisco IPICS dispatcher activates the Emergency VTG, the Cisco IPICS server assigns to the VTG a multicast address from the multicast address pool. It also configures DS0 loopback resources in RMS 1 and RMS 2.

In this way, users in both locations can communicate by using the VTG. Be aware that this scenario requires that there must be multicast connectivity between both locations. If both locations are isolated multicast domains, there must be a way to route the multicast traffic between locations. For related information, see the [“Multiple Site Model” section on page 7-2](#).

## RMS Configuration Example

The following example shows what the Cisco IPICS server configures in the RMS when a VTG that contains two channels is activated. This example allows the RMS to receive voice on the Police channel and to transmit it to the VTG multicast address, and to receive voice on the VTG multicast address and to transmit it to the Police channel. In this example,

- The VTG is named Combined and its multicast IP address is 239.192.21.79:21000. (This address is dynamically allocated for the VTG from the address range that is configured in the multicast pool.)
- The IP address for the Police channel is 239.192.21.64:21000.
- The IP address for the Fire channel is 239.192.21.65:21000.
- One side of the DS0 loopback, 0/2/0:3, is assigned a connection trunk (90929093) that maps to a VoIP dial peer destination pattern. This dial peer has a session target of 239.192.21.79:21000 (the VTG multicast address).
- The other side of the DS0 loopback, 0/2/1:3, is assigned a connection trunk (90929193) that maps to a VoIP dial peer destination pattern. This dial peer has a session target of 239.192.21.64:21000 (the Police channel multicast address).

The following Cisco IOS configuration output shows the RMS configuration in the Cisco IPICS server to support adding the Police channel to the Combined VTG:

```
dial-peer voice 90929093 voip
description #0/2/0:3#1164200525742# INUSE 284
destination-pattern 90929093
voice-class permanent 1
session protocol multicast
session target ipv4:239.192.21.79:21000
codec g711ulaw
no vad
```

```
voice-port 0/2/0:3
voice-class permanent 1
auto-cut-through
lmr m-lead audio-gate-in
lmr e-lead voice
no echo-cancel enable
playout-delay maximum 100
no comfort-noise
timeouts call-disconnect 3
timeouts teardown lmr infinity
timing hookflash-in 0
timing hangover 80
connection trunk 90929093
description #0/2/0:3#1164200525742# INUSE 284
```

```
voice-port 0/2/1:3
voice-class permanent 1
auto-cut-through
lmr m-lead audio-gate-in
lmr e-lead voice
no echo-cancel enable
playout-delay maximum 100
no comfort-noise
timeouts call-disconnect 3
timeouts teardown lmr infinity
timing hookflash-in 0
timing hangover 80
connection trunk 90929193
description #0/2/1:3#1164200525742# INUSE 284
```

```
dial-peer voice 90929193 voip
description #0/2/1:3#1164200525742# INUSE 284
destination-pattern 90929193
voice-class permanent 1
session protocol multicast
session target ipv4:239.192.21.64:21000
codec g711ulaw
```

The following Cisco IOS configuration output shows the RMS configuration in the Cisco IPICS server to support adding the Fire channel to the Combined VTG:

```
dial-peer voice 90929094 voip
description #0/2/0:4#1164200525776# INUSE 285
destination-pattern 90929094
voice-class permanent 1
session protocol multicast
session target ipv4:239.192.21.79:21000
codec g711ulaw
no vad
```

```
voice-port 0/2/0:4
voice-class permanent 1
auto-cut-through
lmr m-lead audio-gate-in
lmr e-lead voice
no echo-cancel enable
playout-delay maximum 100
no comfort-noise
timeouts call-disconnect 3
timeouts teardown lmr infinity
timing hookflash-in 0
timing hangover 80
connection trunk 90929094
description #0/2/0:4#1164200525776# INUSE 285
```

```
voice-port 0/2/1:4
voice-class permanent 1
auto-cut-through
lmr m-lead audio-gate-in
lmr e-lead voice
no echo-cancel enable
playout-delay maximum 100
no comfort-noise
timeouts call-disconnect 3
timeouts teardown lmr infinity
timing hookflash-in 0
timing hangover 80
connection trunk 90929194
description #0/2/1:4#1164200525776# INUSE 285
```

```
dial-peer voice 90929194 voip
description #0/2/1:4#1164200525776# INUSE 285
destination-pattern 90929194
voice-class permanent 1
session protocol multicast
session target ipv4:239.192.21.65:21000
codec g711ulaw
no vad
```

The following Cisco IOS configuration outputs shows the RMS configuration in the Cisco IPICS server to support an IDC user who is assigned both the Police and Fire channels connecting by using the remote location. This configuration allows the IDC to communicate with RMS by using a unicast connection.

The RMS forwards the unicast stream, which is received from the IDC, through a DS0 loopback to the multicast address. Packets that the RMS receives for a multicast address are forwarded through a DS0 loopback to the receiving IDC device as a unicast stream.

This Cisco IOS configuration output pertains to the Police channel:

```
dial-peer voice 909290914 voip
description #0/2/0:14#1164659525783# INUSE 295
destination-pattern 909290914
voice-class permanent 1
session protocol multicast
session target ipv4:239.192.21.64:21000
codec g711ulaw
no vad

voice-port 0/2/0:14
voice-class permanent 1
auto-cut-through
lmr m-lead audio-gate-in
lmr e-lead voice
no echo-cancel enable
playout-delay maximum 100
no comfort-noise
timeouts call-disconnect 3
timeouts teardown lmr infinity
timing hookflash-in 0
timing hangover 80
connection trunk 909290914

voice-port 0/2/1:14
voice-class permanent 1
auto-cut-through
lmr m-lead audio-gate-in
lmr e-lead voice
no echo-cancel enable
playout-delay maximum 100
no comfort-noise
timeouts call-disconnect 3
timeouts teardown lmr infinity
timing hookflash-in 0
timing hangover 80
description #0/2/1:14#1164659525783# INUSE 295

dial-peer voice 909291914 pots
description #0/2/1:14#1164659525783# INUSE 295
destination-pattern 1990000275909291914
port 0/2/1:14
```

This Cisco IOS configuration output pertains to the Fire channel:

```
dial-peer voice 909290915 voip
description #0/2/0:15#1164659525833# INUSE 296
destination-pattern 909290915
voice-class permanent 1
session protocol multicast
session target ipv4:239.192.21.65:21000
codec g711ulaw
no vad

voice-port 0/2/0:15
voice-class permanent 1
auto-cut-through
lmr m-lead audio-gate-in
lmr e-lead voice
```

```

no echo-cancel enable
playout-delay maximum 100
no comfort-noise
timeouts call-disconnect 3
timeouts teardown lmr infinity
timing hookflash-in 0
timing hangover 80
connection trunk 909290915
description #0/2/0:15#1164659525833# INUSE 296

voice-port 0/2/1:15
voice-class permanent 1
auto-cut-through
lmr m-lead audio-gate-in
lmr e-lead voice
no echo-cancel enable
playout-delay maximum 100
no comfort-noise
timeouts call-disconnect 3
timeouts teardown lmr infinity
timing hookflash-in 0
timing hangover 80
description #0/2/1:15#1164659525833# INUSE 296

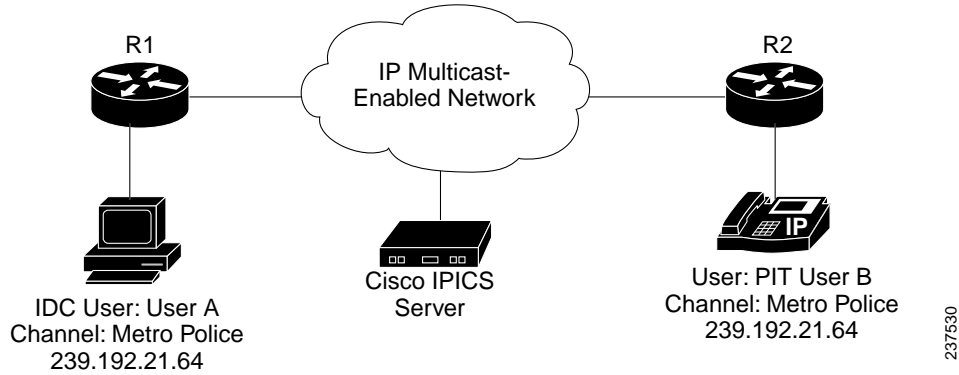
dial-peer voice 909291915 pots
description #0/2/1:15#1164659525833# INUSE 296
destination-pattern 1990000275909291915
port 0/2/1:15

```

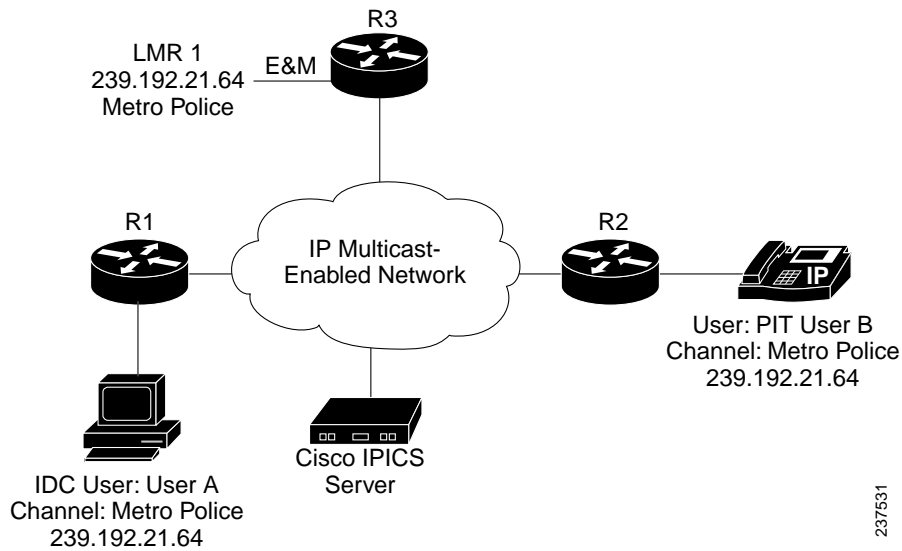
## When is an RMS Required?

Cisco IPICS requires an RMS to establish connectivity between unicast and multicast endpoints (such as remote IDC to channel, mobile client to Cisco IPICS server, remote IDC to VTG, and dial-in user to channel or VTG), and to establish connectivity between multicast endpoints that are on different channels (such as channel to VTG, and VTG to VTG).

However, there are some communication scenarios that do not require RMS DS0 resources. For example, two multicast users can communicate on a single Cisco IPICS channel without consuming RMS DS0 resources, as illustrated in [Figure 2-2](#). This examples shows that, after the users log in to the Cisco IPICS server, they receive their channel information, Metro Police using the multicast group 239.192.21.64. If the users activate the Metro Police channel, they will be able to communicate without using RMS DS0 resources.

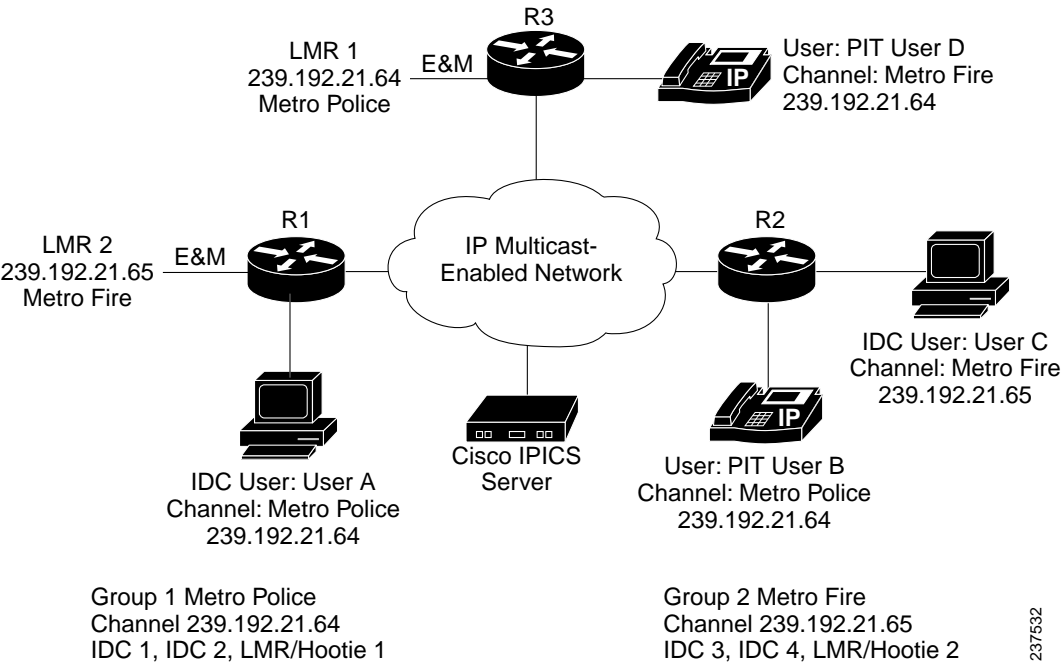
**Figure 2-2** *Single Cisco IPICS Channel*

Adding an LMR gateway and an LMR user to this scenario does not necessarily require RMS DS0 resources. If the LMR user is statically configured to use the same channel as the other users, all users can communicate without consuming RMS DS0 resources, as shown in [Figure 2-3](#).

**Figure 2-3** *Single Cisco IPICS Channel with LMR Gateway*

As another example, a scenario with two sets of users on two separate channels does not consume RMS DS0 resources if communication between the channels is not required. In the scenario shown in [Figure 2-4](#), Metro Police users can communicate with each other, and Metro Fire users can communicate with each other, without consuming RMS DS0 resources. In this scenario, no RMS resources are required because there is no communication between Metro Police and Metro Fire users.

Figure 2-4 Several Cisco IPICS Channels



## Allocation of RMS DS0 Resources

You can create a VTG that allows only specific users to communicate by using that VTG. In this case, the VTG does not include channels and it does not use RMS DS0 resources (unless there are IDC users who connect by using the Remote location), but it does use a multicast address from the multicast pool.

If a VTG needs to include LMR endpoints, each of the LMR channels must be added to the VTG, in addition to the channels for the IDC or phone users. If a user is not added to the VTG but has a channel that is in the VTG, the user will still be able to send to and receive from the VTG.

After an IDC successfully authenticates by using the Remote location, the RMS allocates a DS0 pair to each channel or VTG that is assigned to that authenticated IDC user.

Table 2-1 illustrates the various scenarios in which RMS resources are allocated

Table 2-1 RMS Resource Allocation

Scenario	Multicast Address from the Multicast Address Pool	RMS DS0 Pair
Active VTG with channel	Yes	1 per channel in the VTG
Channel not in VTG	No	No
VTG with users only	Yes	No
Remote IDC	No	1 per assigned channel or VTG
Mobile client	No	1 per assigned incident

For detailed information about RMS DS0 requirements, see *Cisco IPICS Compatibility Matrix*.



## DSP Channel Optimization and Allocation

Follow these recommendations for optimizing DS0 channels and DSP channels:

- So that digital signal processors (DSPs) can be shared, first enable dspfarm, and make sure that all modules are participating in the network clock.
- When you enable dspfarm, you add specific voice cards to the DSP resource pool. This configuration allows several interface cards to share the installed DSP resources. (DSPs can be shared among digital modules or ports (such as T1/E1) and the motherboard, but DSPs cannot be shared among analog ports (such as an FXS)).
- At a minimum, you should enable one dspfarm.
- After the dspfarm is enabled on all modules that have DSPs installed, and all modules are participating in the main network clock, Cisco IOS interacts with these DSPs as part of the DSP resource pool.

To help calculate the DSPs that you need for your configuration, see *High-Density Packet Voice Digital Signal Processor Modules*, which is available at the following URL:

[http://www.cisco.com/en/US/products/hw/modules/ps3115/products\\_qanda\\_item0900aecd8016c6ad.shtml](http://www.cisco.com/en/US/products/hw/modules/ps3115/products_qanda_item0900aecd8016c6ad.shtml)

For detailed information about configuring DSP farms, see the “Configuring the Cisco IPICS RMS Component” appendix in *Cisco IPICS Server Administration Guide* for this release.

## Examples of Hardware Configuration and Supported Voice Streams

This section provides examples of various hardware configurations and the number of voice streams that can be supported for use with Cisco IPICS.

When you use the Cisco 2811 with one T1/E1 Multiflex Trunk Voice/WAN Interface (VWIC-2MFT-T1/E1) card installed on the motherboard, up to 24 pairs of DS0 channels are available for use if the card is configured for T1 mode. If the card is configured for E1 mode, up to 30 DS0 channels are available. The number of supported voice streams varies based on the configuration that you use. For example, with one 64-channel high-density Packet Voice/Fax DSP Module (PVDM2-64) installed, support is provided for up to 32 pairs of voice streams when using the G.711 u-law codec. If you use the G.729 u-law codec, the PVDM2-64 provides support for 16 pairs of voice streams. In this situation, one PVDM2-64 does not support full utilization of all pairs of DS0 channels on a T1 line.

The following options are also available for use with the Cisco 2811:

- Three VWIC-2MFT-T1/E1 interface cards installed on the motherboard with two PVDM2-64 modules, for a total of 128 channels.
- One T1/E1 High Density Digital Voice Network Module (NM-HDV2-2T1/E1) that is fully populated with four PVDM2-64 modules, for a total of 256 channels, and two VWIC-MFT-T1/E1 interface cards.



### Note

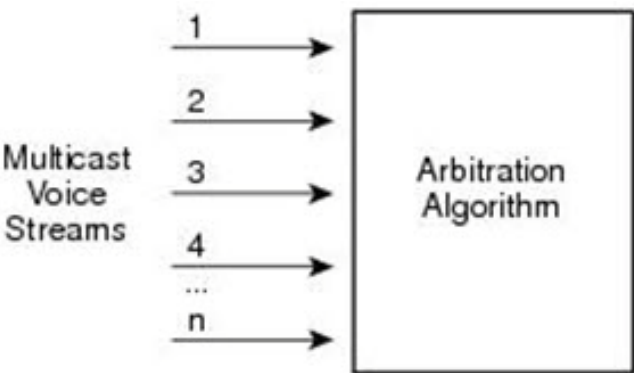
Before you order router hardware for your Cisco IPICS deployment, Cisco recommends that you determine the number of DS0 channels that you need and your DSP requirements, based on the interface modules and codec configurations that you use, to ensure full support for your deployment. For example, if you configure the T1/E1 cards for E1 connectivity, support is provided for 150 pairs of DS0 channels and 384 DSP resources. Based on the codec that you use, this DSP resource can provide support for 96 G.729 voice streams or 150 G.711 voice streams.

For more information about Cisco interfaces and modules, go to the following URL:

[http://www.cisco.com/en/US/products/hw/modules/prod\\_module\\_category\\_home.html](http://www.cisco.com/en/US/products/hw/modules/prod_module_category_home.html)

In the Cisco Hoot `n' Holler over IP implementation, all participants in a VTG can speak simultaneously. However, when voice packets from various sources arrive at the UMS, the arbitration algorithm selects only the three most active voice streams and mixes them. If other voice streams are present, the UMS drops the longest talker by using a round-robin arbitration algorithm. See [Figure 2-5](#).

Figure 2-5 Mixing Voice Streams



[Table 2-2](#) shows an example of how mixing works in a VTG that has four active users on a channel.

Table 2-2 Mixing Example

Event	Remarks
User A starts speaking.	1 user speaking.
User B and User C join User A.	3 users speaking simultaneously. Cisco arbitration engine at the UMS receives 3 voice streams.
User D starts speaking while the other 3 users continue speaking.	Cisco arbitration engine at the UMS receives 4 voice streams. The algorithm can present up to 3 voice streams. It drops the voice stream from the longest talker, User A, and adds User D to the streams that it presents. The voice streams are now from User B, User C, and User D.
After 2 seconds, all 4 users are still speaking.	The current longest talker, User B, is dropped, and User A is added. Voice streams are now User C, User D, and User A.
After 2 seconds, all 4 users are still speaking.	The current longest talker, User C, is dropped, and User A is added. Voice streams are now User D, User A, and User B.
All users continue speaking.	The round-robin process of dropping the current longest talker and adding the other user every 2 seconds continues.

# Media Resource Allocation for the Dial Engine

When a user dials in to the Cisco IPICS dial engine, the user accesses the system through a SIP-based (unicast) connection and obtains a media connection to the Cisco IPICS Dial Management server (DMS). When the user joins a channel or VTG, Cisco IPICS configures a resource on the UMS to enable a multicast connection from the server to the dial engine. This configuration facilitates a multicast connection between the Cisco IPICS server and the selected channel or VTG.

This multicast connection is made one time for a channel or VTG, regardless of the number of dial-in users who select the channel or VTG. When the last dial-in user disconnects from the channel or VTG, the resource is released in the UMS and becomes available for use.

When a dial-in user makes a unicast media connection to the media driver on a Cisco IPICS server, the policy engine sends and receives multicast streams as follows:

1. After the dial-in user successfully authenticates and selects a resource, Cisco IPICS allocates a UMS resource for the user and allocates a multicast address from the multicast pool. Cisco IPICS then performs an Internet Group Management Protocol (IGMP) join operation on the multicast address so that when additional dial-in users select the same resource, the Cisco IPICS server can continue to use same the multicast address.
2. When the dial-in user presses 1 on a telephone and begins to talk, Cisco IPICS transmits the audio to the multicast address of the selected resources.
3. When the UMS receives the multicast packets, it forwards the packets to the multicast address that has been allocated from the multicast pool. Cisco IPICS receives that multicast audio stream and forwards it as a unicast stream to all dial-in users who have selected that resource.

## Virtual Talk Groups

A VTG enables participants on various channels to communicate by using a single multicast address. A VTG contains, in a temporary channel, any combination of the following members:

- Channels
- Channel groups
- Users
- User groups
- Incidents

A Cisco IPICS administrator creates Cisco IPICS channels and assigns a multicast address to each one. The administrator also creates VTGs as needed. When an administrator creates a VTG, the Cisco IPICS server automatically allocates to the VTG an available address from the multicast pool. So while VTGs are dynamically assigned addresses from the multicast pool, channels are configured as static addresses that are outside the range of the addresses that are used by VTGs.

A VTG allows communication between endpoints that are assigned different multicast addresses, such as two endpoints that have activated different channels. When a VTG is enabled to facilitate communications between two or more endpoints with different multicast addresses, a UMS must bridge, or mix, the multicast streams of each channel. In this VTG scenario, the Cisco IPICS sever allocates a loopback voice port for each channel in the VTG.

For example, assume that a Cisco IPICS administrator creates a VTG named Combined and that this VTG includes the Security channel and Facilities channel as members. Also assume that each LMR voice port is statically configured with a multicast address, so that LMR Security users always send to the

## VTG Types

In addition to a normal VTG, Cisco IPICS supports Broadcast VTGs, Incident VTGs, Patch VTGs, and Scan VTGs.

Table 2-1 provides information about how transmit and receive functionality works with these VTG types.

Table 2-1 Transmit and Receive Functionality for VTG Types

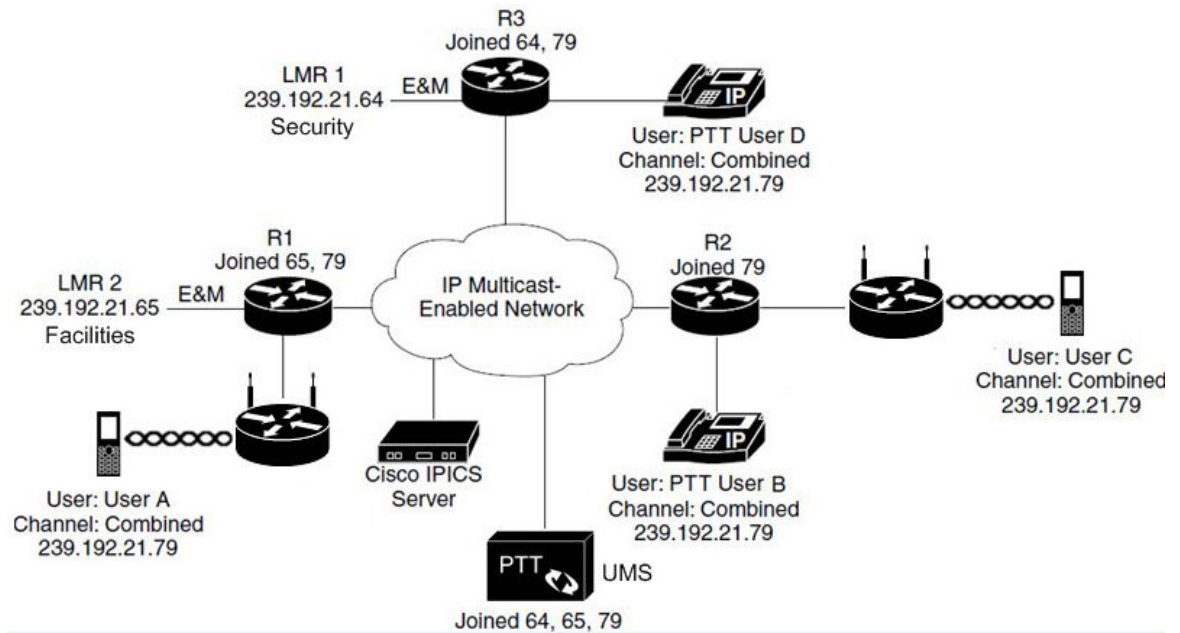
	Broadcast VTG	Incident VTG	Patch VTG	Scan VTG
Transmit	A mechanism by which a privileged user can broadcast an announcement to a set of users.	A group of channels in which, in addition to audio, images and video can be transmitted to participants.	Allows patching of multicast enabled channels. Audio is transmitted to all channels that are part of VTG.	Allows monitoring the communication of participants and communication with a selected participant.
Receive	<p>Users can hear an announcement while continuing to communicate on their respective channels.</p> <p>Media flows from the VTG multicast group to all participating channels and radios. Media does not flow from participating channels and radios to the VTG multicast group.</p>	Receive image and video files in addition to audio.	Audio is received by participants in each channel that is part of the VTG.	<p>You have the option to select the PTT button for the VTG and transmit audio to the channel where audio was last received, or to manually transmit audio on a selected channel by pressing the individual channel PTT button.</p> <p>Media flows from the VTG participant channels to the VTG multicast group. Media flows from the VTG multicast group to only one participating channel or radio. The destination channel or radio is determined by the client in the PTT request.</p>

## Cisco IPICS Endpoint Scenarios—Multicast

When a Cisco IPICS dispatcher activates the Combined VTG (as shown in Figure 2-6), Cisco IPICS configures the UMS to mix the Security, Facilities, and Combined VTG channels. Users who have been added to the VTG will see the new Combined VTG channel on their mobile or desktop clients or Cisco Unified IP Phones. LMR endpoints do not have associated users. An LMR channel is statically configured, so an LMR user can send and receive only from the Cisco IPICS channel that is configured with the same multicast address as the LMR channel. An LMR user can communicate only with endpoints that are not using the same channel if the channel of the LMR user is in a VTG with other channels or users.

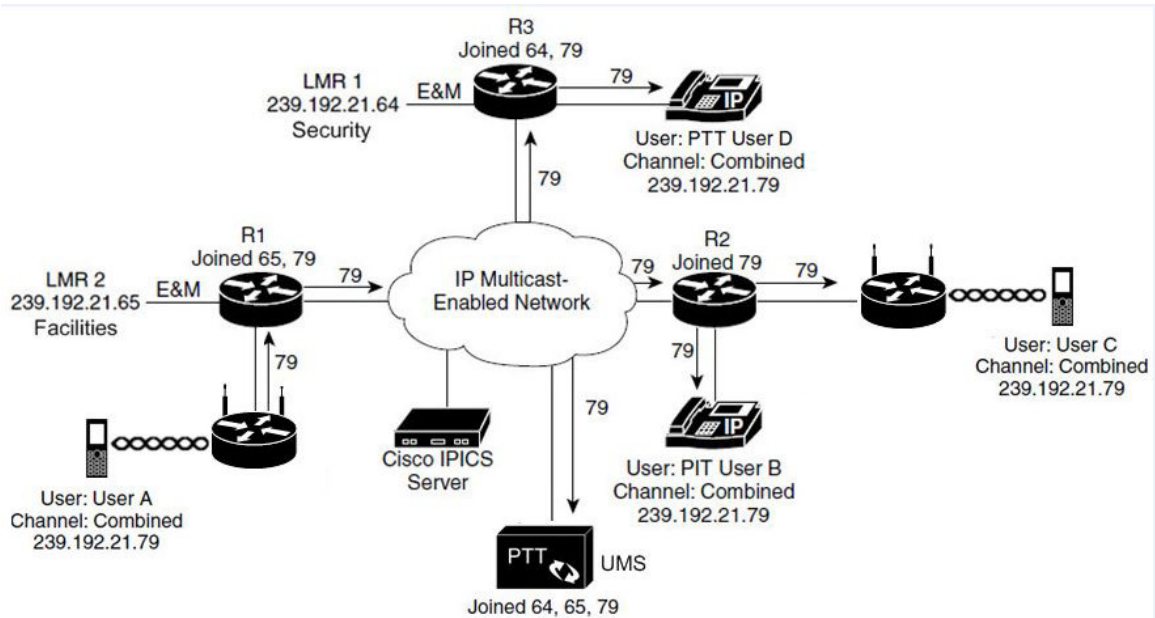
Figure 2-7 illustrates a scenario in which four users have deactivated their Security or Facilities channels and have activated the Combined VTG channel.

Figure 2-1 Multicast Group Membership

**Figure 2-7 Multicast Group Membership**

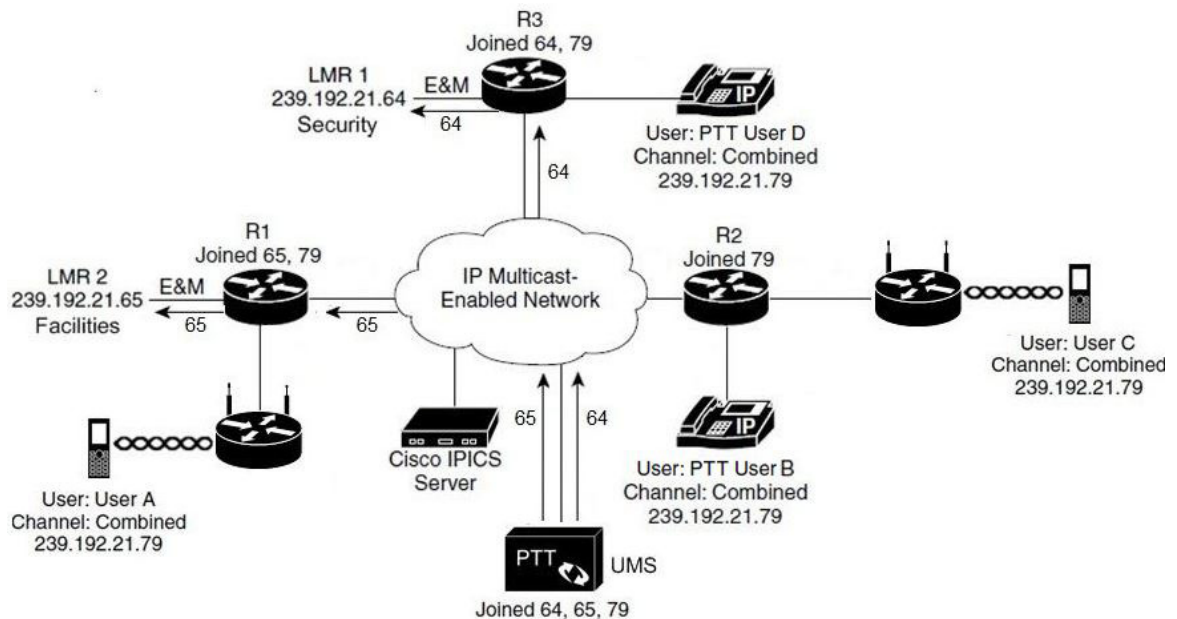
When a user deactivates the Security and Facilities channels and activates the Combined VTG channel, the endpoint sends an Internet Group Management Protocol (IGMP) leave message for the Security and Facilities channels and an IGMP join message for the Combined VTG channel. The LMR voice port channels are statically configured and the virtual interface (VIF) in the router will have already joined the configured multicast group. As shown in [Figure 2-8](#), when user A transmits, the system sends the multicast packets via the multicast distribution tree to each endpoint that has joined the combined group, and to the UMS, which mixes the audio and sends it to the channels in the VTG.

Figure 2-8 Transmitting to the VTG Channel



When the UMS receives the traffic over the Combined VTG channel, it mixes this channel with the Security and Facilities channels and forwards the mixed stream to the LMR endpoints, as shown in Figure 2-9.

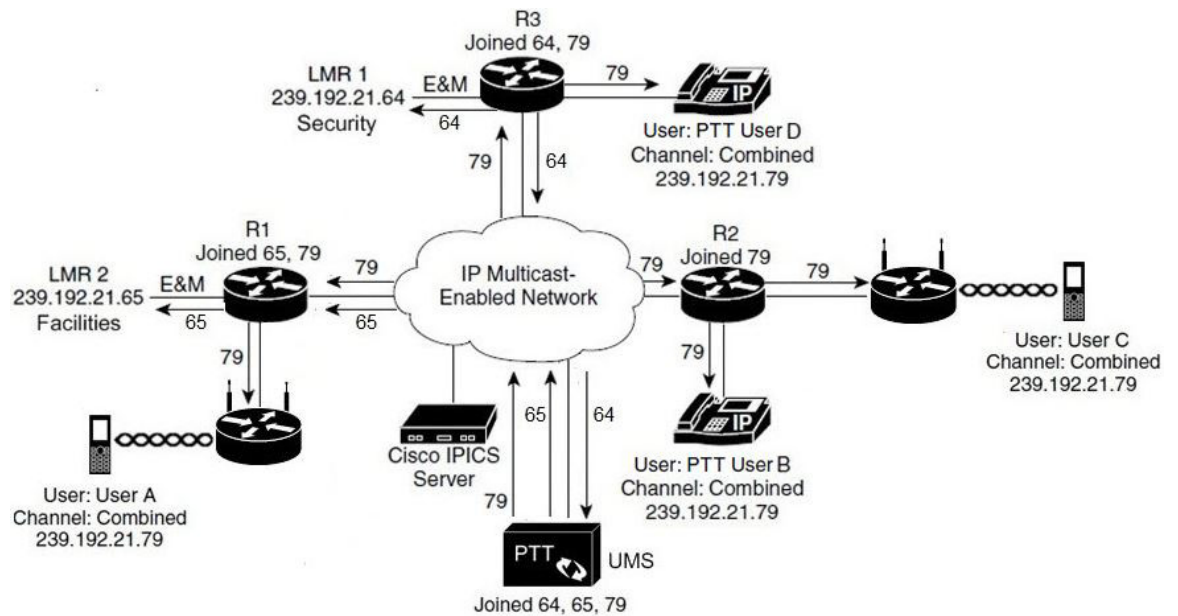
Figure 2-9 Transmitting VTG Channel to Security and Facilities Channels



When the LMR Facilities user transmits, the only other endpoint that has joined this multicast channel is the UMS. The multicast distribution tree forwards the multicast voice traffic to the UMS, where it is mixed with the Facilities channel and the Combined VTG channel and then forwarded to the other

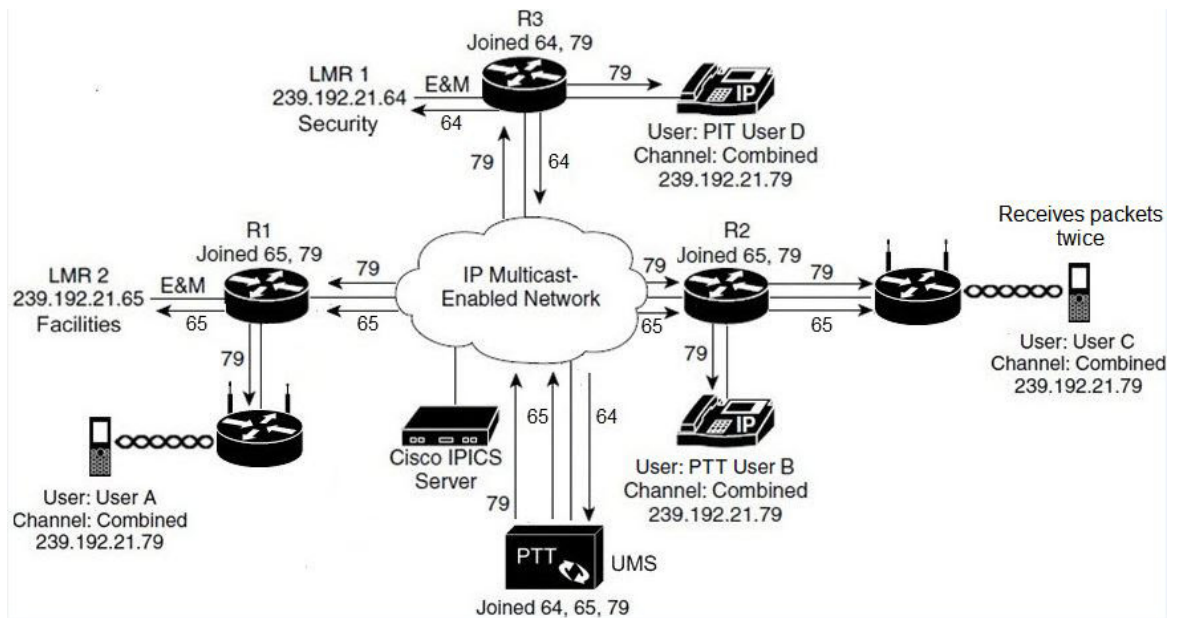
endpoints in the VTG. See [Figure 2-10](#).

**Figure 2-10** LMR Multicast Traffic Flow



[Figure 2-11](#) shows User C with two active channels: the Facilities channel and the Combined VTG channel.

**Figure 2-11** Traffic Flow with Two Active Channels

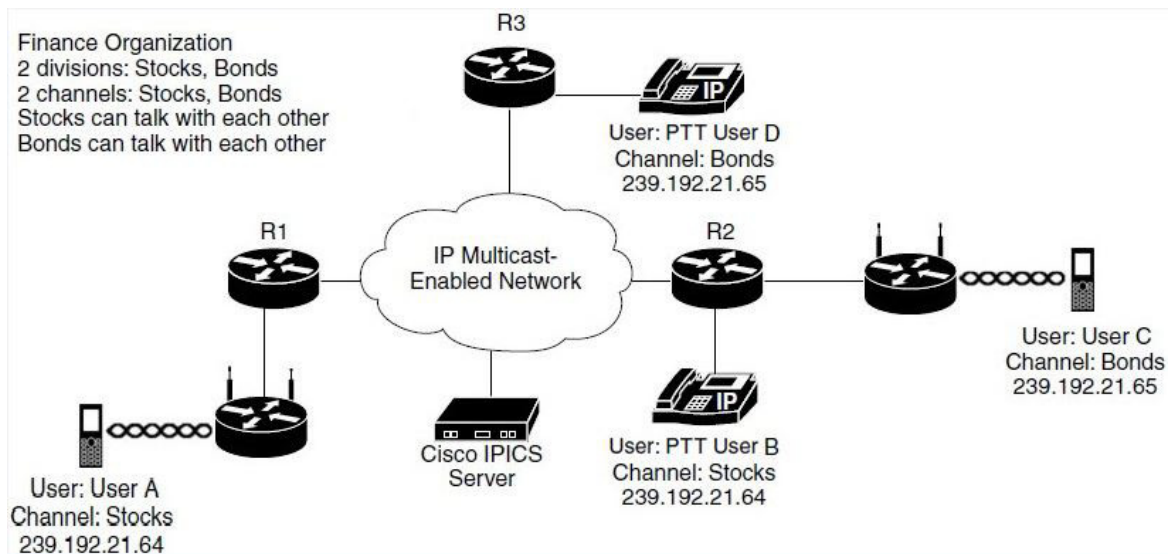




Because User C activated two channels (Facilities and the Combined VTG), two multicast groups are joined through IGMP. As a result, when an endpoint in the Combined VTG transmits, User C will receive the transmitted packets twice. (In this case, the duplicate packets can cause audio quality issues. Take care to avoid this scenario.)

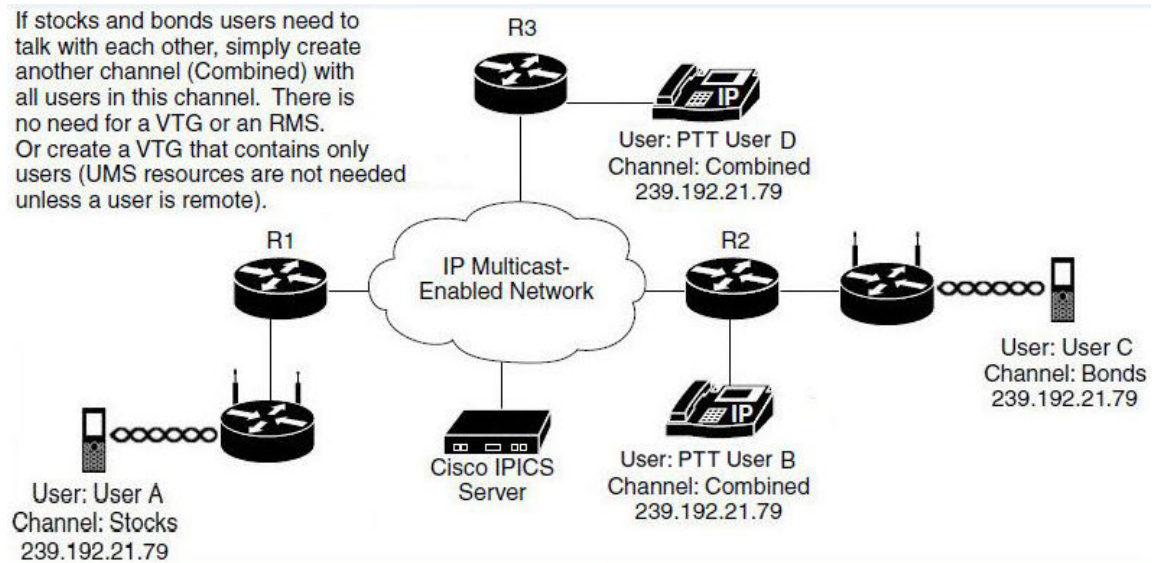
If there are no LMR endpoints in a VTG, UMS resources may not be required for the VTG. For example, consider a financial institution with one Cisco IPICS channel called Stocks and one channel called Bonds. The users who are associated with the Stocks channel can communicate with each other, and the users who are associated with the Bonds channel can communicate with each other. [Figure 2-12](#) illustrates this scenario.

**Figure 2-12** Cisco IPICS Scenario with no LMR Endpoints



If a VTG is created that contains users but no channels, UMS resources are not required. The only resource that is required in this case is a multicast channel from the multicast pool. UMS resources are not needed because Cisco Unified IP Phone users, unlike LMR users, are not statically configured for one channel. If users only are placed in the VTG, users will see the VTG on their Cisco Unified IP Phones. When the VTG activates, these endpoints will simply join the VTG multicast channel that is allocated by the Cisco IPICS server. See [Figure 2-13](#).



**Figure 2-13** VTG with Users Only

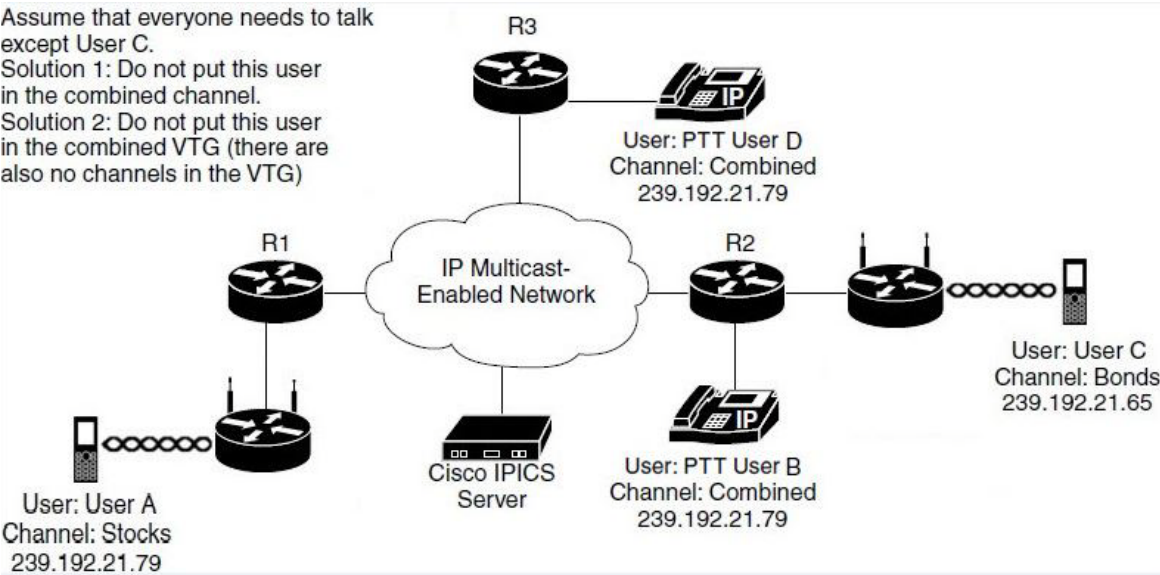
You can also avoid consuming UMS resources by creating a new channel and associating all users with that channel, instead of creating a VTG. In this example shown in [Figure 2-13](#), there is a channel called Combined. Users will see two channels on their Cisco Unified IP Phones: the Combined VTG channel, and either the Stocks channel or the Bonds channel.

If you do not want a user (for example, User C) to participate in such a combined VTG channel, you can take either of these actions:

- Create a channel (you could name it Combined) and associate with it all users except User C
- Create a combined VTG with all users except User C

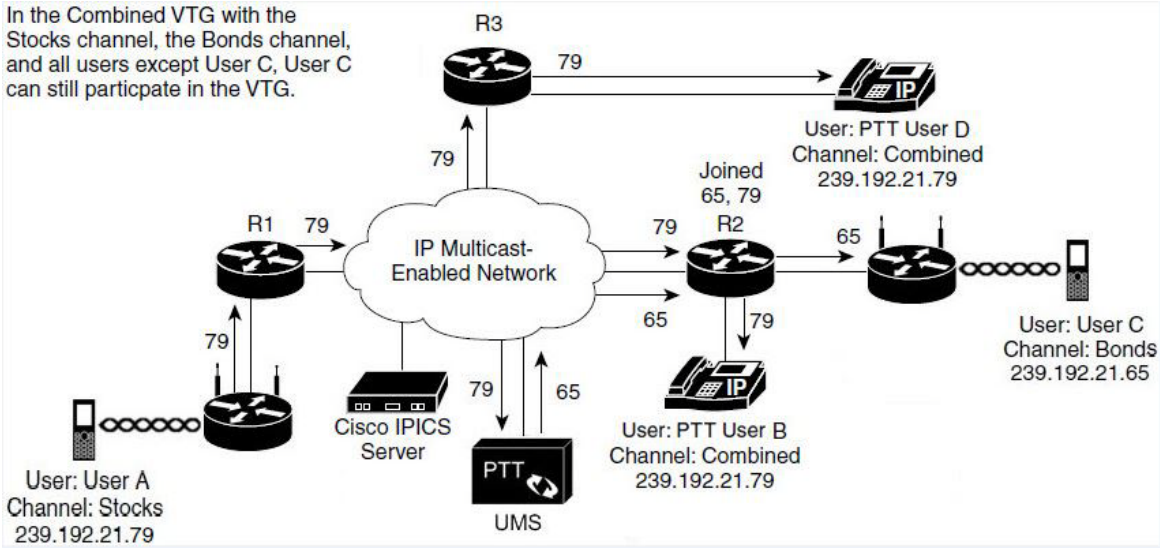
See [Figure 2-14](#) for an illustration of this scenario.

Figure 2-14 Restricting VTG Access



If you create a VTG that includes the Stocks channel, the Bonds channel, and all users except User C, all of the users except User C will see the Combined VTG channel on their Cisco Unified IP Phones. However, because the Stocks channel and the Bonds channel are in the VTG, User C will be able to receive from and transmit to the VTG. See [Figure 2-15](#).

Figure 2-15 Combined VTG with a User Omitted



## Cisco IPICS Endpoint Scenarios—Unicast

Figure 2-16 Unicast Connection Set Up

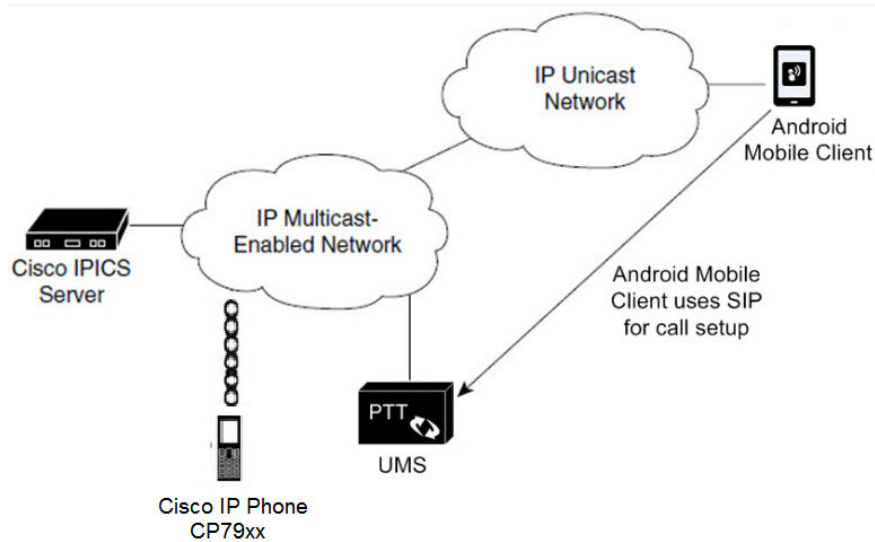
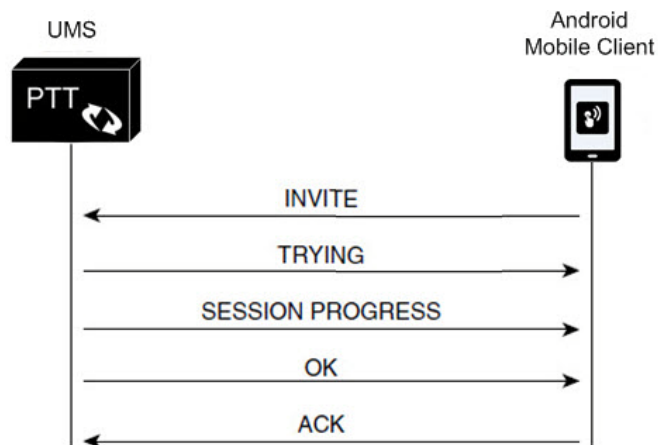
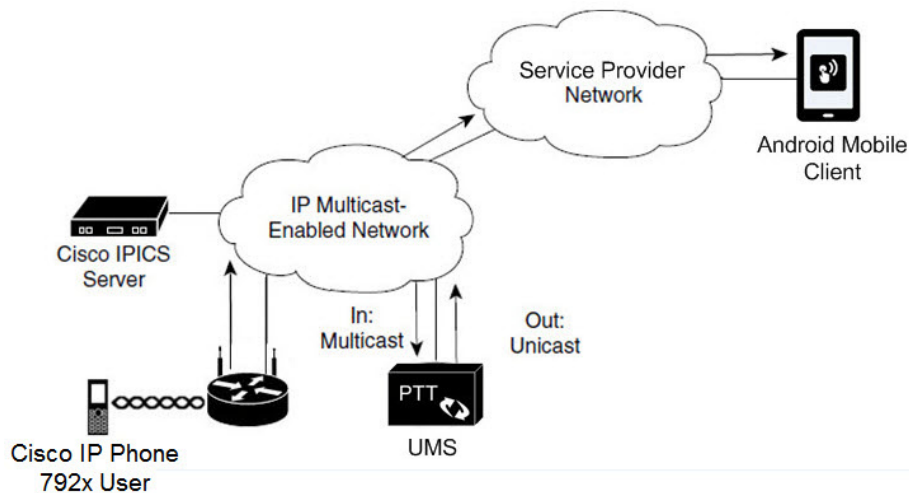


Figure 2-17 SIP Signaling Flow



**Figure 2-18 Multicast to Unicast Call Flow**

## Integrating Cisco IPICS with SIP Providers

The Cisco IPICS dial engine requires a SIP provider to place or receive calls. See *Cisco IPICS Compatibility Matrix* for a list of supported SIP providers (Cisco Unified Communications Manager or Cisco Unified Communications Manager Express with a router running a supported Cisco IOS release).

All calls to or from the Cisco IPICS dial engine go through the configured SIP provider

Because a Cisco IPICS deployment can vary depending on the call flow, it is important to understand how a call flow works so that you can properly configure supporting components. *Cisco IPICS Server Administration* provides instructions for configuring the UMS and the Cisco IOS SIP gateway and SIP provider. The way in which a SIP provider is deployed in a network and the dial plan at your site dictate how components are configured.

The following sections describe how Cisco IOS dial peers are configured to provide connectivity for various scenarios:

- [Requirements for SIP Sessions, page 2-24](#)
- [Default Dial Peer Scenarios, page 2-25](#)

## Requirements for SIP Sessions

Cisco IPICS imposes the following requirements on SIP sessions:

- SIP sessions between the SIP provider and Cisco IPICS are restricted to the following media capabilities:
  - Codec must be G.711u-law
  - Packet size must be 20 bytes (the default value for G.711 u-law)
  - Sampling rate must be 8000 Hz (the default value for G.711 u-law)
  - Telephone event payload must be 101

- The multicast packets that Cisco IPICS sends to the UMS must have a Time to Live (TTL) of 64. This value is not configurable.
- A firewall must allow TCP and UDP traffic to pass on ports 5060 and 5061 for SIP signaling. A firewall must allow UDP traffic to pass on ports 1600 through 20480 for the voice payload.
- NAT traversal is not supported by Cisco IPICS. There cannot be a NAT between Cisco IPICS and the UMS or between Cisco IPICS and the SIP provider.

## Default Dial Peer Scenarios

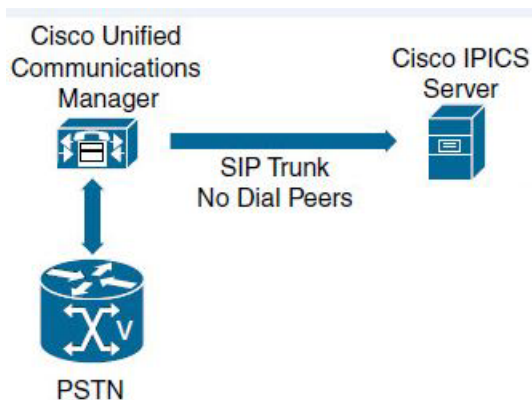
You must configure specific incoming dial peers and outgoing dial peers on the telephony gateway. These configurations vary depending on whether you use the Cisco IOS gateway or Cisco Unified Communications Manager. There also are dial peer requirements when you use the Cisco IPICS direct dial feature. For related information about configuring Cisco IPICS for the direct dial feature, see the “Configuring SIP” section in *Cisco IPICS Server Administration*.

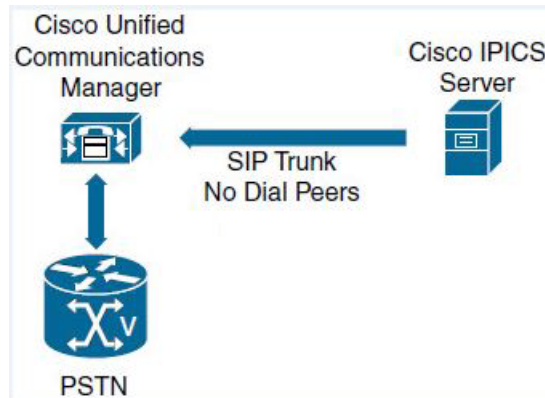
### Dial Peer Use in Scenarios

The following figures describe which dial peers are used in different scenarios:

- [Figure 2-19 on page 2-25, “Calls to Policy Engine in Deployment that Uses Cisco Unified Communications Manager”](#)
- [Figure 2-20 on page 2-26, “Calls from Policy Engine in Deployment that Uses Cisco Unified Communications Manager”](#)

**Figure 2-19**      *Calls to Policy Engine in Deployment that Uses Cisco Unified Communications Manager*



**Figure 2-20** *Calls from Policy Engine in Deployment that Uses Cisco Unified Communications Manager*

## Call Flow and Dial Peer Examples

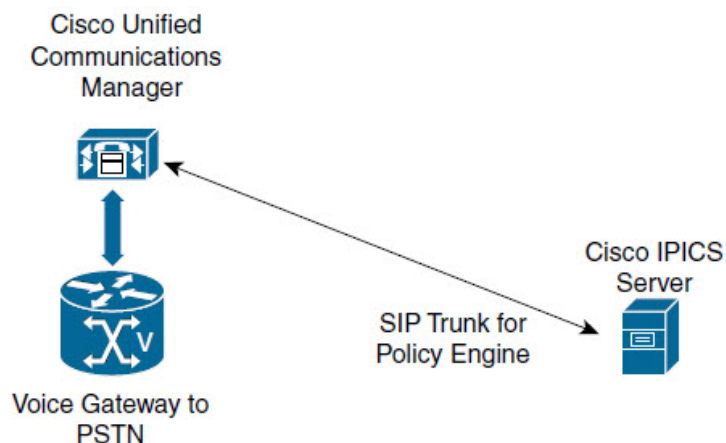
The following sections describe possible call flows and provide dial peer configuration examples for various scenarios:

- [Scenario 1: Policy Engine <-> SIP <-> Cisco Unified Communications Manager 8.6 through 10.0, page 2-26](#)
- [Scenario 2: Policy Engine <-> SIP <-> Cisco IOS SIP Gateway, with no Cisco Unified Communications Manager or Cisco Unified Communications Manager Express, page 2-27](#)
- [Scenario 3: Policy Engine <-> SIP <-> Cisco IOS SIP Gateway, Cisco Unified Communications Manager, page 2-27](#)

### Scenario 1: Policy Engine <-> SIP <-> Cisco Unified Communications Manager 8.6 through 10.0

This scenario requires a SIP trunk between Cisco IPICS and Cisco Unified Communications Manager for dial in and dial out.

[Figure 2-21](#) illustrates this scenario.

**Figure 2-21** *Calls in Deployment that Uses Cisco Unified Communications Manager*

This scenario does not include a Cisco IOS SIP gateway, so only relevant dial peer entries are configured in the UMS.

Cisco Unified Communications Express dial peers are configured as follows. The dtmf-relay rtp-nte setting is required to allow parties called by the dial engine to enter DTMF digits when the parties connect to the Cisco IPICS telephony user interface (TUI).

```
dial-peer voice 555 voip
  voice-class codec 2
  session protocol sipv2
  incoming called-number .
  dtmf-relay rtp-nte
  no vad
!
dial-peer voice 556 voip
  description sip provider
  destination-pattern .T
  voice-class codec 1
  session protocol sipv2
  session target ipv4:<Cisco Unified Communications Manager IP Address>
  session transport tcp
  dtmf-relay rtp-nte
```

### Scenario 2: Policy Engine <-> SIP <-> Cisco IOS SIP Gateway, with no Cisco Unified Communications Manager or Cisco Unified Communications Manager Express

This scenario is dependent on the desired SIP call routing. The appropriate dial peers must be configured based on your requirements. In most cases, this configuration will be a subset of scenario 3 in which the dial peers that are used for connectivity with the Cisco Unified Communications Manager are modified to reflect the desired dial patterns and destinations.

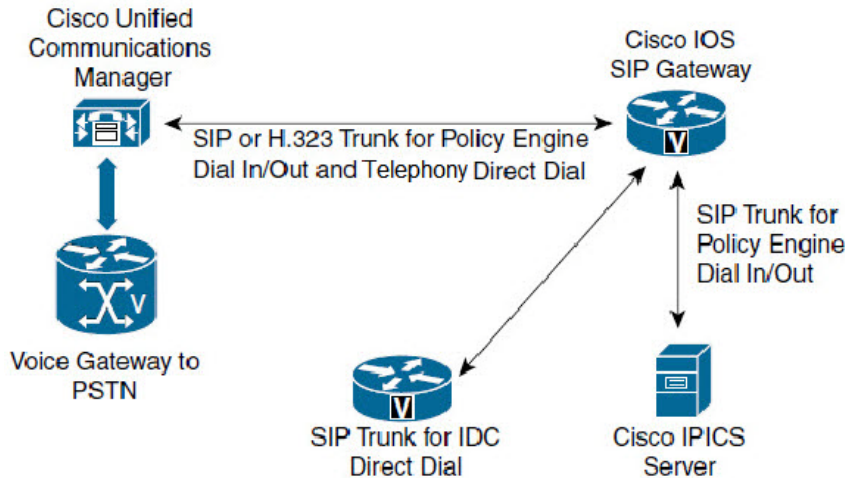
### Scenario 3: Policy Engine <-> SIP <-> Cisco IOS SIP Gateway, Cisco Unified Communications Manager

In scenario, the Cisco IOS SIP gateway is the SIP provider and the SIP trunk for direct dial is on a separate router.

[Figure 2-22](#) illustrates this scenario.



**Figure 2-22** *Calls in Deployment that Uses Cisco IOS SIP Gateway and Cisco Unified Communications Manager, SIP Trunk Functionality not on the Cisco IOS SIP Gateway*



The example dial peer configuration in this scenario assumes the following:

- Phones that are connected to Cisco Unified Communications Manager have five-digit extensions.
- Outbound calls to the PSTN and to other Cisco Unified Communications Manager servers are routed in the Cisco Unified Communications Manager servers by using 9 and 8.
- Dial numbers that ops views use to reach the dial engine are five-digit numbers that start with 251.
- There is no direct dial prefix so no translation rules are required.

This scenario addresses the following call types:

- Calls from Cisco Unified Communications Manager (incoming dial peer 555, outgoing dial peer 25100 on Cisco IOS SIP gateway)
- SIP calls from the dial engine through the Cisco IOS SIP gateway to Cisco Unified Communications Manager (incoming dial peer 555, outgoing dial peers 25000.8000 and 9000 on Cisco IOS SIP)

Cisco IOS SIP gateway dial peers are configured as follows:

```
dial-peer voice 555 voip
voice-class codec 2
session protocol sipv2
incoming called-number .
dtmf-relay rtp-nte
no vad
!
dial-peer voice 25000 voip
destination-pattern .....
voice-class codec 1
session target ipv4:<Cisco Unified Communications Manager 4.1 IP Address>
session transport tcp
dtmf-relay h245-alphanumeric
!
dial-peer voice 9000 voip
destination-pattern 9T
voice-class codec 2
session target ipv4:<Cisco Unified Communications Manager 4.1 IP Address>
dtmf-relay h245-alphanumeric
!
dial-peer voice 8000 voip
destination-pattern 8T
```



```
voice-class codec 2
session target ipv4:<Cisco Unified Communications Manager 4.1 IP Address>
dtmf-relay h245-alphanumeric
!
dial-peer voice 25100 voip
destination-pattern 251..
session protocol sipv2
session target ipv4:<Cisco IPICS Server IP Address>
session transport tcp
dtmf-relay rtp-nte
```

## Cisco IPICS Integration with LDAP

Cisco IPICS lets you use the Lightweight Directory Access Protocol (LDAP) to authenticate against an Active Directory (AD) server users who access Cisco IPICS.

You enable and configure this LDAP integration through the Cisco IPICS Administration Console by following these general steps:

- In the Dial Information and Dial Port Resource Allocation pane in the Ops View Window, check the **Use LDAP Authentication** check box in the LDAP Authentication pane to enable LDAP authentication for users who are associated with an ops view
- Make configuration settings as described in the “Configuring LDAP” section in *Cisco IPICS Server Administration Guide*

In addition, you can use the Cisco IPICS CLI to add users to Cisco IPICS directly from an LDAP server, as described in the “Bulk Users Import Command” section in *Cisco IPICS Command Line Interface Reference Guide*.

For related information, see *IPICS LDAP User Configuration Example*, which is available at <https://www.cisco.com/c/en/us/support/unified-communications/instant-connect/products-technical-reference-list.html>.

## Cisco Instant Connect for Android Devices

Cisco Instant Connect for Android Devices is an app that allows you to use an Android device to interact with other participants in a Cisco PICS incident. The device can communicate with Cisco IPICS either via a WiFi network connection or a 3G, 4G, or LTE connection. For detailed information about this application, and information about feature limits when using a WiFi connection, see *Cisco Instant Connect for Android Devices User Guide*.

When using an Android device as a mobile client, be aware of the following:

- If you are using a WiFi connection, the Cisco IPICS server and the UMS component must be accessible on the wireless network.
- Network connectivity for all Cisco IPICS components that are to be used with the mobile client should be established before using the mobile client.
- When you view a list of talk lines, the information in the screen updates automatically. The update interval is defined by the IDC Update Poll option in the **Administration > Options > IDC/Client tab** in the Cisco IPICS Administration Console. The default update interval is 5 seconds.

The following sections provide related information:

- [DNS Configuration, page 2-30](#)

- [Point-to-Point Calls, page 2-31](#)
- [Using Cisco Jabber with Cisco Instant Connect for Android Devices, page 2-31](#)

## DNS Configuration

The mobile client uses SSL to communicate with the server. SSL requires that DNS be enabled in your network.

The following sections provide information about the models that you can use to configure DNS in your network.

- [Intranet Access Model, page 2-30](#)
- [Internet/Intranet Access Model, page 2-30](#)

### Intranet Access Model

This section provides guidelines for how to configure DNS when a mobile client will connect to an IPICS server only on a local intranet.

- Ensure that a DNS server is configured in your LAN.
- Configure each component in the Cisco IPICS component to use this DNS server for hostname resolution.
- Configure the hostname for the DNS server as an entry in the DNS server.
- Ensure that you can ping the Cisco IPICS server by its hostname from each mobile client.
- If you are using DHCP for IP address assignments, ensure that the correct search domain is configured on the DHCP server or the wireless controller that is acting as a DHCP server. The search domain is not populated automatically.
- If you are not using DHCP for IP address assignment, ensure that the correct domain name and client ID are configured on the mobile client in addition to the IP address, mask, and default gateway values.

DHCP servers use the client ID to bind the mobile client to a specific IP address. This binding ensures that the mobile client can communicate through firewalls, and access restrictions (Access Control Lists) in your network. If you do not configure a client ID, you cannot access the Incident app on a mobile client.

### Internet/Intranet Access Model

This section provides guidelines for how to configure DNS when a mobile client will connect to a Cisco IPICS server via the Internet and a company intranet.

- Ensure that a DNS server is configured in your LAN.
- Configure each component in the Cisco IPICS component to use this DNS server for hostname resolution.
- Configure the hostname for the DNS server as an entry in the DNS server.
- Do not use the Hosts file to bypass the DNS name resolution.
- Ensure that you can ping the Cisco IPICS server by its hostname from each mobile client.

- If you are using DHCP for IP address assignments, ensure that the correct search domain is configured on the DHCP server or the wireless controller that is acting as a DHCP server. The search domain is not populated automatically.
- If you are not using DHCP for IP address assignment, ensure that the correct domain name and client ID are configured on the mobile client that you populate the DNS server address on the mobile client in addition to the IP address, mask, and default gateway values.
- If you are not using the DHCP Server for IP Address assignment, then you also need to ensure that you populate the DNS Server address on the mobile client in addition to the IP Address, Mask and Default Gateway that you may specify.
- If the mobile client needs to access two domains (one for the intranet and one for the Internet), the intranet DNS must be configured to forward requests from the mobile client to the Internet DNS, and the Internet DNS must be configured to forward requests to the intranet DNS.
- If the Cisco IPICS server is reachable on the Internet and has a FQDN registered on the web, any Internet DNS can be used to resolve the IP address of the server. In such a scenario, the local DNS should be configured with the DNS address that is provided by the local ISP. Alternatively, you can use a public DNS, such as 4.2.2.2 and 8.2.2.2, to provide name resolution.

## Point-to-Point Calls

Cisco Instant Connect for Android Devices and the IDC allow you to make a direct point-to-point call to any user that is logged in to Cisco IPICS. This type of call is a SIP call via the UMS. When you select a user to whom to place a point-to-point call, the UMS sets up a SIP call between you and the called user. When the called user answers the call, the audio (RTP) stream starts flowing via the UMS.

## Using Cisco Jabber with Cisco Instant Connect for Android Devices

A user of Cisco Instant Connect for Android Devices can use this app to send and receive calls to and from a Cisco Jabber client. This functionality requires the following:

- Cisco Instant Connect for Android Devices and Cisco Jabber be registered with Cisco Unified Communications Manager
- Call routing must be enabled on Cisco Unified Communications Manager between these Cisco Instant Connect for Android Devices and Cisco Jabber
- The Cisco Jabber client must be installed on the Android device

For related information, see *Jabber Configuration for Cisco Instant Connect Integration*, which is available at <https://www.cisco.com/c/en/us/support/unified-communications/instant-connect/products-technical-reference-list.html>.

## Wireless Network Configurations

If your Cisco IPICS deployment supports the following endpoints, you must include a wireless network in the deployment. This network can be a single Lightweight Wireless Access Point (LWAP) or a High Density Unified Wireless Network using wireless LAN controllers.

- Cisco Unified IP Phone 7925G
- Cisco Unified IP Phone 7926

- Cisco Instant Connect for Android devices

Cisco recommends that you perform a site survey before you deploy a wireless network to assess RF behavior in your environment. For information about site surveys, see *Site Survey Guidelines for WAN Deployment*, which is available at:

<http://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.html#anc0>

For additional information that relates to wireless networks, see the following documents:

- *Campus Wireless LAN Technology Design Guide*, which is available at:  
[http://www.cisco.com/web/offer/grs/189097/en-05\\_campus-wireless\\_cvd\\_cte\\_en.pdf](http://www.cisco.com/web/offer/grs/189097/en-05_campus-wireless_cvd_cte_en.pdf)
- *Campus Wireless IP Phone 792X Design Guide*, which is available at:  
[http://www.cisco.com/c/dam/en/us/td/docs/voice\\_ip\\_comm/cuipph/7925g/7\\_0/english/deployment/guide/7925dply.pdf](http://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cuipph/7925g/7_0/english/deployment/guide/7925dply.pdf)
- *Wireless LAN Controller (WLC) Configuration Best Practices*, which is available at:  
<http://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/82463-wlc-config-best-practice.pdf>

## Wireless Controller Configuration Example

The Cisco 5508 Wireless Controller can be used in a Cisco IPICS deployment. [Table 2-3](#) describes guidelines that apply when configuring this controller from its web-based administration interface. When you make updates on a page, make sure to click the **Apply** button on the page to save the updates.

**Table 2-3** Cisco 5508 Wireless Controller Configuration

Option	Setting
<b>Controller &gt; General page</b>	
802.3x Flow Control Mode	Choose <b>Disabled</b> from the drop-down list.
LAG Mode on next reboot	Choose <b>Disabled</b> from the drop-down list.
Broadcast Forwarding	Choose <b>Enabled</b> from the drop-down list.
AP Multicast Mode	Choose <b>Multicast</b> from the drop-down list. Set the Multicast Group Address to <b>239.0.0.0</b> .
AP Fallback	Choose <b>Enabled</b> from the drop-down list.
Fast SSID change	Choose <b>Enabled</b> from the drop-down list.
WebAuth Proxy Redirection Mode	Choose <b>Enabled</b> from the drop-down list.
<b>Controller &gt; Multicast page</b>	
Enable Global Multicast Mode	Check this check box.
Enable IGMP Snooping	Check this check box.
<b>Wireless &gt; Media Stream &gt; General page</b>	
Multicast Direct feature	Check the <b>Enabled</b> check box.

Table 2-3 Cisco 5508 Wireless Controller Configuration (continued)

Option	Setting
<b>Wireless &gt; Media Stream &gt; Streams page</b>	
Add New	<p>Follow these steps to create a new media stream:</p> <ol style="list-style-type: none"> <li>1. Click the <b>Add New</b> button.</li> <li>2. In the <b>Stream Name</b> field, enter a name for the media stream.</li> <li>3. In the <b>Multicast Destination Start IP Address</b> field, enter the first IP address of the multicast group IP address range.</li> <li>4. In the <b>Multicast Destination End IP Address</b> field, enter the last IP address of the multicast group IP address range.</li> <li>5. In the <b>Maximum Expected Bandwidth</b> field, enter <b>1000</b>.</li> <li>6. In the <b>Average Packet Size</b> field enter <b>1200</b>.</li> <li>7. Check the <b>RRC Periodic Update</b> check box.</li> <li>8. In the <b>RRC Priority</b> field, enter <b>8</b>.</li> <li>9. Choose <b>best-effort</b> from the <b>Traffic Profile Violation</b> drop-down list.</li> <li>10. Click the <b>Apply</b> button.</li> </ol>
<b>Wireless &gt; 802.11b/g/n &gt; Network page</b>	
Data Rates	<p>Choose <b>Disabled</b> from the <b>1 Mbps</b>, <b>2 Mbps</b>, <b>5.5 Mbps</b>, <b>6 Mbps</b>, and <b>9 Mbps</b> drop-down lists.</p> <p>Choose <b>Mandatory</b> from the <b>11 Mbps</b> and <b>12 Mbps</b> drop-down lists.</p> <p>Choose <b>Supported</b> from the remaining Data Rates drop-down lists.</p>
<b>Wireless &gt; 802.11b/g/n &gt; Media page, Media tab</b>	
Unicast Video Redirect	Check this check box.
Multicast Direct Enable	Check this check box.
<b>WLANS &gt; WLANS &gt; WLANS page, General tab</b>	
To access the General tab, choose <b>WLANS &gt; WLANS &gt; WLANS</b> , then click the WLAN that you want to configure.	
Status	Check the <b>Enabled</b> check box.
Radio Policy	Choose <b>802.11b/g only</b> from the drop-down list.
Interface/Interface Group	Choose the appropriate Interface from the drop-down list.
Multicast Vlan Feature	Uncheck the <b>Enabled</b> check box.
Broadcast SSID	Check the <b>Enabled</b> check box.
NAS-ID	Enter the appropriate ID for NAS access requests.
<b>WLANS &gt; WLANS &gt; WLANS page, Security &gt; Layer 2 tab</b>	
To access the Security > Layer 2 tab, choose <b>WLANS &gt; WLANS &gt; WLANS</b> , then click the WLAN that you want to configure.	
Layer 2 Security	Choose <b>WPA+WPA2</b> from the drop-down list.

Table 2-3 Cisco 5508 Wireless Controller Configuration (continued)

Option	Setting
<b>WLANs &gt; WLANs &gt; WLANs page, QoS tab</b>	
To access the QoS tab, choose <b>WLANs &gt; WLANs &gt; WLANs</b> , then click the WLAN that you want to configure.	
Quality of Service	Choose <b>Platinum (voice)</b> from the drop-down list.
Multicast Direct	Check this check box.
<b>WLANs &gt; WLANs &gt; WLANs page, Advanced tab</b>	
To access the Advanced tab, choose <b>WLANs &gt; WLANs &gt; WLANs</b> , then click the WLAN that you want to configure.	
Scan Defer Priority	Check the <b>0</b> check box and uncheck the <b>1, 2, 3, 4, 5, 6,</b> and <b>7</b> check boxes.
Scan Defer Time	Enter <b>1000</b> .

## Cisco Unified IP Phones

If your Cisco IPICS deployment includes Cisco Unified Communications Manager or Cisco Unified Communications Manager Express, you can use the Cisco Unified IP Phone services application programming interface (API) to provide PTT capabilities to certain Cisco Unified IP Phone models. A phone with the PTT capability enabled can provide an easy-to-use GUI that allows users to monitor or participate in a PTT channels or VTG over a VoIP network. A phone can participate in one channel or VTG at a time. To participate in a channel or VTG, a phone user chooses the desired channel or VTG from a list that displays on the phone.

The Cisco IP Phone 6941/45, 8841/61, 8941/45/61, 7841, 7911/40/41/42/45, 7960/61/62/65, 7970/71/75 and 9951/717925G can use the XML service. The Cisco Wireless IP Phone 7925 and 7926 can use either the XML service or the more advanced Instant Connect MIDlet service.

To access the XML service from the Cisco Unified IP Phone services menu, the following URL must be configured in Cisco Unified Communications Manager or Cisco Unified Communications Manager Express, where *IPICS\_server* is the host name or IP address of the Cisco IPICS server:

[http://IPICS\\_server/ipics\\_server/servlet/IPPhoneManager](http://IPICS_server/ipics_server/servlet/IPPhoneManager)



### Note

- The Cisco Unified Wireless IP Phone 7925 does not seamlessly roam when it crosses IP subnets, which can result in transmission interruptions to Cisco IPICS users
- When used as Cisco IPICS PTT XML clients, the Cisco Unified Wireless IP Phone models 7921 and 7925 do not automatically reestablish a media connection to a Cisco IPICS channel when switching from phone calls to the XML application

The IPICS MIDlet service treats channels and VTGs as talk lines. In addition, MIDlet provides a person to person direct connectivity capability through Cisco IPICS. The MIDlet works only with Cisco Unified Communications Manager. Cisco Unified Communications Manager Express does not support this MIDlet.

To access the MIDlet service, from the Cisco Unified IP Phone services menu, the following URL must be configured in Cisco Unified Communications Manager, where *IPICS\_server* is the host name or IP address of the Cisco IPICS server.

`http://IPICS_server/ipics_server/midlet/CiscoInstantConnect.jad`

For related information about configuring this feature, see the “Setting Up the Cisco IP Phone for use with Cisco IPICS” appendix in *Cisco IPICS Server Administration Guide* for this release. For a list of Cisco Unified IP Phones that Cisco IPICS supports as PTT devices, see *Cisco IPICS Compatibility Matrix*.

This section includes these topics:

- [Cisco Unified Communications Manager Configuration Overview, page 2-35](#)
- [Cisco Unified Communications Manager Express Configuration Overview, page 2-35](#)

## Cisco Unified Communications Manager Configuration Overview

You use the Cisco IP Phone Services Configuration page in the Cisco Unified Communications Manager Administration application to define and maintain the list of Cisco Unified IP Phone services to which users can subscribe. These services are XML applications that enable the display of interactive content on supported models of a Cisco Unified IP Phone.

After you configure a list of IP phone services, Cisco Unified IP Phone users can access the Cisco Unified Communications Manager User Options menu and subscribe to the services, or an administrator can add services to Cisco Unified IP Phones and device profiles. Administrators can assign services to speed-dial buttons, so users have one-button access to the services.

For detailed information about configuring phone services, see the “Cisco IP Phone Services” chapter in *Cisco Unified Communications Manager System Guide*.

## Cisco Unified Communications Manager Express Configuration Overview

The following is a sample Cisco IOS router configuration that enables Cisco Unified Communications Manager Express to support a Cisco Unified IP Phone as a Cisco IPICS PTT device.



### Note

The Cisco Instant Connect MIDlet is not supported with Cisco Unified Communications Manager Express.

```
ip dhcp excluded-address 10.1.1.1
!
ip dhcp pool pool1
 network 10.1.1.0 255.255.255.248
 domain-name yourdomainname
 dns-server dns1 dns2
 default-router 10.1.1.1
 option 150 ip 10.1.1.1

tftp-server flash:filename1
tftp-server flash:filename2

telephony-service
 load 7960-7940 filename1
 load 7970 filename2
 max-ephones n
```

```

max-dn m
ip source-address 10.1.1.1 port 2000
auto assign 1 to n
url services http://10.1.2.1/ipics_server/servlet/IPPhoneManager
create cnf-files
max-conferences 8 gain -6

ephone-dn 1 dual-line
number abcd
!
ephone-dn 2 dual-line
number efgh

```

## Notification

Notification is the process of Cisco IPICS contacting designated recipients and providing them with information that you specify. Cisco IPICS offers the following notification implementations:

- Policy engine notification—Controlled through the Cisco IPICS Administration Console and can provide notification to recipients that are configured in Cisco IPICS. You designate the way in which notification is provided by configuring notification actions. Policy engine notifications include e-mail, IP phone text, dial, talk group, and dial engine script notifications.
- Bulk Notification (using external source)—Administered outside of the Cisco IPICS Administration Console. The recipients list and prompts are passed to Cisco IPICS by a third-party application

Cisco IPICS supports multiple Cisco Unified Communications Managers for notification, which enables text and audio paging to Cisco Unified IP Phone devices that are registered on different Cisco Unified Communications Managers simultaneously.

The following sections describe following policy engine notification actions that you can configure for Cisco IPICS:

- [Email Notification Action, page 2-36](#)
- [IP Phone Text Notification Action, page 2-36](#)
- [Dial Notification Action, page 2-38](#)
- [Talk Group Notification Action, page 2-38](#)

## Email Notification Action

An Email notification action sends a message that you enter to the e-mail, SMS, and pager addresses that are configured as notification preferences for each user that you designate as a recipient. When this type of notification executes, the policy engine sends the message via SMTP to the SMTP server that is configured on the IPICS Dial Engine Parameters screen. Email notification recipients can be Cisco IPICS users or user groups.

## IP Phone Text Notification Action

An IP phone text notification action displays a designated message on supported Cisco Unified IP Phone models when used with Cisco Unified Communications Manager. Cisco Unified Communications Manager Express does not support this feature. The telephone numbers of each phone must be configured as a dial preference for the associated user. This type of notification action requires that you



use the Cisco IPICS Administration Console to configure parameters in the Cisco Unified Communications Manager Configuration for IP Phone Notifications area in the SIP Configuration menu. For instructions, see *Cisco IPICS Server Administration Guide* for this release. Recipients of this notification action can be Cisco IPICS users or user groups.

When an IP phone text notification action executes, several activities, including the following, occur:

1. IPICS sends an AXL query to the first configured Cisco Unified Communications Manager.
2. Cisco Unified Communications Manager returns the IP address of each device for which a DN is configured.
3. Cisco IPICS sends notification via XML to each device for which it receives a valid IP address.

**Note**

- The IP phone text notification action requires that the IP phone text notification parameters be configured on the Policy Engine > Dial Engine > IP Phone Notification Configuration page in the Cisco IPICS Administration Console.
- Cisco IPICS sends each DN in the notification list as a query to each Cisco Unified Communications Manager that is configured for notification.
- The Cisco Unified Communications Manager must be running the Cisco AXL service.
- Each Cisco Unified Communications Manager must be configured in the IP Phone Notification Configuration page with the correct version number, administrator and phone user name and password. This information is required to validate Cisco Unified Communications Manager and send appropriate AXL queries because the queries are different for various Cisco Unified Communications Manager versions.
- The configured Cisco Unified Communications Managers must be reachable or “Connection Failure” errors result when the Cisco IPICS attempts to send an AXL query.
- The Cisco Unified Communications Manager should be configured to accept SOAP requests.
- Cisco Unified Communications Manager limits the number of DNs in an AXL query to 200. It truncates requests that contain more than 200 DNs. To accommodate this limit, Cisco IPICS sends requests that contain no more than 200 DNs. If Cisco IPICS needs more than 200 DNs, it sends requests in batches that contain 200 or fewer DN requests.
- Cisco IPICS precedes a text notification with an audible tone, which comes from a prerecorded .wav file that is sent to each phone in the recipient list. Cisco IPICS requires that an available multicast address be configured in the multicast address pool for each batch of simultaneous broadcasts of the alert audio.
- If Cisco IPICS cannot reach a Cisco Unified IP Phone or if notification to a phone fails, Cisco IPICS adds the phone to a retry list. When Cisco IPICS completes a round of notification to identified phones, it attempts to resend the notification to the phones in the retry list. Cisco IPICS attempts to send notification up to three times (one regular notification attempt and up to two retry notification attempts). Any phones that it cannot reach after these attempts are not notified via IP phone text notification.
- Cisco IPICS sends an AXL query to all Cisco Unified Communications Managers in a cluster. If more than one Cisco Unified Communications Manager is configured with phones that register to the same DN, all the phones associated to that DN are notified.

## Dial Notification Action

The policy engine executes a dial notification action as follows:

- If the Cisco Unified Communications Manager Configuration for IP Phone Notifications parameters are configured in the SIP Configuration menu, the Cisco IPICS checks whether each designated user has an associated Cisco Unified IP Phone configured in Cisco Unified Communications Manager. If a user does have an associated phone, Cisco IPICS plays the designated message on the speaker of the phone.
- If Cisco Unified Communications Manager Configuration for IP Phone Notifications parameters are configured but a user does not have an associated Cisco Unified IP Phone, or if the phone of a user is busy, the system calls the user as specified in the dial preferences and plays the designated message.
- If Cisco Unified Communications Manager Configuration for IP Phone Notifications parameters are not configured, the Cisco IPICS calls the user as specified in the dial preferences and plays the designated message.

When you create a dial notification action, you can specify a prerecorded prompt or record a new prompt. A prompt should be no more than 90 seconds long.

If you use this action to contact Cisco Unified IP Phones, make sure that at least one multicast address is available in the multicast pool.

For more detailed information, see *Cisco IPICS Server Administration Guide* for this release.

## Talk Group Notification Action

A talk group notification action plays the selected prompt to all participants in the selected VTG.

When you create a talk group notification action, you can specify a prerecorded prompt or record a new prompt. A prompt should be no more than 90 seconds long.



### Note

- When a Talk Group notification executes, the designated message is added to the multicast stream of the VTG. To inform users that a system message is being played, consider starting the message with a statement such as, “This is the Cisco IPICS administrator with an important recorded message.”
- A VTG participant who is dialed in through the TUI and who has the floor does not hear the talk group notification message.

## Trust Management

Trust between Cisco IPICS nodes, UMS nodes, and LDAP nodes in a Cisco IPICS cluster are established with the following types of access:

- Secure Shell (SSH)—A connection used to automate configuration tasks and to perform file synchronization across servers.
- Secure Socket Layer (SSL)/Transport Layer Security (TLS)—A trusted pipe that is used for heartbeats and command/control messages between servers, and to encrypt data that is sent to clients and requests that are sent to servers

Trust between nodes can be established by either of these types of certificate exchanges:

- Self-signed certificates—Establish trust with self signed certificates.
- Third party signed certificates—Establish trust with a third party certificate authority (CA) signed certificates. (Cisco IPICS uses the Rooted Hierarchical Trust Model for these certificate types.)

When using self signed certificates, you must download and install certificates on each node.

When using third party certificates, you must install the CA certificates on the Cisco IPICS server.

For detailed information about installing certificates, see the “Installing Signed Certificates” in *Cisco IPICS Server Administration Guide*.

## IDC Coexistence with Cisco Safety And Security Desktop

Cisco Safety and Security Desktop (SASD) version 7.8 and the IDC can be installed on the same PC. If the PC is running the following software, the SASD and the IDC can function can operate simultaneously without affecting each other, even through they share a runtime environment.

- Microsoft Windows 10
- Microsoft DirectX End-User Runtime (installed with Microsoft Windows 10)
- Microsoft .NET 4.0 (installed with Microsoft Windows 10)
- Visual C++ 2008 SP1

To enable a PC to run the SASD and IDC simultaneously and properly, follow these guidelines:

1. Install the SASD on the PC. Use the SASD to connect to a live video stream and ensure that you can view the stream.
2. Install the IDC on the same PC. When the installation program prompts you to install runtime environments and media drivers, choose **No**.

## Port Usage

Table 2-4 describes the ports and transport protocols that various components use in a Cisco IPICS deployment.

**Table 2-4** Port Usage

Port Number	Where Used	Function	Transport Protocol
80	<ul style="list-style-type: none"> <li>• Cisco IPICS server</li> <li>• Mobile client</li> </ul>	HTTP	TCP
443	<ul style="list-style-type: none"> <li>• Cisco IPICS server</li> <li>• Mobile client</li> </ul>	HTTPS	TCP
1194	<ul style="list-style-type: none"> <li>• Cisco IPICS server</li> </ul>	Administration	TCP
1196	<ul style="list-style-type: none"> <li>• Cisco IPICS server</li> </ul>	Dial engine heartbeat	TCP
2224	<ul style="list-style-type: none"> <li>• Cisco IPICS server</li> </ul>	UMS heartbeat	UDP
2225	<ul style="list-style-type: none"> <li>• Radio control service</li> </ul>	UMS radio control service	UDP

Table 2-4 Port Usage (continued)

Port Number	Where Used	Function	Transport Protocol
3444	• UMS	Remote Cisco IPICS server heartbeat	TCP
3446	• UMS	UMS monitor	UDP
3447	• UMS	Dial engine monitor	UDP
3448	• UMS	Radio control service	UDP
4100	• Cisco IPICS server	Radio control service	TCP
5060	• Cisco IPICS server • Mobile client • UMS	SIP	TCP and UDP
5061	• Cisco IPICS server • Mobile client • UMS	SIP - TLS	TCP
5062	• UMS	UMS WebSocket SIP connector	TCP
5555	• Cisco IPICS server • Mobile client • UMS	HTTPS to UMS	TCP
6294	• Cisco IPICS server	Dial engine	TCP
8080	• Cisco IPICS server • UMS	HTTP to UMS	TCP
8443	• Tomcat	HTTPS redirect	TCP
11099	• Cisco IPICS server	Policy engine	TCP
20000	• Cisco IPICS server • Mobile client	Media engine	TCO
32778	• Cisco IPICS server • UMS	Remote heartbeat receiver	TCP
16384 through 20480	• Mobile client • UMS	Media mixer	UDP
21000, 21001	• Cisco IPICS server • Mobile client	RTP / RTCP multicast	UDP
25000 through 29096	• Cisco IPICS server • Mobile client	TGMS (restreamer)	UDP
35000 through 39096	• Cisco IPICS server • Mobile client	Dial Media Service (DMS)	UDP

**Table 2-4** Port Usage (continued)

Port Number	Where Used	Function	Transport Protocol
4000 through 20480	<ul style="list-style-type: none"><li>Mobile client</li></ul>	RTP/RTCP, SRTP	UDP
8005, 8443	<ul style="list-style-type: none"><li>Cisco IPICS server</li><li>Mobile client</li></ul>	Tomcat	TCP

The following section provide related information:

- [Guidelines for Using IP Multicast Addresses with Cisco IPICS, page 2-41](#)
- [QOS Policy Considerations, page 2-41](#)

## Guidelines for Using IP Multicast Addresses with Cisco IPICS

When you use multicast communications with Cisco IPICS be aware of the following guidelines:

- This address range is part of the Administratively Scoped Block, as specified by RFC 3171, and is intended for use in a local domain. As such, this address range is less likely to cause an addressing conflict in an existing multicast domain.
- Although RFC 3171 permits the use of IP multicast addresses that span the 224.0.0.0 through 239.255.255.255 range, where the first octet contains 224, 232, 233, 238, or 239 and subsequent octets contain 0 through 255, be aware that Cisco recommends the use of the 239.192.0.0 to 239.251.255.255 range to ensure proper use and desired results.
- For more information, see RFC 3171 - Internet Assigned Numbers Authority (IANA) Guidelines for IPv4 Multicast Address Assignment and RFC 2365 - Administratively Scoped IP Multicast.

## QOS Policy Considerations

When defining QOS policies that will be assigned to a UDP port range, using Source Host and Destination Host addresses of ANY allows the QOS policy to be properly set based on the mobile client UDP port range. In this case, UDP ports that are assigned by the UMS are not considered, which helps to simplify the QOS policies.





## Cisco IPICS LMR Gateway Configurations

---

This chapter provides an overview of how to install and configure a land mobile radio (LMR) gateway to interface to audio devices. These audio devices typically consist of radios. For a information features that are supported by various, see *Cisco IPICS Compatibility Matrix*.

The Cisco Hoot ‘n’ Holler feature is used to enable land mobile radios (LMRs) in a Cisco IPICS solution. An LMR is integrated by providing an ear and mouth (E&M) interface to an LMR or to other PTT devices, such as Sprint and Nextel phones. This interface is in the form of a voice port that is configured to provide an appropriate electrical interface to the radio. The voice port is configured with a connection trunk entry that corresponds to a VoIP dial peer, which in turn associates the connection to a multicast address. You can configure a corresponding channel in Cisco IPICS, using the same multicast address, which enables Cisco IPICS to provide communication paths between the desired endpoints.

For information about Cisco Land Mobile Radio (LMR) over IP, see the documentation at the following URLs:

- [http://www.cisco.com/en/US/products/ps6441/products\\_feature\\_guide09186a00801f092c.html](http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a00801f092c.html)
- [http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products\\_implementation\\_design\\_guide\\_book09186a0080347c1b.html](http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_implementation_design_guide_book09186a0080347c1b.html)

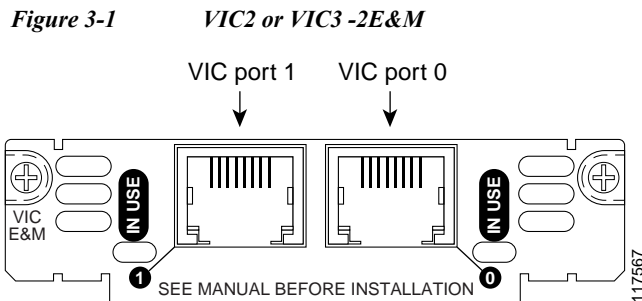
This chapter includes these topics:

- [Interfacing the Cisco IPICS LMR Gateway with Land Mobile Radios, page 3-2](#)
- [Cisco IOS LMR Gateway Configurations, page 3-7](#)
- [Pooled Radios, page 3-52](#)
- [Serial Radio Control, page 3-54](#)
- [Trunked Radio Optional Workaround, page 3-64](#)
- [Analog Tap Recording Configuration, page 3-68](#)
- [Cisco IPICS Integration with ISSI Gateways, page 3-70](#)
- [Cisco IPICS Integration with DFSI Gateways, page 3-71](#)
- [Feature Support for Radios, page 3-71](#)

# Interfacing the Cisco IPICS LMR Gateway with Land Mobile Radios

Audio connections between the radio and Cisco IPICS solution is accomplished by using a software feature license with Cisco E&M interface cards. (These cards have been used for years to interface telephone switching equipment and Cisco routers.) The combination of the feature license and the E&M card creates an LMR gateway.

Figure 3-1 shows a VIC2 or VIC3 -2E&M card.



This section includes these topics:

- [Cabling, page 3-2](#)
- [Analog E&M Interface, page 3-4](#)
- [Analog E&M signaling Types, page 3-4](#)

## Cabling

This section describes how to determine the proper cable to use when connecting a device to E&M card.

The LMR signaling enhancements in Cisco IOS software apply to the analog E&M interface for LMR signaling only. For a description of how the leads on the analog E&M interface are implemented on Cisco IOS voice gateways, Cisco recommends that you review *Understanding and Troubleshooting Analog E&M Interface Types and Wiring Arrangements* before proceeding further. This document is available at this URL:

<http://www.cisco.com/warp/public/788/signalling/21.html>

LMR cable building requires an understanding of the radio. Some equipment requires components in the cable, such as resistors, capacitors, inductors, or inverters. It is important that you understand the LMR side of the cable and which signals are expected to and from the LMR before connecting it to the E&M port on the router.



An LMR gateway is configured to support 2-wire or 4-wire audio. The audio and control signals enter and exit the E&M port via an RJ-45 jack on the E&M card. The simplest cable is a standard Category 5 Ethernet cable on which one end is unterminated. Stripping back the wire jacket exposes four pairs of wires:

- The blue pair of wires (Tip-1 and Ring-1) maps to pins 4 and 5 on the RJ-45 plug of the E&M card. In a 4-wire operation, this pair of wires carries the outbound audio from the gateway card. The leads are transformer-isolated with an impedance of 600 ohms across each pair, providing a 600 ohm transformer coupled audio appearance to radios. These leads typically connect to a microphone jack or pin on an LMR. In two-wire operation, the Tip-1 and Ring-1 leads carry the full-duplex audio.
- The green pair of wires (Tip and Ring) maps to pins 3 and 6 on the RJ-45 plug of the E&M card. In 4-wire operation, this pair of wires carries the inbound audio to the gateway card. The leads are transformer-isolated with an impedance of 600 ohms across each pair, providing a 600 ohm transformer coupled audio appearance to radios. These leads typically connect to a speaker jack or pin on an LMR. In two-wire operation, the Tip and Ring leads are not used.
- The brown pair of wires map to pins 7 and 8 on the RJ-45 plug of the E&M card. This pair of wires is used to signal PTT to the LMR. In E&M type II and III, signaling polarity must be observed: pin 8 maps to Signal Ground (SG) and pin 7 maps to the “E” lead, which also is the PTT connection of the LMR.
- The orange pair of wires maps to pins 1 and 2 on the RJ-45 plug of the E&M card. This pair of wires is optional and used only if the LMR provides signaling for Carrier Operated Relay (COR) or Carrier Operated Squelch (COS) functionality. If the LMR does not provide COR/COS output signals, this pair of wires is not used. In E&M type II and III signaling, polarity must be observed: pin 1 maps to Battery Voltage (SB) and pin 2 maps to the “M” lead.

Figure 3-2 shows the sequential pin orientation on a standard RJ-45 connector.

**Figure 3-2** *RJ-45 Pinout*

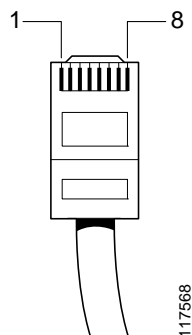


Table 3-1 shows the pin orientation of a standard RJ-45 connector.

**Table 3-1** *E&M VIC Pinout*

Router RJ-45 Pin No.	Router Function	Category 5 Color Code	Radio Connection
1	Signal Battery (SB)	Orange	Signal Battery (SB)
2	M-Lead	White/Orange	COR/COS
3	Ring	White/Green	Speaker +
4	Ring-1	Blue	Microphone –
5	Tip-1	White/Blue	Microphone +

*Table 3-1 E&M VIC Pinout (continued)*

Router RJ-45 Pin No.	Router Function	Category 5 Color Code	Radio Connection
6	Tip	Green	Speaker –
7	E-Lead	White/Brown	PTT
8	Signal Ground (SG)	Brown	Ground

## Analog E&M Interface

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

## Analog E&M signaling Types

Cisco LMR routers support Type II, Type III, and Type V E&M signaling. With each signaling type, the router supplies one signal, known as the M (for Mouth) signal, and accepts one signal, known as the E (for Ear) signal. Conversely, the LMR equipment accepts the M signal from the router and provides the E signal to the router. The M signal that is accepted by the LMR equipment at one end of a circuit becomes the E signal that is output by the remote LMR interface.

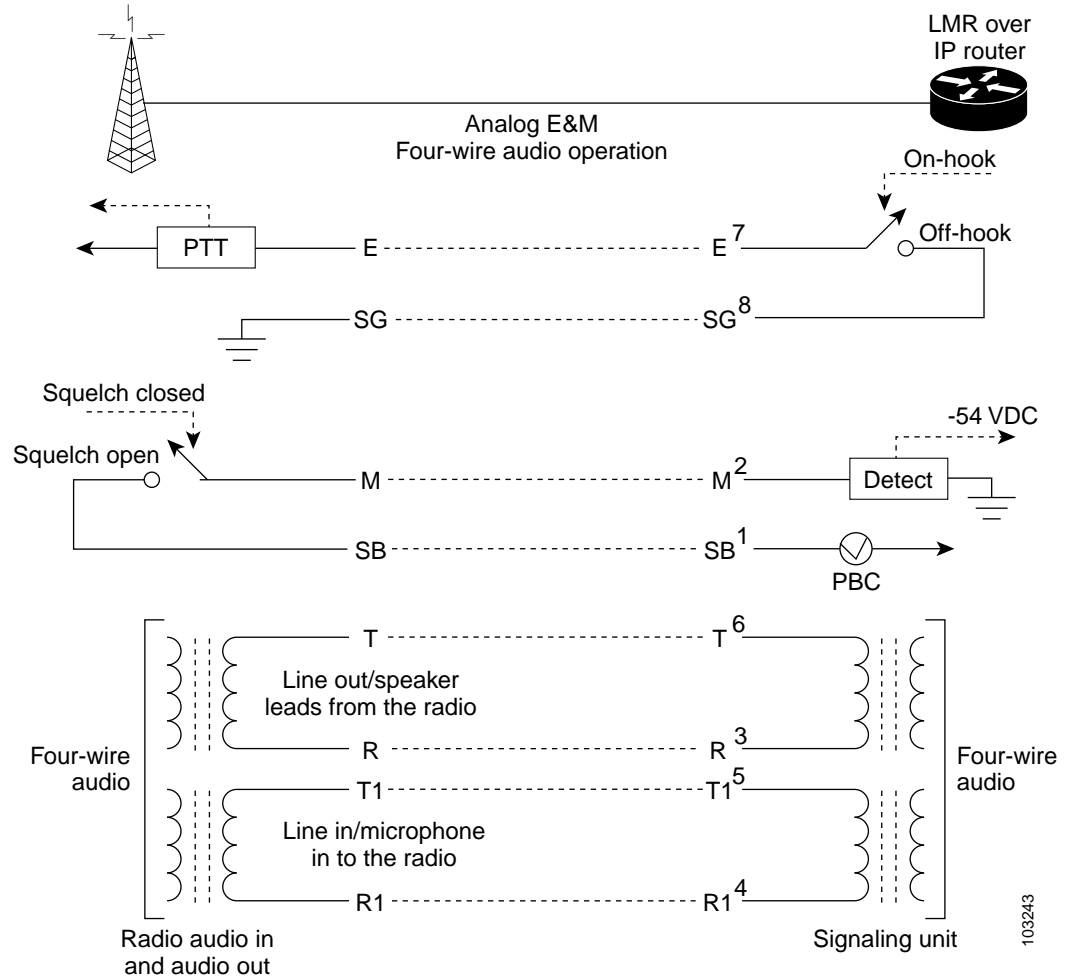
When configuring a voice port, you must select the E&M interface type that is matched to the connected device.

Type II indicates the following lead configuration:

- E—Output, relay to SG
- M—Input, referenced to ground
- SB—Feed for M, connected to –48V
- SG—Return for E, galvanically isolated from ground

Figure 3-3 shows the lead designations and functions for the Type II E&M interface.

Figure 3-3 E&amp;M Type II Interface

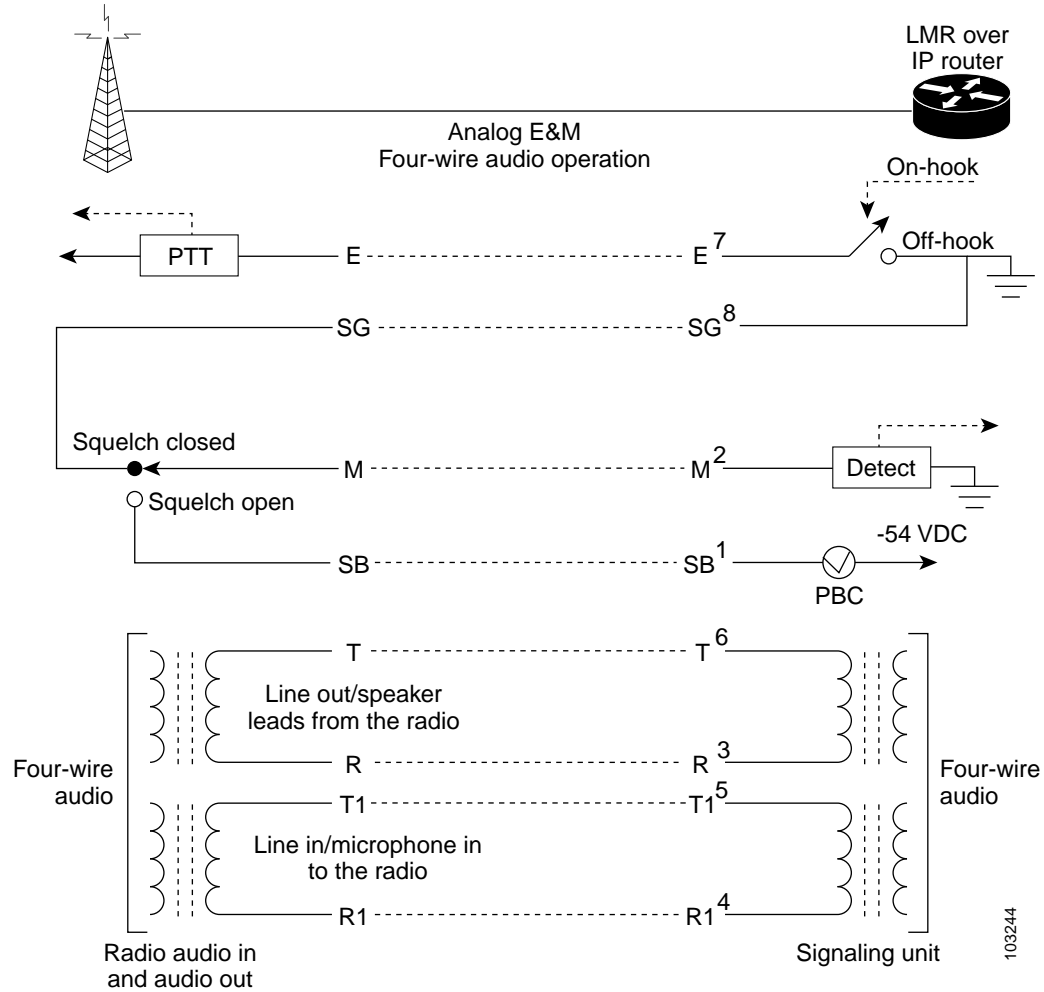


Type III indicates the following lead configuration:

- E—Output, relay to ground
- M—Input, referenced to ground
- SB—Connected to -48V
- SG—Connected to ground

Figure 3-4 shows the lead designations and functions for the Type III E&M interface.

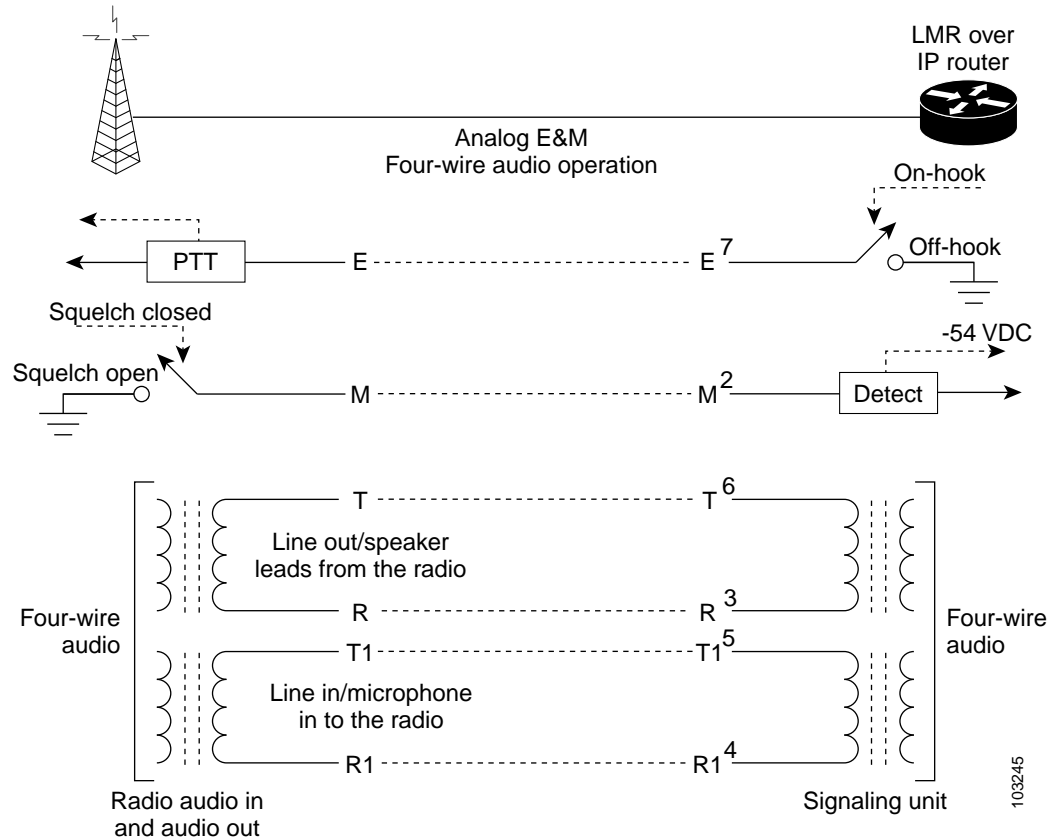
Figure 3-4 E&amp;M Type III Interface



- Type V indicates the following lead configuration:
  - E—Output, relay to ground
  - M—Input, referenced to -48V

Figure 3-5 shows the lead designations and functions for the Type V E&M interface.

Figure 3-5 E&amp;M Type V Interface



## Cisco IOS LMR Gateway Configurations

This section describes the Cisco IOS configurations that are used for different types of radios. An LMR port must have a configuration that is similar to what is described in this section.

This section includes these topics:

- [Determining Correct Cisco IOS Radio Control, page 3-7](#)
- [Required Baseline LMR Gateway Configuration, page 3-8](#)
- [VAD Operated Signaling Configuration, page 3-9](#)
- [COR/COS Operated Signaling Configuration, page 3-11](#)

### Determining Correct Cisco IOS Radio Control

Router configuration and connections typically are determined by the capabilities of the radio to be interfaced. There are three basic types of Cisco IOS radio control configurations. Use the router configuration that best matches your situation.

- **VAD Operated Signaling**—Typically used when the radio device does not provide Carrier Operated Relay/Carrier Operated Signal (COR/COS) signaling. Without the COR/COS signaling interface from the radio device, the router uses the voice activation detection (VAD) function within Cisco IOS to determine when a signal is being received from the radio device and to begin sending VoIP packets on the designated multicast address. Typically, this option is used when a portable radio device is the endpoint because these devices do not normally provide signaling for COR/COS.
- **COR/COS Signaling**—Should be used when a radio device has the ability to provide COR/COS signaling. In this situation, the router begins sending VoIP packets on the assigned multicast address when this line is activated by the radio device. Typically, this approach provides the most reliable audio reception and eliminates the clipping at the beginning of a conversation that may occur when the VAD Operated Signaling function is employed.

## Required Baseline LMR Gateway Configuration

The following baseline Cisco IOS configuration commands are required regardless of the signaling that is implemented:

```
voice service voip
ip address trusted list
ipv4 0.0.0.0 0.0.0.0
allow-connections h323 to h323
allow-connections h323 to sip
allow-connections sip to h323
allow-connections sip to sip
fax protocol cisco
h323
sip
    bind control source-interface Loopback0
    bind media source-interface Loopback0!
ip multicast-routing
!
voice class codec 1
    codec preference 1 g729r8
    codec preference 2 g711ulaw
!
interface Loopback0
ip address 192.168.4.6 255.255.255.255
ip pim sparse-dense-mode
!
interface Vif1
ip address 192.168.3.5 255.255.255.252
ip pim sparse-dense-mode
!
interface FastEthernet0/0
description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0/0$
ip address 192.168.0.6 255.255.255.0
ip pim sparse-dense-mode
duplex auto
speed auto

ip pim rp-address 192.168.1.1 bi-dir
ip rtcp report interval 5001
!
gateway
timer receive-rtcp 5
timer receive-rtp 1200
```

## VAD Operated Signaling Configuration

You must issue the **lmr m-lead inactive** command for VAD Operated Signaling. When this configuration is used, the router ignores signals that are sent by voice on the M-lead. The flow of voice packets is determined by VAD. Typically, six of the eight wires are employed.

Table 3-2 shows the wiring connections that are used when interfacing to a VAD-operated radio.

**Table 3-2** VAD Physical LMR Connections

Router RJ-45 Pin No.	Router Function	Category 5 Color Code	Radio Connection
1 <sup>1</sup>	Signal Battery (SB)	Orange	Not Connected
2 <sup>1</sup>	M-Lead	White/Orange	Not Connected
3	Ring	White/Green	Speaker +
4	Ring-1	Blue	Microphone –
5	Tip-1	White/Blue	Microphone +
6	Tip	Green	Speaker –
7	E-Lead	White/Brown	PTT
8	Signal Ground (SG)	Brown	Ground

1. Does not apply to this configuration.

Cisco VAD has two layers: application programming interface (API) layer and processing layer. There are three states into which the processing layer classifies incoming signals:

- speech
- unknown
- silence

The state of the incoming signals is determined by the noise threshold, which can be configured with the **threshold noise** command.

If the incoming signal cannot be classified, the variable thresholds that are computed with the speech and noise statistics that VAD gathers are used to make a determination. If the signal still cannot be classified, it is marked as unknown. The final VAD qualification is made by the API. In some scenarios, the audio that is classified as unknown can create unwanted voice packet traffic, which can consume extra bandwidth. The sound quality of the connection is slightly degraded with VAD, but the connection takes much less bandwidth.

### VAD Command States

The following VAD command states are possible:

- Silence State—If the voice level is below the noise threshold, the signal is classified as silence and no VoIP packets are sent over the network
- Speech/Unknown States—Signals classified as Speech and Unknown are sent over the network as VoIP packets

### VAD Aggressive Command States

When the aggressive keyword is used with the **vad** command in dial peer configuration mode, the VAD noise threshold is reduced from –78 to –62 dBm. Noise that falls below the –62 dBm threshold is considered to be silence and is not sent over the network.

- **Silence / Unknown States**—If the voice level is below the noise threshold, the signal is classified as silence and no VoIP packets are sent. Additionally, unknown packets are considered to be silence and are discarded when the aggressive keyword is used.
- **Speech State**—Only the incoming signal that is classified as speech causes packets to be sent over the network.

The following shows a sample configuration for an LMR voice port that is configured for VAD operated signaling.

In this example, type { 2 | 3 | 5 } typically is type 3, but see [Figure 3-3 on page 3-5](#), [Figure 3-4 on page 3-6](#), and [Figure 3-5 on page 3-7](#) to select the type that best matches your radio requirements. Input gain { -27 - 16 } typically is 10, but adjust this value as needed to best receive audio on Cisco IPICS endpoints. Output attenuation { -16 - 27 } typically is 10, but adjust this value as needed to best receive audio on radios. When connecting a radio to a voice port in an LMR gateway, you may need to make adjustments to properly balance the audio levels. A radio typically provides gain adjustments, and the level of the signal from the radio to the voice port and the level of the signal from the voice port to the radio may require some adjustments on the radio and the voice port. When using a tone controlled radio, it is important to note that the tones that are sent from the LMR gateway to the radio also are affected by the voice ports output attenuation settings. When optimizing these settings to achieve the desired audio levels, take care to ensure that the voice port adjustments do not have an adverse effect on the level and quality of the tone signals.

```
voice class permanent 1
  signal timing oos timeout disabled
  signal keepalive disabled
  signal sequence oos no-action
!
voice-port 0/2/1
  voice-class permanent 1
  auto-cut-through
  operation 4-wire
  type { 2 | 3 | 5 }
  signal lmr
  lmr e-lead voice
  bootup e-lead off
  lmr duplex half
  lmr led-on
  input gain { -27 - 16 }
  output attenuation { -16 - 27 }
  no echo-cancel enable
  no comfort-noise
  timeouts call-disconnect 3
  timeouts wait-release 3
  timing hookflash-in 10
  timing hangover 80
  timing delay-voice tdm 40
  connection trunk 102
  description VAD Operated Voice Port
  threshold noise -40
!
dial-peer voice 102 voip
  destination-pattern 102
  session protocol multicast
  session target ipv4:239.193.1.2:21000
  codec g711ulaw
  vad aggressive
```



## COR/COS Operated Signaling Configuration

When the COR/COS operated signaling configuration is used, the router employs signals that are sent by voice on the M-lead pin 2. The M-lead corresponds to the COR/COS of the radio system, which indicates receive activity on the radio system. The **lmr m-lead audio-gate-in** command configures the voice port to generate VoIP packets only when a seize signal is detected on the M-Lead. The router stops generating VoIP packets when the seize signal is removed from the M-lead. It is important to understand that even if there is audio on pins 3 and 6 coming from the radio, the router begins to send VoIP packets on the assigned multicast address only if the signal on pin 2 has become active. Typically all eight wires are employed.

Table 3-3 shows the wiring connections that are used when interfacing to a COR/COS operated radio.

**Table 3-3** COR/COS Physical LMR Connections

Router RJ-45 Pin No.	Router Function	Category 5 Color Code	Radio Connection
1	Signal Battery (SB)	Orange	Signal Battery (SB)
2	M-Lead	White/Orange	COR/COS
3	Ring	White/Green	Speaker +
4	Ring-1	Blue	Microphone –
5	Tip-1	White/Blue	Microphone +
6	Tip	Green	Speaker –
7	E-Lead	White/Brown	PTT
8	Signal Ground (SG)	Brown	Ground

The following shows a sample configuration for an LMR voice port that is configured for COR/COS operated signaling.

In this example, type { 2 | 3 | 5 } typically is type 3, but see [Figure 3-3 on page 3-5](#), [Figure 3-4 on page 3-6](#), and [Figure 3-5 on page 3-7](#) to select the type that best matches your radio requirements. Input gain { -27 - 16 } typically is 10, but adjust this value as needed to best receive audio on Cisco IPICS endpoints. Output attenuation { -16 - 27 } typically is 10, but adjust this value as needed to best receive audio on radios. When connecting a radio to a voice port in an LMR gateway, you may need to make adjustments to properly balance the audio levels. A radio typically provides gain adjustments, and the level of the signal from the radio to the voice port and the level of the signal from the voice port to the radio may require some adjustments on the radio and the voice port. When using a tone controlled radio, it is important to note that the tones that are sent from the LMR gateway to the radio also are affected by the voice ports output attenuation settings. When optimizing these settings to achieve the desired audio levels, take care to ensure that the voice port adjustments do not have an adverse effect on the level and quality of the tone signals.

```
voice class permanent 1
  signal timing oos timeout disabled
  signal keepalive disabled
  signal sequence oos n4o-action
!
voice-port 0/2/0
  voice-class permanent 1
  auto-cut-through
  operation 4-wire
  type { 2 | 3 | 5 }
  signal lmr
  lmr m-lead audio-gate-in ! RX audio IP packets only sent when this lead is active.
```

```
lmr e-lead voice
bootup e-lead off
lmr duplex half
lmr led-on
input gain { -27 - 16 }
output attenuation { -16 - 27 }
no echo-cancel enable
no comfort-noise
timeouts call-disconnect 3
timeouts wait-release 3
timing hookflash-in 0
timing hangover 80
connection trunk 101
description COR/COS Operated Voice Port
threshold noise -40
!
dial-peer voice 101 voip
destination-pattern 101
session protocol multicast
session target ipv4:239.193.1.1:21000
codec g711ulaw
```

## DSP Channel Optimization and Allocation

Follow these recommendations for optimizing DS0 channels and DSP channels:

- So that digital signal processors (DSPs) can be shared, first enable dspfarm, and make sure that all modules are participating in the network clock.
- When you enable dspfarm, you add specific voice cards to the DSP resource pool. This configuration allows several interface cards to share the installed DSP resources. (DSPs can be shared among digital modules or ports (such as T1/E1) and the motherboard, but DSPs cannot be shared among analog ports (such as an FXS)).
- At a minimum, you should enable one dspfarm.
- After the dspfarm is enabled on all modules that have DSPs installed, and all modules are participating in the main network clock, Cisco IOS interacts with these DSPs as part of the DSP resource pool.

To help calculate the DSPs that you need for your configuration, see *High-Density Packet Voice Digital Signal Processor Modules*, which is available at the following URL:

[http://www.cisco.com/en/US/products/hw/modules/ps3115/products\\_qanda\\_item0900aecd8016c6ad.shtml](http://www.cisco.com/en/US/products/hw/modules/ps3115/products_qanda_item0900aecd8016c6ad.shtml)

For detailed information about configuring DSP farms, see the “Configuring the Cisco IPICS RMS Component” appendix in *Cisco IPICS Server Administration Guide* for this release.

## Important Considerations When Deploying Cisco IPICS with Tone Controlled Radios

This section contains information about important considerations that you need to be aware of when you deploy Cisco IPICS with tone controlled radios. It includes the following topics:

- [Understanding Tone Control Signaling in Cisco IPICS, page 3-13](#)
- [Tone Signaling with Radios, page 3-15](#)

- [Using the IDC with a Tone Controlled Radio Channel, page 3-18](#)
- [Requirements for Tone Remote Radio Configuration in a Cisco IPICS Deployment, page 3-19](#)
- [Understanding Descriptor Files, page 3-20](#)
- [Providing Tone Sequences to Radios Without Using the Cisco IPICS Tone Remote Feature, page 3-23](#)
- [Tone Controlled Radio Channels in VTGs, page 3-25](#)
- [Troubleshooting Techniques, page 3-25](#)
- [IDC Caveats, page 3-38](#)

## Understanding Tone Control Signaling in Cisco IPICS

When a Cisco IPICS deployment includes tone controlled radios, Cisco IPICS endpoints can perform radio control functionality by using the native tone remote control feature in Cisco IPICS or by manually configuring Cisco IOS software to inject inband audio tone sequences. This section includes information about each of these methods in the following topics:

- [Using the Native Functionality in Cisco IPICS for Tone Remote Control, page 3-13](#)
- [Manually Configuring Cisco IOS for Injection of Inband Audio Tone Sequences, page 3-14](#)

### Using the Native Functionality in Cisco IPICS for Tone Remote Control

Cisco IPICS integrates the tone remote control feature to enable the IDC to send predefined RFC 2833 packets to the multicast address that you configured in the LMR gateway router. (This multicast address is assigned to the actual voice port in the LMR gateway router to which the radio network tone control interface connects.) The RFC 2833 packets represent tone sequences that you define in the Cisco IPICS server by using descriptor files. These descriptor files are well formed XML documents that you upload to the Cisco IPICS server and assign to the desired radio channels via the Administration Console. This configuration enables a radio channel on the IDC to use the channel selector (function) buttons that have been assigned to the user.

Figure 3-6 describes this sequence:

1. The descriptor file gets uploaded to the Cisco IPICS server.
2. When the IDC user presses a channel selector button or the PTT channel button, the configured RFC 2833 packet is sent to the LMR gateway.
3. The LMR gateway sends the corresponding inband audio tone to the device that is connected to the ear and mouth (E&M) port.

**Figure 3-6** IDC Tone Remote Control Sequence



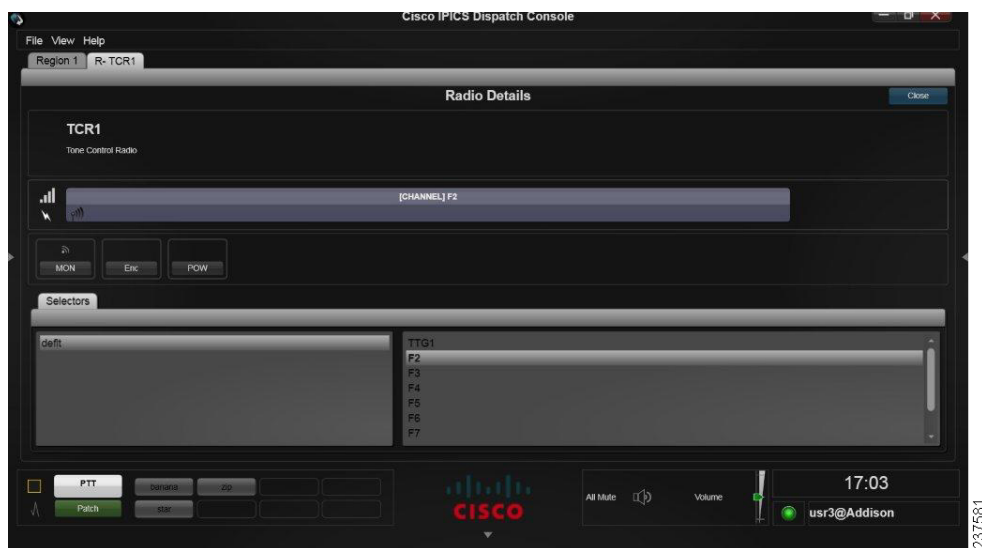
Figure 3-7 shows an illustration of an IDC radio channel that is configured with the name Kenwood-CPI. This example shows an active channel with the KENF1 channel selector button depressed.

In this example, KENF1 and F2 are the channel selector function buttons and On/Off, MON, and High/Med/Low (POW) are the control function buttons.


**Note**

Based on the configuration of the POW control function in the descriptor file, this control may display as three power selector buttons (High/Med/Low).

**Figure 3-7 IDC Radio Channel**



## Manually Configuring Cisco IOS for Injection of Inband Audio Tone Sequences

In addition to the features that are included in Cisco IPICS, you can manually configure Cisco IOS to inject inband audio tones. This configuration can be performed directly on the E&M voice port of the radio or by using DS0 loopbacks to insert inband tones whenever the left side of the loopback receives multicast audio.

Figure 3-8 illustrates the sequence when the tone signal configuration is assigned to the radio E&M voice port. In this case, the tones are output toward the connected device whenever it receives a multicast stream.

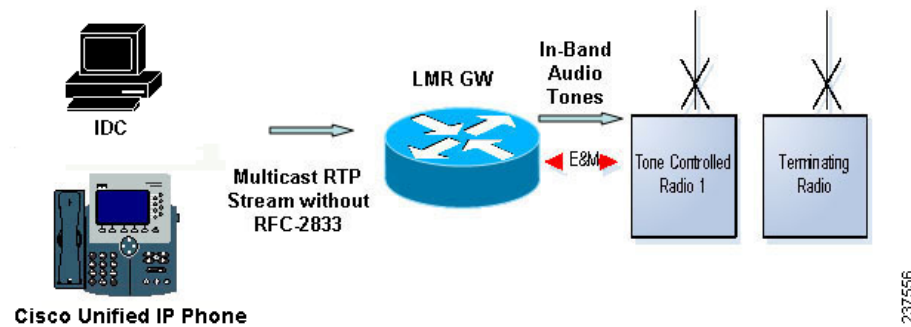
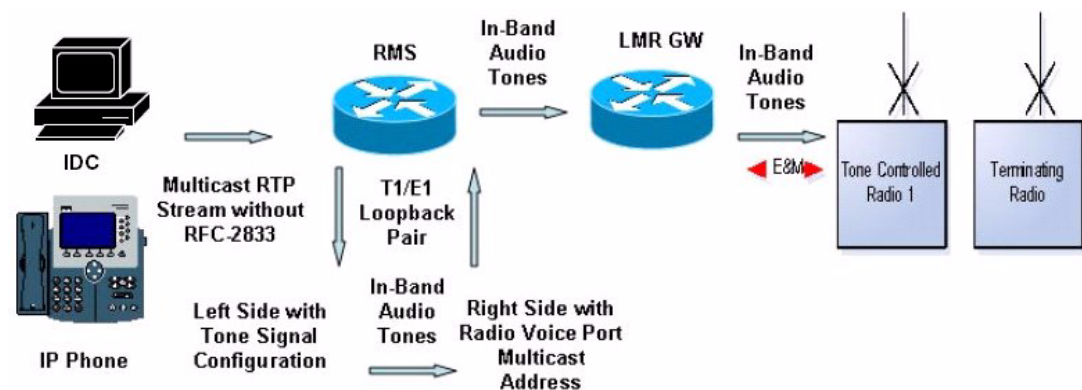
**Figure 3-8** Manual Cisco IOS Tone Signal Sequence

Figure 3-9 illustrates the sequence when the tone signal configuration is assigned to the left side of a DS0 loopback. In this case, the tones are output toward the loopback cable to the right side of the loopback and then to the multicast address of a tone controlled radio as inband audio.

**Figure 3-9** Tone Signal Configuration with DS0 Loopback

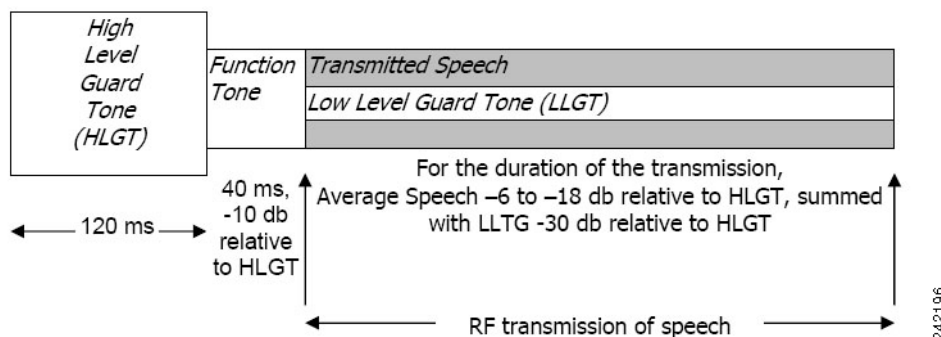
Both scenarios, as shown in Figure 3-8 and Figure 3-9, enable Cisco IPICS endpoints to select a Cisco IPICS channel that is associated to the left side of the loopback; when these endpoints transmit, the appropriate tones can be inserted and sent to the required radio.

## Tone Signaling with Radios

Many conventional radio systems use inband tone signaling to indicate activity, key the transmitter, and control channel selection. (Inband audio refers to audio that is included in the normal voice transmission.) The Cisco LMR gateway can be configured to generate these tones to control the radio. There are typically three phases of tone signaling:

- Wakeup tone/High Level Guard Tone (HLGT)—A tone of a specific duration and frequency that acts as a preamble to base stations to indicate that additional signaling is coming.
- Frequency selection (or control) tone/Function tone—One of a range of tones that is used to select a frequency (channel) for the audio.
- Guard tone/Low Level Guard Tone (LLGT)—A tone of a specific frequency that is maintained while there is activity on a channel. This tone indicates that the channel has been seized.

Figure 3-10 illustrates a typical tone sequence.

**Figure 3-10** Typical Tone Sequence

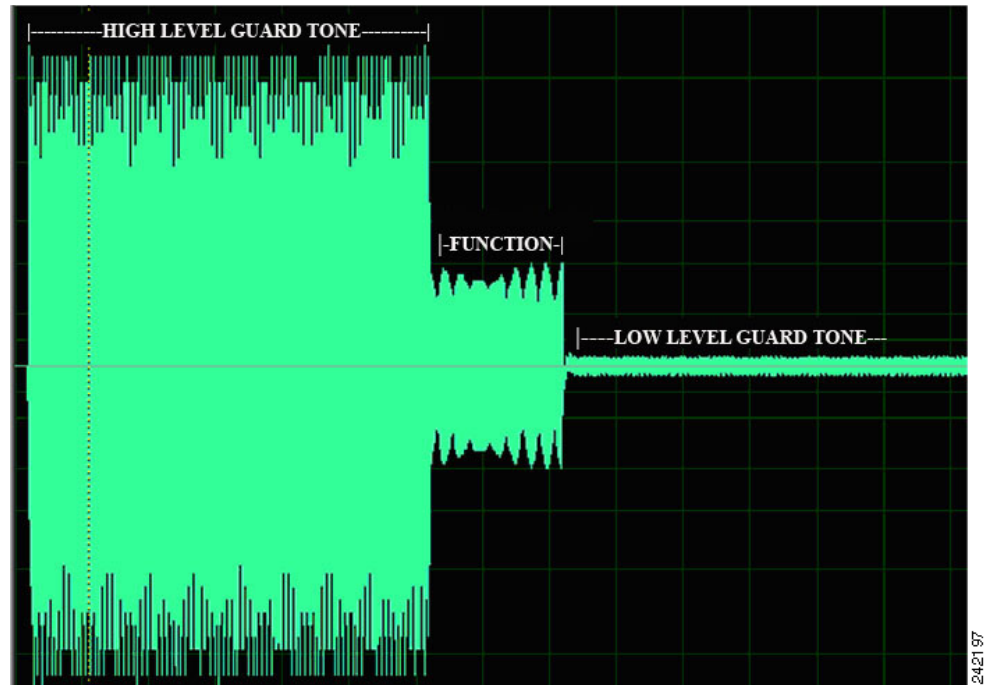
To eliminate the need for inband audio tones to be passed across the IP network, this feature provides the capability to inject tones at the Cisco LMR gateway E&M router voice port that is connected directly to the tone control interface of the radio network.

Static tone injection is one fixed sequence of single tones, with no more than ten tones or pauses in a given sequence, that is used on all transmissions from the voice port to the attached radio system. Static tone injection begins with E-lead activity and ends when the hangover time expires on voice playout. Hangover time ensures that all buffered audio plays out before the Cisco LMR gateway unkeys the radio.

The tone sequence comprises a combination of the following tones:

- Single tone—Of fixed frequency, duration, and amplitude.
- Pause—Of fixed duration.
- Guard tone—Of fixed frequency and amplitude. Plays out with the audio for the duration of the voice packet.
- Idle tone—Plays out in the absence of voice packets. Idle tone and guard tone are mutually exclusive.

Figure 3-11 illustrates a sample tone sequence, as viewed by using the analysis capability in Cool Edit Pro/Adobe Edition. It shows an example of a tone sequence that consists of a High Level Guard Tone, Function Tone, and Low Level Guard Tone (keying tone).

**Figure 3-11**      *Sample Tone Sequence*

With Cisco IPICS, the RFC 2833 packets that the IDC sends get converted to this type of audio tone sequence by the LMR gateway. When you use IP phones or other forms of manually configured tone signaling, the audio tones that generate are the result of the explicit manual configuration that is required to generate the audio tones. These tones can be assigned to a voice port by using the **voice class tone-signal** command in Cisco IOS.

If you configure injected tones, make sure to use the **timing delay-voice tdm** command to configure a delay before the voice packet is played out. Configuring a delay prevents injected tones from overwriting the voice packet. The delay must be equal to the sum of the durations of the injected tones and pauses in the tone-signal voice class.

Table 3-4 lists common tone control frequencies.

**Table 3-4**      *Common Tone Control Frequencies*

Tone Frequency	Function Tone	Relative Levels	Tone Duration
2175 Hz	Wake Up	+10 dB	120 msec
1950 Hz	Transmit F1	0 dB	40 msec
1850 Hz	Transmit F2	0 dB	40 msec
1750 Hz	Transmit F7	0 dB	40 msec
1650 Hz	Transmit F8	0 dB	40 msec
1550 Hz	Wildcard	0 dB	40 msec
1450 Hz	Wildcard	0 dB	40 msec
1350 Hz	Transmit F3	0 dB	40 msec
1250 Hz	Transmit F4	0 dB	40 msec
1150 Hz	Transmit F5	0 dB	40 msec



Table 3-4 Common Tone Control Frequencies (continued)

Tone Frequency	Function Tone	Relative Levels	Tone Duration
1050 Hz	Transmit F6	0 dB	40 msec
2050 Hz	CTCSS Monitor	0 dB	40 msec
2175 Hz	Guard Tone	-20 dB	Duration of PTT

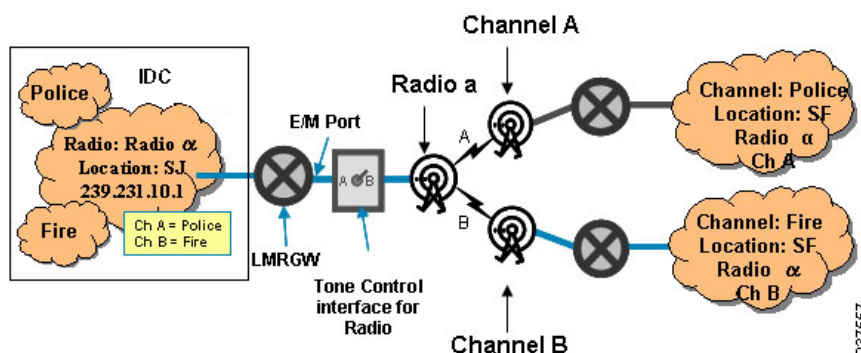
**Note**

If the E&M port is the only device that is connected to the tone control panel for the radio, either 2-wire or 4-wire configurations are supported. If there are devices other than a single E&M port connected to the tone control panel, only 2-wire tone control configurations are supported. If you try to introduce a Cisco IPICS E&M 4-wire configuration into an environment with multiple connections, such as existing consoles, the IDC may not be able to hear the console transmitting and the console may not hear the IDC transmitting. Cisco recommends that you use 2-wire tone control where possible because it provides a more robust solution.

## Using the IDC with a Tone Controlled Radio Channel

In Figure 3-12, the left side of the illustration represents an IDC with a radio channel that has channel selectors for the Fire and Police channels on the radio that are shown on the right side.

Figure 3-12 IDC with Tone Controlled Radio Channel



In this example, the IDC user has an active radio channel (Radio a) with a descriptor that provides channel selector buttons for Police and Fire. When the IDC user presses a channel selector button, the corresponding tone sequence, as defined in the descriptor, gets sent as RFC 2833 packets in the Real-Time Transport Protocol (RTP) stream to the configured multicast address.

If the dial peer for the E&M port that is assigned to the multicast address has been properly configured with the **payload type** commands, the LMR gateway interprets the RFC 2833 packets and sends the corresponding tone sequence, as audio, to the device that is connected to the E&M port.

To enable the LMR gateway to interpret the RFC packets that the IDC sends, configure the following commands on the dial peer that is assigned to the voice port that is connected to the tone controlled radio:

```
Router(config-dial-peer)# rtp payload-type nte-tone 108
Router(config-dial-peer)# rtp payload-type lmr-tone 107
```

When the connected device receives the tone sequence, it responds accordingly. That is, if it has been configured to perform a particular function when it receives that tone sequence, it will do so.



**Note**

In addition to sending the RFC 2833 packets when the channel selector button is pressed, the IDC also sends the RFC 2833 packets on the currently selected channel when the PTT button is pressed. The exact behavior is determined by the descriptor file definitions. More specifically, the actions that you define in the “tune” element occur when the selector is pressed. The actions that you define in the “begintransmit” element occur when the PTT button is pressed. It is typical to define tone sequences in the following way:

- tune = HLGT + rfc2833tone
- begintransmit = HLGT + rfc2833tone + LLGT

## Requirements for Tone Remote Radio Configuration in a Cisco IPICS Deployment

Table 3-5 describes the items that are required for the various tone controlled radio scenarios in a Cisco IPICS deployment. See Table 3-6 and Table 3-7 for a preinstallation form that includes the information that must be provided by the Cisco IPICS integrator and by the radio team.

**Table 3-5** Required Items for Tone Controlled Radio Scenarios

Configurable Item	When Required	Use Cases
Descriptor file	For any tone controlled radio that IDC users control	IDC users who perform radio control functions.
E&M voice port	For interfacing to any radio	All Cisco IPICS deployments with radios require configuration of voice ports to match the radio interface.
E&M voice port dial peer	For interfacing to any radio	All Cisco IPICS deployments with radios require configuration of a dial peer to establish multicast connectivity to the IP network.
E&M voice port dial peer with the <b>rtp payload-type</b> command defined	For any tone controlled radio that the IDC users control	Cisco IPICS deployments with tone controlled radios require configuration of a dial peer to establish multicast connectivity to the IP network, with the <b>rtp payload type</b> commands, when RFC 2833 packets are sent by IDC clients that perform tone control functions.
Tone signal definition	For any tone controlled radio that is controlled by inband audio tone sequences that you define and which are not generated by the LMR gateway as the result of RFC 2833 packets sent by an IDC.	Use tone signal configuration to assign tone sequences to voice ports to enable the injection of inband audio tones into the stream. When no RFC 2833 packets are received, you can perform this configuration on the E&M port or on a DS0 loopback to enable a received multicast stream to cause the tones to be injected through the loopback toward the multicast address that is associated with the voice port, which the tone controlled radio is connected to.

**Table 3-5** Required Items for Tone Controlled Radio Scenarios (continued)

Configurable Item	When Required	Use Cases
Manually configured DS0 loopbacks	For inband audio tone sequences that need to be generated as the result of a Cisco IPICS user sending a multicast stream without RFC 2833 packets.	Use for a Cisco IPICS IP phone user, or an IDC user with a regular channel, to transmit toward a multicast channel that is received at one side of a loopback. This action results in the tones being injected and sent toward the other side of the loopback. The other side of the loopback is assigned to a multicast address that is being used by a voice port connected to a tone controlled radio.

## Understanding Descriptor Files

Tone descriptor files are well formed XML documents. You upload these documents to the Cisco IPICS server and associate them to radio channels. Cisco IPICS uses these descriptor files to determine which buttons to display on the IDC radio channel and the functionality that each button performs. Uploaded descriptor files reside in the Cisco IPICS database.

By default, the Cisco IPICS installation includes several sample descriptor files. This section references content from the sample file called CPIExample.xml.

Use the following guidelines and references to understand how to properly define the elements within a Cisco IPICS descriptor file:

- All Cisco IPICS descriptor files should begin with the following version and encoding statement:  
`<?xml version="1.0" encoding="UTF-8"?>`
- Cisco IPICS descriptor files should include the following entries with a “name” attribute that defines the descriptor name. This name displays in the descriptor window in the Cisco PICS Administration Console:  
`<ipics:RadioTypeDescriptor xmlns:ipics="urn:com.cisco.ipics.RadioDescriptor" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:schemaLocation="urn:com.cisco.ipics.RadioDescriptor ../RadioDescriptor.xsd" name="CPI Example">`

### Commands

The Commands tag defines the reusable CommandRefs that can be used throughout the descriptor file. For example, if the High Level Guard Tone (HLGT) is always going to be a 2175 Hz signal at 0 dB for 120 ms, you can define a command with an ID of “hlgt.” The “hlgt” CommanRef can then be used throughout the Channel tags to indicate that it is the desired tone to be used.

```
<Commands>
  <Command id="hlgt">
    <Rfc2833Tone db="0" duration="120" frequency="2175" />
  </Command>
  <Command id="llgt">
    <Rfc2833Tone db="-30" duration="0" frequency="2175" />
  </Command>
  <Command id="dtmf-5">
    <Rfc2833Event db="-30" duration="20" event="5" />
  </Command>
</Commands>
```

### ChannelSelectors

ChannelSelectors represent the different channels/frequencies/channel selector buttons that the radio supports. That is, if a specific radio can tune to eight channels, eight ChannelSelector elements should display, with each element describing the tones that are required to tune to its respective channel. In addition to describing the tones that are required to tune the channel, you must also describe the tones that should play out before every transmission on that radio channel. These tones are usually referred to as the low level guard tones (LLGT).

The following elements are included within the ChannelSelectors tag:

- ChannelSelector—Represents a single channel on the radio and supports the following required attributes:
  - Label—Specifies a unique identifier that pertains to the channel.
  - Action—Groups a sequence of Commands and CommandRefs. A channel selector supports two types of action elements: tune and begintransmit.

The tune action tones play out when the IDC user selects the ChannelSelector from the IDC.

The begintransmit action tones play out when the IDC user transmits (pushes the PTT button) on the radio.

Required attributes: type = tune or begintransmit

- DefaultChannelSelector (optional)—When the IDC first receives a radio talkgroup from the server, it does not know which ChannelSelector the radio is tuned to. However, to transmit on this “unknown” channel, the LMR gateway may still require a low level guard tone before every transmission. The IDC always sends the DefaultChannelSelector begintransmit tones if it cannot detect the tuned channel.

The following example shows a portion of the CPIExample descriptor file ChannelSelectors elements, including DefaultChannelSelector, F1, and Scan:

```
<ChannelSelectors>
  <DefaultChannelSelector>
    <Action type="begintransmit">
      <CommandRef href="hlgt" />
      <CommandRef href="llgt" />
    </Action>
  </DefaultChannelSelector>

  <ChannelSelector label="F1">
    <Action type="tune">
      <CommandRef href="hlgt" />
      <Command>
        <Rfc2833Tone db="-10" duration="40" frequency="1950" />
      </Command>
    </Action>
    <Action type="begintransmit">
      <CommandRef href="hlgt" />
      <Command>
        <Rfc2833Tone db="-10" duration="40" frequency="1950" />
      </Command>
      <CommandRef href="llgt" />
    </Action>
  </ChannelSelector>
  <ChannelSelector label="SCAN">
    <Action type="tune">
      <CommandRef href="hlgt" />
      <Command>
        <Rfc2833Tone db="-10" duration="40" frequency="1050" />
      </Command>
    </Action>
```

```

    <Action type="begintransmit">
      <CommandRef href="hlgt" />
      <Command>
        <Rfc2833Tone db="-10" duration="40" frequency="1050" />
      </Command>
      <CommandRef href="llgt" />
    </Action>
  </ChannelSelector>
</ChannelSelectors>

```

### Control Functions

The following example shows a portion of the ControlFunctions elements, including, Enc and POW in the CPIExample descriptor files:

```

<ControlFunctions>
  <Stateful shortName="Enc" longName="Encryption"
    description="Enable/Disable OTA Encryption"
    presentation="multiple">
    <State shortName="On">
      <Action type="pressed">
        <Command>
          <Rfc2833Tone db="-30" duration="20"
            frequency="1105" />
        </Command>
      </Action>
    </State>
    <State shortName="Off">
      <Action type="pressed">
        <Command>
          <Rfc2833Tone db="-30" duration="20"
            frequency="1110" />
        </Command>
      </Action>
    </State>
  </Stateful>
  <Stateful shortName="POW" longName="Power"
    description="High/Medium/Low Transmit Power"
    presentation="multiple">
    <UnknownState shortName="PUkwn" longName="Power Unknown"
      description="The power is in an unknown state" />
    <State shortName="High">
      <Action type="pressed">
        <Command>
          <Rfc2833Tone db="-30" duration="20"
            frequency="1115" />
        </Command>
      </Action>
    </State>
    <State shortName="Med">
      <Action type="pressed">
        <Command>
          <Rfc2833Tone db="-30" duration="20"
            frequency="1120" />
        </Command>
      </Action>
    </State>
    <State shortName="Low">
      <Action type="pressed">
        <Command>
          <Rfc2833Tone db="-30" duration="20"
            frequency="1125" />
        </Command>
      </Action>
    </State>
  </Stateful>

```

```
        </Action>
      </State>
    </Stateful>
  </ControlFunctions>
```

## Providing Tone Sequences to Radios Without Using the Cisco IPICS Tone Remote Feature

In addition to the IDC tone remote feature implementation in Cisco IPICS, you can also leverage Cisco IOS to send tone sequences as inband audio in an RTP stream. This approach can be used in Cisco IPICS deployments with, or instead of, the Cisco IPICS native tone remote capabilities.



### Note

Although it is possible to mix the Cisco IPICS IDC tone remote feature with manually defined tone configurations, care must be taken to fully understand the limitations and caveats before you do so.

The following sections describe how to deploy, and interface to, various types of radios, including those that are tone controlled. For information about caveats, see the [“Caveats” section on page 3-24](#). For information about how to configure Cisco IOS to enable the insertion of tone sequences in the multicast stream by leveraging loopbacked DS0s, see the [“2-Wire Tone Control Configuration for Two-Ten Frequencies” section on page 3-42](#).

In a Cisco IPICS deployment, you may have a need to allow a Cisco IPICS user to transmit to a tone remote controlled radio from an IP phone by using the Cisco IPICS XML client. Because the IP phone does not support sending RFC 2833 packets, you can manually configure the insertion of the required tones as inband audio by using DS0 loopback ports.

For example, an IP phone user with assigned channels that are configured with the required loopback and tone signal configuration can select a channel and key the radio when they transmit on the corresponding channel. To switch channels, the IP phone user simply selects another configured channel that also has the corresponding manual loopback configuration, and transmits on that channel. This approach enables Cisco IPICS users to control tone controlled radio networks without using RFC 2833 packets.

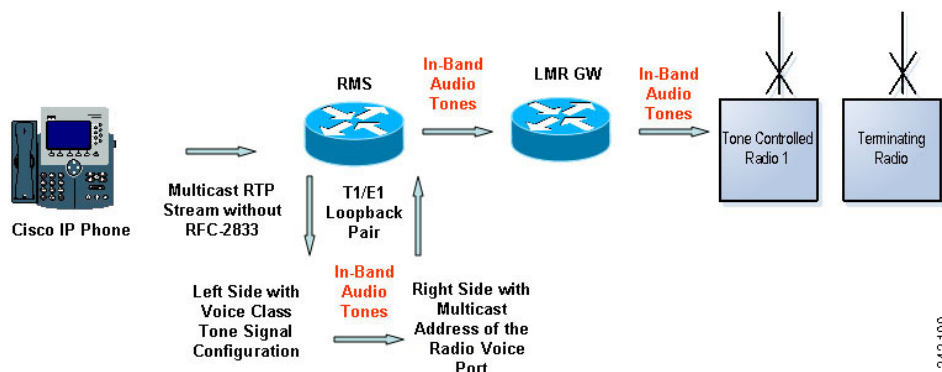
[Figure 3-13](#) illustrates an IP phone user sending audio on a channel.

1. The audio is received on a router that has DS0 loopbacks configured (in this example, the router is an RMS).
2. The channel (in Cisco IPICS) is assigned the same multicast address as the left side of the loopback.
3. When the audio is received on the left side of the loopback pair, the associated voice port tone signal commands cause the desired inband tone sequence to be sent out the loopbacks TDM interface.
4. The tones are received on the right side of the loopback pair.
5. This audio stream now contains the desired inband audio that gets sent to the right side multicast address.
6. The right side multicast address should match the address that is configured on the radio voice port.
7. The static tone sequence gets sent to the connected tone controlled radio, which causes it to select the corresponding channel and key the radio transmit.



### Note

Care should be taken to ensure that the tones are inserted as close to the LMR gateway as possible to avoid transmitting the tones across a WAN link or experiencing other topology-related degradation.

**Figure 3-13 Audio From IP Phone User**

This approach can be implemented with multiple channels and loopback pairs to enable IP phone users, remote IDC users, and non-multicast IDC users to select and key multiple channels on a tone controlled radio.

The following configurations are required to support the use case that is described in [Figure 3-13](#):

- Define the Cisco IPICS channel and assign it a multicast address.
- Assign the channel to a Cisco IPICS user.
- In the RMS or another LMR-enabled router, manually configure a pair of DS0s in a loopback configuration to insert tones toward the radio multicast address.

**Note**

For specific configuration details that are required for the manual loopback configuration, see the [“Tone Signaling with Radios”](#) section on page 3-15.

**Caveats**

Be aware of the following caveats when you use this approach:

- This approach actually sends inband audio tones. Therefore, it is more susceptible to network topology considerations than the RFC 2833 implementation that is used by the Cisco IPICS IDC in conjunction with the LMR gateway running a supported version of Cisco IOS. For the most updated information about the versions of Cisco IOS that Cisco IPICS supports, refer to *Cisco IPICS Compatibility Matrix*.
- If you use an RMS to provide the static configured loopback pairs, the corresponding DS0s must be disabled and marked as reserved in the Cisco IPICS Administration Console for that RMS.
- It is important to note that when you use this approach in conjunction with the Cisco IPICS tone remote IDC, the IDC clients do not have the capability to reflect channel changes that were initiated by IP phone users. Be sure that this limitation with a mixed implementation is fully understood.
- When an IDC user presses a channel selector button on a radio channel, all other (non-remote) IDC clients with the same active radio channel, receive the RFC 2833 packets and update their channel selector indicators accordingly.

## Tone Controlled Radio Channels in VTGs

In certain situations, the tones that are required to key a radio do not get sent if more than one radio channel is included in a VTG. Therefore, consider the following key points when you add multiple radio channels to a VTG and see the [“VTG Caveats” section on page 3-25](#).

- When a Cisco IPICS IDC uses a radio channel, it transmits RFC 2833 packets on its configured multicast address. These packets should arrive at the LMR gateway that hosts the E&M voice port that is connected to the tone controlled radio. In this scenario, the LMR gateway interprets the RFC 2833 packets and sends the corresponding tones to the connected device (on the E&M port).
- In addition to the voice port, the RMS that hosts the VTG loopbacks also receives the RFC 2833 packets from the IDC. However, when the loopbacks are used to mix the received RTP stream to the other multicast addresses in the VTG, the RFC packets are lost. That is, the RFC 2833 packets that the IDC transmits are not sent to devices that are listening to any other radio channels in the VTG. The result is that the LMR gateway does not insert the tones that are required to key those radios.

To ensure that the tones are generated to key the radios, you can manually configure the radio voice ports. This configuration requires that you assign a **voice class tone-signal** configuration to the voice port to which the radio is connected. This configuration must include the tone sequence that is required to key the radio.

In some cases, the radio can be keyed on the currently selected channel. In other cases, the tone sequence must include a channel selector function tone. If a function tone is required, that radio may only use a specific channel when it is in a VTG with another radio.

### VTG Caveats

Be aware of the following caveats that pertain to VTGs:

- The radio must be programmed for a keying sequence that does not include a function tone for channel selection, or the tone sequence must contain a static channel selection sequence, which limits that radio base station, when it receives audio from another device in a VTG, to use one particular channel.
- The Cisco IOS gateway software gives precedence to the RFC 2833 packets over a manual configuration when both are present. This means that while it is acceptable to have both, make sure that all participants fully understand the potential effects of this scenario.

## Troubleshooting Techniques

When you debug issues with tone controlled radios in a Cisco IPICS deployment, the most important step is to establish that the integrity of the tones that are sent to the connected tone controlled radio network match what the radio expects.

The Cisco IPICS integrator is responsible for proving that the tone sequence is correctly provided at the point of demarcation. This point should be the electrical interface of the E&M voice port. To do so, the integrator must be able to capture audio streams for analysis.

You can use the following technique to confirm that the required tone sequence is present at the E&M interface.

When interfacing to the tone control interface of a radio system, you must know which tone sequences are required to control the radio functions.

See [Table 3-6](#) and [Table 3-7](#) for a preinstallation form that you can use to document the details that are required to deploy a radio in Cisco IPICS. One part of the form requires input from the Cisco IPICS integrator and the other part of the form requires input from the party who is responsible for the radios. Complete this form for each radio that you want to deploy.

**Table 3-6** *Cisco IPICS Preinstallation Form for Tone Control Radios—Cisco IPICS Integrator*

Item	Provided by the Cisco IPICS Integrator
<b>Cisco IPICS Configuration Information</b>	
Cisco IPICS radio name	
Cisco IPICS channel name	
Descriptor file name	
Location	
<b>LMR Gateway Configuration Information</b>	
Voice-port	
Dial-peer	
Destination pattern	
Multicast address	

**Table 3-7** *Cisco IPICS Preinstallation Form for Tone Control Radios—Radio Team*

Item	Provided by the Radio Team
<b>LMR Gateway Configuration Information</b>	
2/4-wire	
Signaling type (II, III, V)	
COR/COS or VAD	
<b>Tone Controlled Radio Details</b>	
Radio name	
HLGT frequency	
HLGT level	
HLGT duration	
LLGT frequency	
LLGT level	
Function 1 name	
Function 1 frequency	
Function 1 level	
Function 1 duration	
Function 1 sequence	
Function 2 name	



**Table 3-7** *Cisco IPICS Preinstallation Form for Tone Control Radios—Radio Team (continued)*

Item	Provided by the Radio Team
Function 2 frequency	
Function 2 level	
Function 2 duration	
Function 2 sequence	
Function 3 name	
Function 3 frequency	
Function 3 level	
Function 3 duration	
Function 3 sequence	
Function 4 name	
Function 4 frequency	
Function 4 level	
Function 4 duration	
Function 4 sequence	
Function 5 name	
Function 5 frequency	
Function 5 level	
Function 5 duration	
Function 5 sequence	
Function 5 name	
Function 6 name	
Function 6 frequency	
Function 6 level	
Function 6 duration	
Function 6 sequence	
Function 7 name	
Function 7 frequency	
Function 7 level	
Function 7 duration	
Function 7 sequence	
Function 8 name	

Table 3-7 Cisco IPICS Preinstallation Form for Tone Control Radios—Radio Team (continued)

Item	Provided by the Radio Team
Function 8 frequency	
Function 8 level	
Function 8 duration	
Function 8 sequence	
Function 9 name	
Function 9 frequency	
Function 9 level	
Function 9 duration	
Function 9 sequence	
Function 10 name	
Function 10 frequency	
Function 10 level	
Function 10 duration	
Function 10 sequence	
Function 10 name	

If all of the required details are implemented and the required Cisco IPICS configuration has been completed, but you do not see the desired effect, use the information in the following topics to capture the audio for analysis.

- [Hardware and Software Requirements, page 3-28](#)
- [Test Scenario, page 3-29](#)
- [Analyzing RTP Streams, page 3-30](#)

## Hardware and Software Requirements

These tests require that you use the following components:

- Laptop/PC with IP connectivity to the LMR gateway
- IDC
- Wireshark network protocol analyzer or other suitable sniffer tool
- Adobe Edition/Cool Edit Pro (Optional)
- SSH/telnet connectivity to the LMR gateway
- E&M crossover cable with the following RJ-45 connector wiring (this cable configuration can be used with a receive port, which is port 0/2/0 in the sample configuration shown below, that is set for 4-wire):

0/2/1

0/2/0

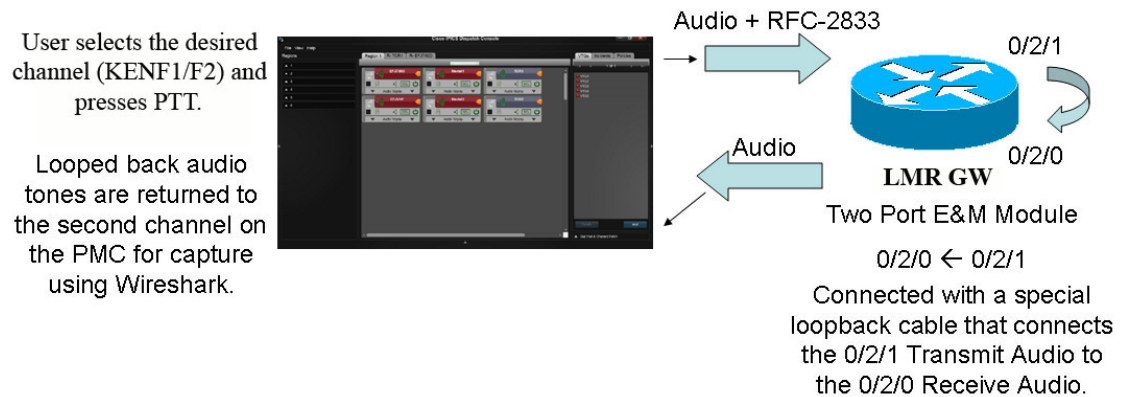
Voice Port Transmit R1: Pin 4 > Pin 3 Voice Port Receive R

Voice Port Transmit T1: Pin 5 > Pin 6 Voice Port Receive T

Figure 3-14 describes the setup that is required to verify that the IDC is properly sending RFC 2833 packets and that the LMR gateway is properly sending the corresponding tone sequence.

Placing a simple loopback cable between E&M ports enables a baseline measurement by using a test tone for calibration purposes, as well as actual LMR gateway generated tones. You use the PC to capture the IP packets by using a sniffer. Therefore, it is important to eliminate the IP network from this test by establishing local connectivity to a port on the LMR gateway.

**Figure 3-14 Setup to Verify Proper Tone Sequence Flow**



237558

## Test Scenario

To test this scenario, perform the following steps:

1. A non-remote IDC transmits on the radio channel. This transmission sends the RFC 2833 packets to the LMR gateway.
2. The LMR gateway receives the stream on port 0/2/1.
3. Because the **rtp payload-type** commands are defined on that dial peer for that port, the LMR gateway generates the corresponding audio tones toward the loopback cable. (High level guard tone, function tone, and low level guard tone bed on the configuration in the referenced descriptor file.)
4. The audio tones are output on the loopback cable and received on port 0/2/0 so that the inband audio tones are sent to the Test Channel 2 multicast address.
5. Because that channel is active on the IDC, the RTP stream that is sent to 239.192.105.100 can be captured by using a sniffer on the IDC client.
6. After you capture the audio, it can be analyzed.

See the below example for the voice port and dial peer configuration that is used for this test scenario.

Port 0/2/0 specifies the receive port:

```
voice-port 0/2/0
voice-class permanent 1
auto-cut-through
operation 4-wire
type 3
signal lmr
lmr e-lead voice
lmr duplex half
lmr led-on
input gain 1
```

```

output attenuation 1
no echo-cancel enable
no comfort-noise
timeouts call-disconnect 3
timing hookflash-in 10
timing hangover 80
connection trunk 50100
threshold noise -40

dial-peer voice 55550100 voip
destination-pattern 50100
session protocol multicast
session target ipv4:239.192.105.100:21000
codec g711ulaw
vad aggressive

```

Port 0/2/1 specifies the transmit port:

```

voice-port 0/2/1
voice-class permanent 1
auto-cut-through
operation 4-wire
type 3
signal lmr
lmr e-lead voice
lmr duplex half
lmr led-on
input gain 1
output attenuation 1
no echo-cancel enable
no comfort-noise
timeouts call-disconnect 3
timing hookflash-in 0
timing hangover 80
connection trunk 50101
threshold noise -40

dial-peer voice 55550101 voip
destination-pattern 50101
rtp payload-type lmr-tone 107
rtp payload-type nte-tone 108
session protocol multicast
session target ipv4:239.192.105.101:21000
codec g711ulaw
vad aggressive

```

## Analyzing RTP Streams

The above test scenario deploys the sniffer on the IDC client. Therefore, we expect that both of the multicast streams should be present in the capture as a result of the IDC performing Internet Group Management Protocol (IGMP) joins for both of the active channels.

To capture a stream, perform the following procedure:

### Procedure

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Start a capture on the sniffer.  |
| <b>Step 2</b> | Press the radio channel PTT button on the IDC and send a short audio stream. |
| <b>Step 3</b> | Stop the capture.  |

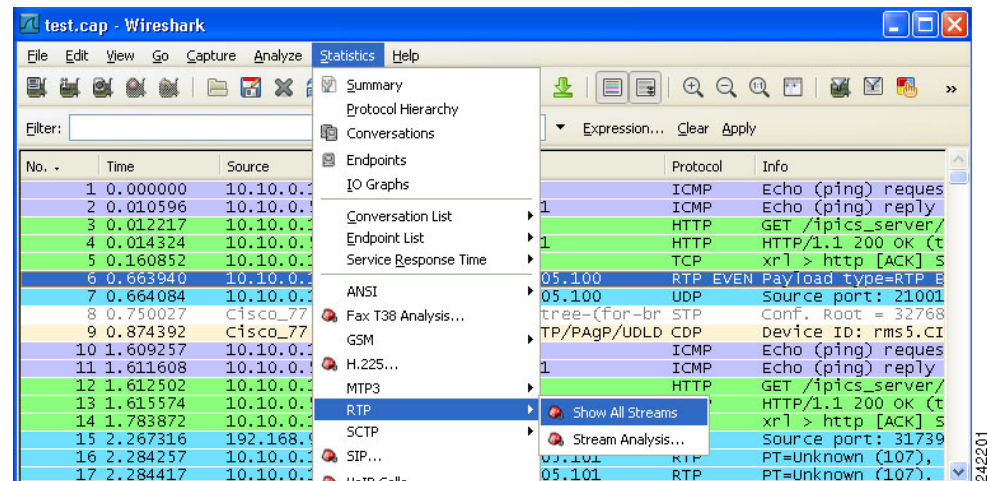
**Step 4** With the desired capture results visible in Wireshark, choose **Statistics > RTP > Show All Streams**. A pop-up window displays with all of the RTP streams that are available in the capture.

In our example, you can see one stream for each of the destination addresses:

239.192.105.100

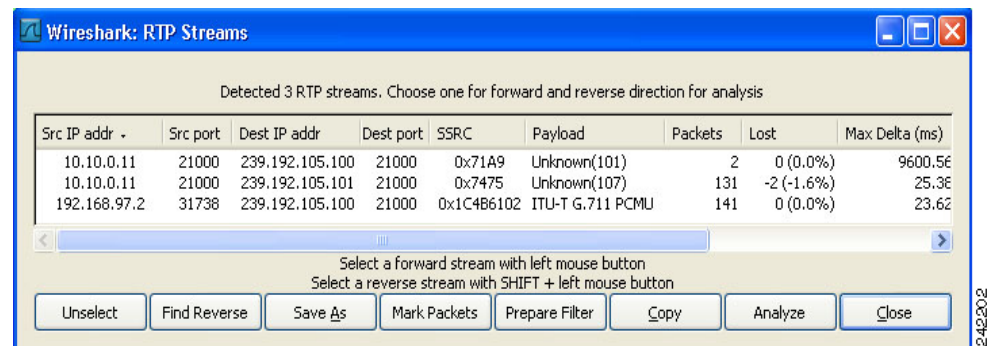
239.192.105.101

**Figure 3-15** *Wireshark Statistics Window*



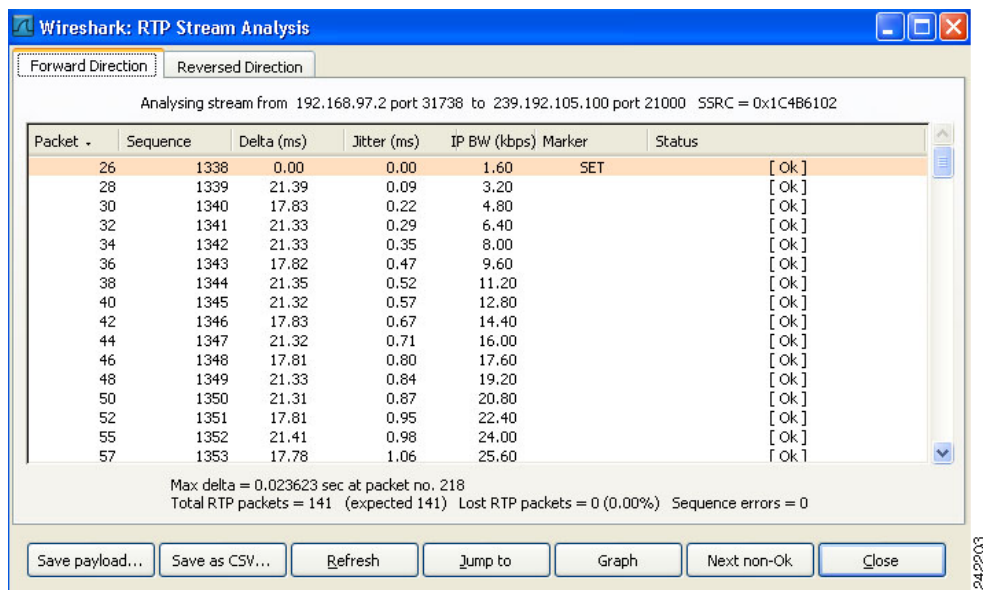
**Step 5** Click to select the **239.192.105.100** stream that shows the correct codec in the payload column; then, click **Analyze**.

**Figure 3-16** *Wireshark RTP Streams Window*



**Step 6** Click **Save payload**, as shown in Figure 3-17.

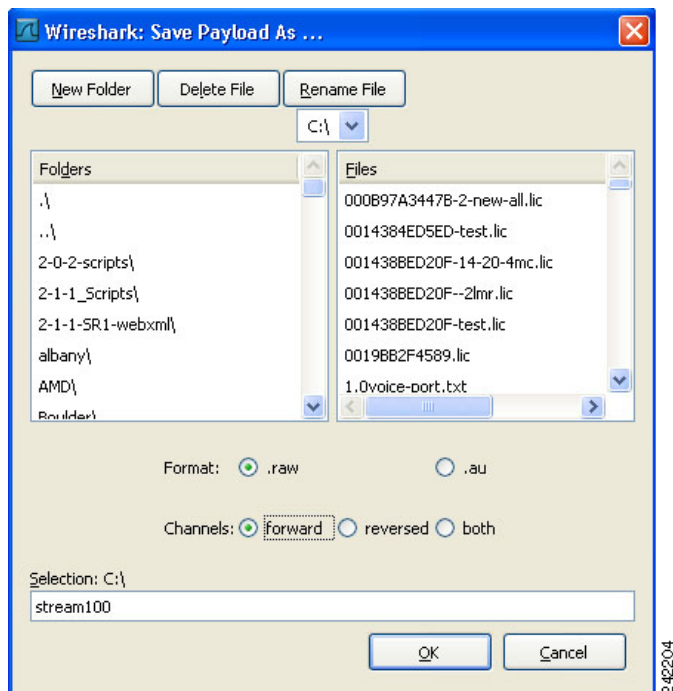
Figure 3-17 Wireshark RTP Stream Analysis Window



**Step 7** Navigate to the desired folder to save the file by following these steps, as shown in Figure 3-18:

- In the Format field, click the **.raw** radio button
- In the Channels field, click the **forward** radio button
- Enter a file name; then, click **OK**.

Figure 3-18 Wireshark Payload Window



The system creates a .raw file that you can analyze.

**Note**


To analyze the file, you must have an application such as Cool Edit Pro/Adobe Edition. With an application that allows for analysis of .raw files, you can establish the characteristics of the generated tones to determine if they are within the required tolerances. [Figure 3-24](#) shows a graphical representation of a .raw file with a captured tone sequence.

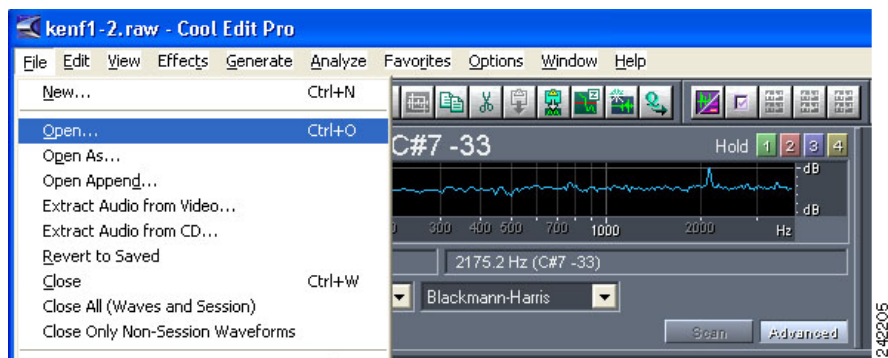
In addition to capturing the stream that the IDC/LMR gateway sent, you can also capture a tone that is generated by the LMR gateway to establish a baseline of the behavior of the looped-back ports.

To demonstrate this technique, you can use the following command on the LMR gateway to capture the resulting audio stream that was sent through the loopback to the 239.192.105.100 multicast address. This stream was used to generate a .raw file (in this example, test1k.raw) that was analyzed to determine that the expected behaviors did occur correctly.

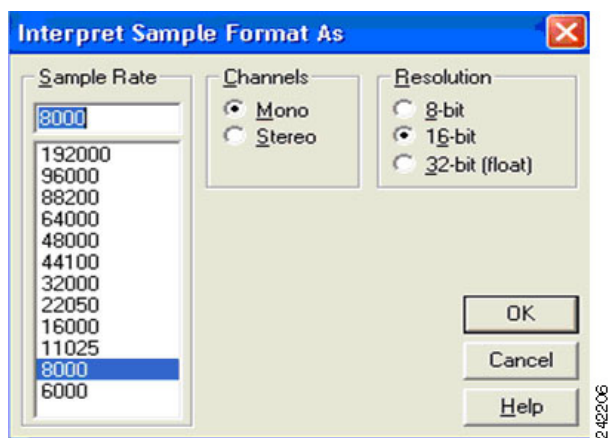
To capture a tone, perform the following procedure:

**Procedure**

- 
- Step 1** Start a capture on the sniffer.
- Step 2** To start the tone on the LMR gateway, enter the following Cisco IOS command from privileged EXEC mode on the LMR gateway where the E&M voice port is installed:
- ```
Router# test voice port 0/2/1 inject-tone local 1000hz
```
- where:
- 0/2/1* specifies the slot/subunit/port
  - local* directs the injected tone toward the local interface (near end)
  - 1000hz* injects a 1-kilohertz test tone
- Step 3** To stop the tone, enter the following command:
- ```
Router# test voice port 0/2/1 inject-tone local disable
```
- where:
- disable* ends the test tone
- 
-  **Note** Make sure that you enter the disable keyword to end the test tone when you have completed your testing.
- 
- Step 4** Stop the capture.
- Step 5** Perform [Step 2](#) and [Step 3](#) to generate a .raw file.
- Step 6** Open the file in Cool Edit by choosing **File > Open**; then, click to select the file, as shown in [Figure 3-19](#).

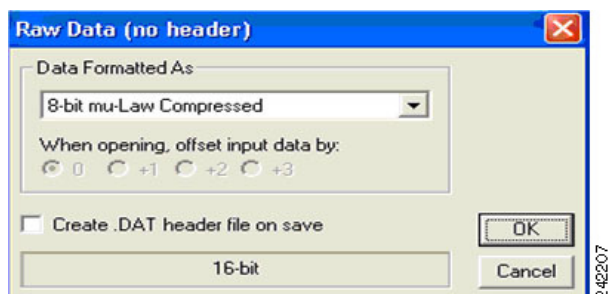
**Figure 3-19** *Cool Edit Pro Window*

A pop-up window displays, as shown in [Figure 3-20](#).

**Figure 3-20** *Interpret Sample Format Window*

**Step 7** Use the settings, as shown in [Figure 3-20](#); then, click **OK**.

A pop-up window displays, as shown in [Figure 3-21](#).

**Figure 3-21** *Raw Data Window*

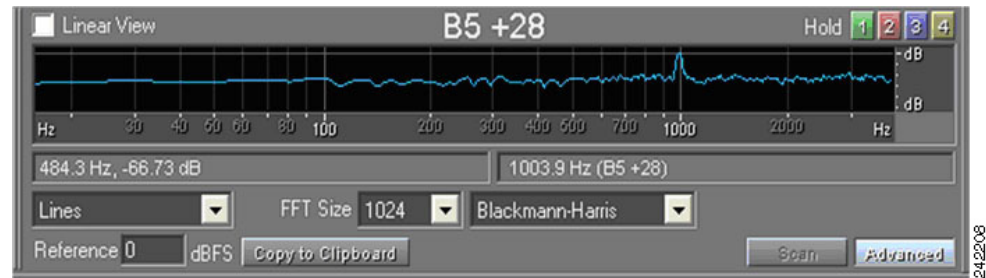
**Step 8** Use the above settings, as shown in [Figure 3-21](#); then, click **OK**.

**Step 9** When the wave form displays, choose **Show Frequency Analysis** from the Analyze drop-down list box.



A window displays to show the frequency and the details of the tone, as shown in [Figure 3-22](#).

**Figure 3-22** *Linear View*

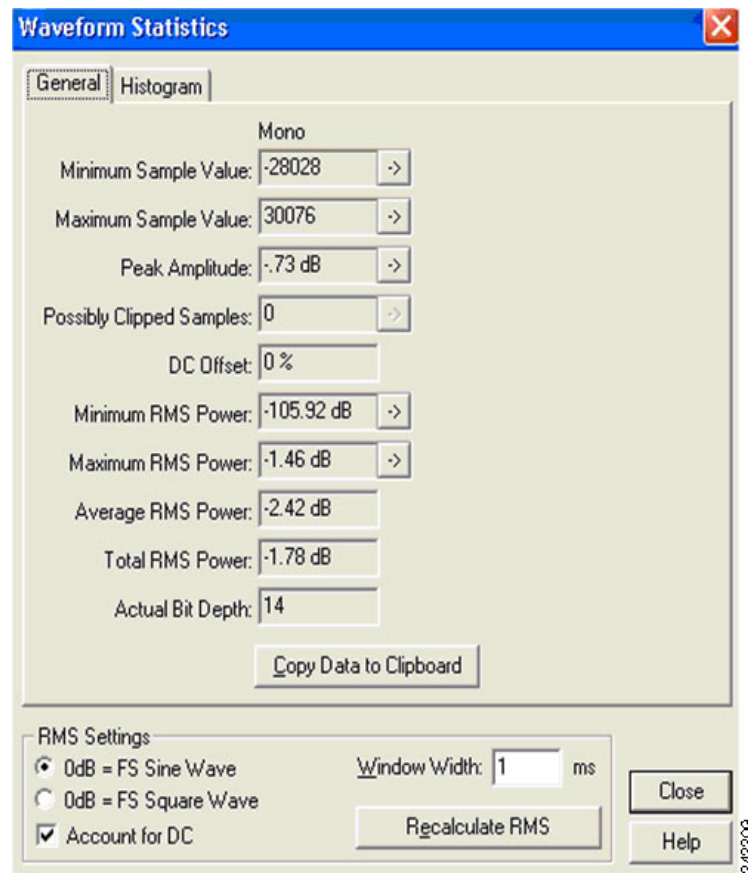


This example shows a frequency of 1003.9 Hz.

- Step 10** To establish the average level, choose **Analyze > Statistics**.

A pop-up window displays to show an average RMS power of -2.42 dB, as shown in [Figure 3-23](#).

**Figure 3-23** *Waveform Statistics General Window*



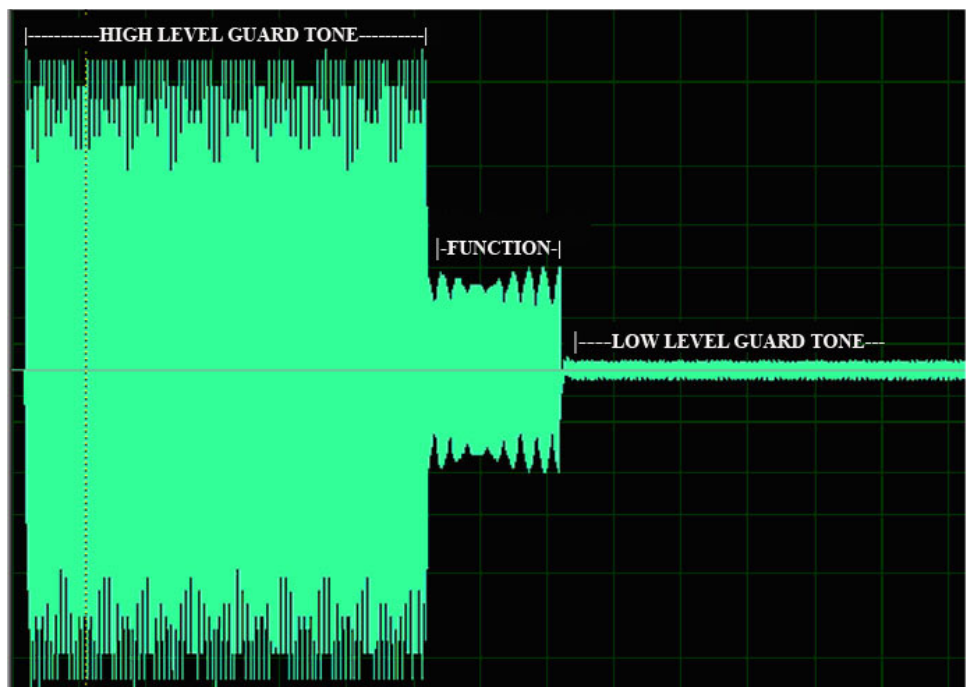
Because this sample was the result of the inject tone command that we entered, the frequency is expected to be 1000 Hz sent at 0 dB, which is very close to the expected results. You can take several more samples to analyze and determine consistency.

To analyze the tone sequence that was captured when the IDC transmitted on radio channel 1, follow the procedure to capture the stream, generate the .raw file, and open it. You should see an alignment with the settings that are specified in the descriptor file that is associated with the radio channel. In this example, we expect the following results:

- HLGT— 2175 Hz at 0 dB for 120 ms
- Function Tone—1950 Hz at -10 dB for 40 ms
- LLGT— 2175 Hz at -30 dB for the duration of the seizure

Figure 3-24 shows the contents of the captured.raw file.

**Figure 3-24** Graphical Representation of a .raw File with a Captured Tone Sequence



To analyze each tone in the sequence, perform the following procedure:

#### Procedure

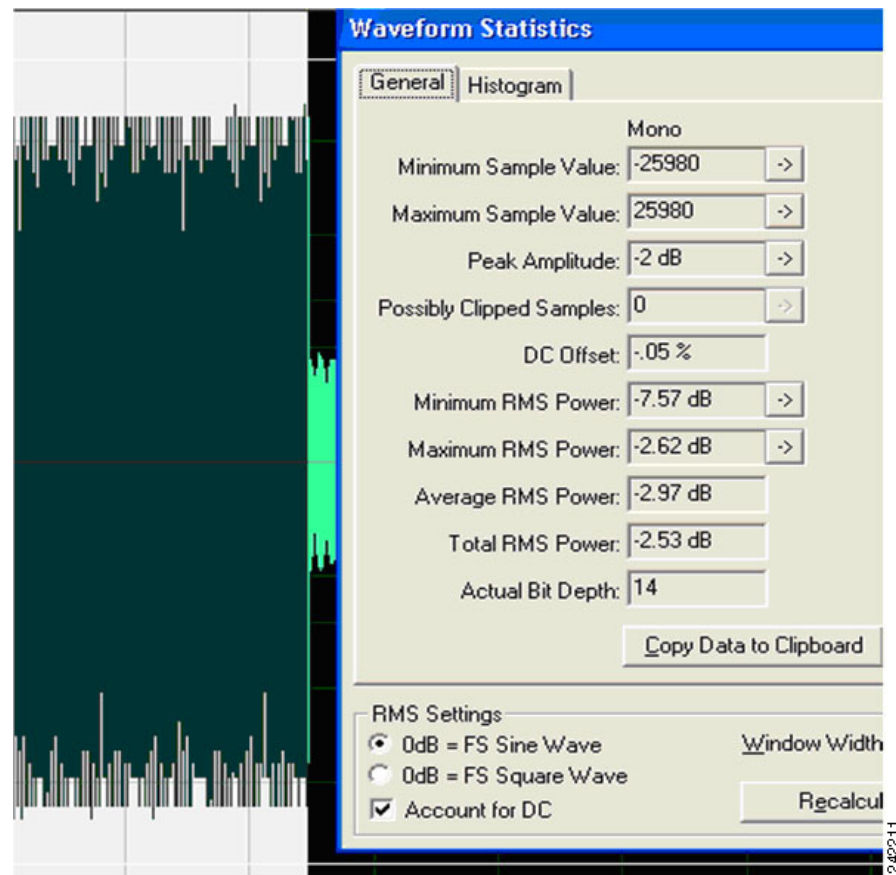
- Step 1** Select the portion of the wave that you want to analyze by pressing the left mouse button and dragging over a section of the wave form; then, release the mouse button.
- Step 2** After you select a section of the wave, check the bottom right corner to see the length of the highlighted section.

In the example, we expect the HLGT length to be 120ms.

The frequency displays in the Frequency Analysis window and the average RMS power level is viewable by choosing **Analyze > Statistics**.

Figure 3-25 shows the first tone in the sequence as being highlighted with the statistics display showing an average RMS power of -2.97 dB. This measurement is about .5 dB lower than the reference we established with the 1000 Hz sample so it should be considered a minor deviation that is related to the test setup.

Figure 3-25 Waveform Statistics General Window—Average RMS Power



#### Note

You can follow the same procedure for the other tones in the sequence to measure frequency, amplitude, and duration. If you do not have access to a suitable application for analysis, send the .raw files to the Cisco IPICS support external mailing list, [ask-ipics-support@external.cisco.com](mailto:ask-ipics-support@external.cisco.com), for analysis.

For details about how to configure an extra voice port to record the audio on a particular multicast address see the “Analog Tap Recording Configuration” section on page 3-68.

## IDC Caveats

Be aware of the following caveats, which pertain to the use of tone-controlled radio channels on the IDC in Cisco IPICS:

- The server configuration determines the order in which the IDC displays the radio channel selector buttons. There is currently no provision to enable reordering or sorting of these buttons.
- Each channel in a radio channel inherits the volume, spatial positioning, VAD, preferred codec, and RX mute during PTT settings from the radio channel. There is currently no provision to enable individual settings.
- The secure indicator is set based on the security setting of the radio channel itself and not on the individual channel selector buttons.
- The voice replay feature records and plays back any audio that is played out to the speakers across radio channels. That is, the voice replay feature records and plays back audio according to the channel that was tuned (active) at the time of capture. The voice replay feature does not track or provide indication of the channel that was active when the audio was received.
- In certain situations, performing one or more simultaneous operations on the same radio may result in unpredictable results.
  - If two IDC users simultaneously attempt to change channels on the same radio, the radio may not change channels and transmissions may be mixed from other speaker(s), or the radio may change to a different channel than either of the channels that were selected.
  - If an IDC user presses a channel selector button and another user presses a different channel selector button before the first user presses the PTT button to talk, the transmission may be sent over an unintended frequency if the first user does not reselect the channel selector button.
  - If an IDC user begins to transmit while another user attempts to change channels on the same radio, transmission may occur in the channel that was selected by the second user. Or, the channel may not actually be changed but the tone control sequence sent by the attempted channel change may transmit. In this case, the IDC may incorrectly represent the channel that is currently selected.
  - If an IDC user tries to change the active channel on the radio at the same time that a voice transmission is being received, the physical radio channel may not change, depending on network and radio configurations. However, because the IDC cannot detect if the radio channel actually changed, the IDC may incorrectly reflect that the channel has been changed even if it has not been changed. When the user next presses the PTT button, while no transmission is being received, the radio will tune to the channel that the user last selected.
  - If a conflict causes the LMR gateway to not generate tones, even though IDC users are transmitting, the low level guard tone may not be present. In this situation, user transmissions may not flow over the radio network.
- Scan mode behavior on the IDC depends on the specific radio configuration. When you use the scan functionality and press the PTT button, the IDC may not be able to accurately detect the frequency that is currently tuned. In this case, the scan functionality may stop or continue and transmission may be sent over an unintended frequency.
- When you press a channel selector button, the function tone may change the state of one or more controls at the same time, depending on the configuration.
- When you connect the IDC by using SIP, radio functionality is limited because the RMS does not pass the RFC tones. In cases where the RMS is running a version of Cisco IOS software that supports the tone remote feature, and the default incoming dial peer (555) has been configured with the

required **rtp payload-type** commands, the RFC 2198 and RFC 2833 packets that are sent by IDC clients get translated by the RMS loopback interface into audible inband tones. These tones may cause the physical radio to retune.

- Intermixing SIP-based (remote) IDC users with local (multicast) users on the same radio may cause the following issues:

**Note**

The behaviors that are listed below may depend on the following factors:

- The version of Cisco IOS that the RMS is running and if that version supports the tone remote feature
- Whether the default incoming dial peer (555) configuration that the IDC users to establish SIP calls to the RMS includes the required **rtp payload-type** commands.

When the above conditions are met, remote IDC users send RFC 2198 and RFC 2833 packets via unicast to the RMS loopbacks, which results in the inband audio tones being sent out the other side of the loopback.

- Control and signaling tones that are normally not audible to multicast users may become audible to participants in VTGs and those who are connected remotely. This situation can cause some tones to play out for the entire duration of the audio.
- Controls that are sent inband because of an RMS loopback, which is used for communications between SIP multicast/VTGs, cannot be properly recognized by multicast users or other SIP users.
- Radio control tones can traverse radio channel VTGs and tune radios that they were not intended for.
- IDC clients that are in different locations (or the same location for SIP-based users) may not be able to properly reflect radio state changes.
- The IDC channel control and signal buttons do not change to reflect the currently selected channel. Therefore, a signal (such as a page) could be transmitted over an unintended channel.
- Radio controls that toggle by using the same tone sequence cannot be reliably detected because the starting or current state of the control cannot be determined.
- There is no correlation between radio controls and channel selection. That is, pressing a channel selector button on one radio is sent only to that radio.

Consider the flow of the RFC 2833 packets in a scenario that involves a remote IDC (10.10.10.5) and a local multicast IDC (10.10.1.2). The behavior in this scenario depends on these factors: the version of Cisco IOS that the RMS is running, and the incoming dial peer configuration that the remote IDC uses to establish SIP calls to the RMS.

- When the RMS is not running the required Cisco IOS software or the dial peer does not have the **rtp payload-type** commands, the RFC packets that the remote IDC sends to the RMS get dropped.
- When the required Cisco IOS software is running and the dial peer configuration is complete, the RMS injects the inband audio tones in the multicast stream that is sent to the LMR gateway and the multicast IDC user.

Although the tones can be used to control the radio, they may also be considered undesirable because all of the endpoints that monitor the multicast stream hear the audio tones. Therefore, make sure that you understand the various behaviors before you decide which one is most appropriate for your implementation.

## Configuration Examples for Manual Tone Control Operated Signaling Scenarios

This section provides sample configurations that can be used to manually configure Cisco IOS software to insert tone sequences that are required for the operation of tone controlled radios. It includes the following topics:

- [2-Wire Tone Control Configuration for Single Frequency, page 3-40](#)
- [4-Wire Tone Control Configuration for Single Frequency, page 3-41](#)
- [2-Wire Tone Control Configuration for Two-Ten Frequencies, page 3-42](#)

### 2-Wire Tone Control Configuration for Single Frequency

When the tone control panel with which you are interfacing is configured for 2-wire operation, the transmit and receive audio and control tones are carried over a single pair of wires. You must issue the **operation 2-wire** command under the voice-port that is being configured. Typically, two of the eight wires are employed.



#### Note

If you configure one port as operation 2-wire, both E&M ports on the same card are automatically set to 2-wire operation.

[Table 3-8](#) shows 2-wire tone control physical LMR connections.

**Table 3-8** 2-Wire Tone Control Physical LMR Connections

Router RJ-45 Pin No.	Router Function	Category 5 Color Code	Radio Connection
1 <sup>1</sup>	Signal Battery (SB)	Orange	No Connection
2 <sup>1</sup>	M-Lead	White/Orange	No Connection
3 <sup>1</sup>	Ring	White/Green	No Connection
4	Ring-1	Blue	TX and RX Audio
5	Tip-1	White/Blue	TX and RX Audio
6 <sup>1</sup>	Tip	Green	No Connection
7 <sup>1</sup>	E-Lead	White/Brown	No Connection
8 <sup>1</sup>	Signal Ground (SG)	Brown	No Connection

1. Does not apply to this configuration.

The following shows a sample configuration for an LMR voice port that is configured for 2-wire tone control operated signaling:

```
voice class permanent 1
  signal timing oos timeout disabled
  signal keepalive disabled
  signal sequence oos no-action
!
voice class tone-signal 1950Hz
  digital-filter 2175hz
  inject tone 1 2175 3 120
  inject tone 2 1950 -5 40
  inject guard-tone 2175 -20
```

```

!
voice-port 0/2/0
 voice-class permanent 1
 voice-class tone-signal 1950Hz
 auto-cut-through
 signal lmr
 lmr duplex half
 lmr led-on
 input gain 1
 output attenuation 1
 no echo-cancel enable
 no comfort-noise
 timeouts call-disconnect 3
 timeouts wait-release 3
 timing hookflash-in 0
 timing hangover 80
 timing delay-voice tdm 160
 connection trunk 101
 description 1950Hz 2-Wire Tone Controlled Radio
 threshold noise -40
!
dial-peer voice 101 voip
 destination-pattern 101
 session protocol multicast
 session target ipv4:239.193.1.1:21000
 codec g711ulaw

```

## 4-Wire Tone Control Configuration for Single Frequency

When the tone control panel with which you are interfacing is configured for 4-wire operation, the transmit audio and control tones are carried over one pair of wires and the receive audio is carried on a second pair of wires. You must issue the **operation 4-wire** command under the voice-port that is being configured. Typically four of the eight wires are employed.



### Note

If you configure one port as operation 4-wire both, E&M ports on the same card are automatically set to operation 4-wire.

Table 3-9 shows 4-wire tone control physical LMR connections.

**Table 3-9** 4-Wire Tone Control Physical LMR Connections

Router RJ-45 Pin No.	Router Function	Category 5 Color Code	Radio Connection
1 <sup>1</sup>	Signal Battery (SB)	Orange	No Connection
2 <sup>1</sup>	M-Lead	White/Orange	No Connection
3	Ring	White/Green	RX Audio
4	Ring-1	Blue	TX Audio
5	Tip-1	White/Blue	TX Audio
6	Tip	Green	RX Audio
7 <sup>1</sup>	E-Lead	White/Brown	No Connection
8 <sup>1</sup>	Signal Ground (SG)	Brown	No connection

1. Does not apply to this configuration.

The following shows a sample configuration for an LMR voice port that is configured for 4-wire tone control operated signaling.

```
voice class permanent 1
  signal timing oos timeout disabled
  signal keepalive disabled
  signal sequence oos no-action
!
voice class tone-signal 1950Hz
  digital-filter 2175hz
  inject tone 1 2175 3 120
  inject tone 2 1950 -5 40
  inject guard-tone 2175 -20
!
voice-port 0/2/0
  voice-class permanent 1
  voice-class tone-signal 1950Hz
  auto-cut-through
  operation 4-wire
  signal lmr
  lmr duplex half
  lmr led-on
  input gain 1
  output attenuation 1
  no echo-cancel enable
  no comfort-noise
  timeouts call-disconnect 3
  timeouts wait-release 3
  timing hookflash-in 0
  timing hangover 80
  timing delay-voice tdm 160
  connection trunk 101
  description 1950Hz 4-Wire Tone Controlled Radio
  threshold noise -40
!
dial-peer voice 101 voip
  destination-pattern 101
  session protocol multicast
  session target ipv4:239.193.1.1:21000
  codec g711ulaw
```

## 2-Wire Tone Control Configuration for Two-Ten Frequencies

There may be scenarios in which you need to change channels via tone control. Cisco IOS lets you insert only a single **tone** command on a voice-port, as described in the [“2-Wire Tone Control Configuration for Single Frequency” section on page 3-40](#). But it is possible to use the DS0 pairs as a bridge to inject a new **tone** command for multiple frequency control. In general, there is a multicast address assigned for each tone sequence and Cisco IPICS has a channel assigned for each multicast address that the tone sequence is assigned to. In this way, an IDC user or Cisco Unified IP Phone user can be assigned these channels to use.



### Note

Be aware that when you use the RMS DS0 pairs to control multiple frequencies, the remote IDC and the Cisco Unified IP Phone cannot detect these frequency changes. That is, when a remote IDC or a Cisco Unified IP Phone uses this implementation to select a different channel, these endpoints may incorrectly reflect the channel that is currently selected and transmissions may be sent over an unintended frequency. Because of this unpredictable behavior, Cisco recommends that you use the Cisco IPICS tone control feature for IDC clients and that you do not mix the RMS DS0 implementation with the native Cisco IPICS tone control feature.



For example, if the radio base station uses 1,950 Hz for F1 repeater frequency and 1,850 Hz for F2 talk around, you could configure Channel 1 for multicast address 239.193.2.1:21000 for 1,950 Hz tone generation and channel 2 for multicast address 239.193.2.2:21000 for 1,850 Hz tone generation. Typically, two of the eight wires are employed.

**Note**

- The use of multiple tone sequences to control the radio must be carefully considered. If a user selects a different channel via DS0 tone control, as described above, other users get no indication of this change. When a non-remote IDC user performs a channel change by using the Cisco IPICS tone control feature, other non-remote IDC clients are updated to reflect the change, making the native solution more reliable for tone control. For related information, see the “Managing Radios and Radio Descriptors” chapter in Cisco IPICS Administration Guide.
- This solution consumes one LMR license for each tone sequence that is sent to the physical radio. Make sure that you have sufficient LMR licenses to deploy this solution.

Table 3-10 shows the wiring connections that are used when interfacing to a 2-wire tone control two-ten frequency operated radio.

**Table 3-10**      *2-Wire Tone Control Two-Ten Frequency Physical LMR Connections*

Router RJ-45 No.1 Pin No.	Router Function	Category 5 Color Code	Radio Connection
1 <sup>1</sup>	Signal Battery (SB)	Orange	No Connection
2 <sup>1</sup>	M-Lead	White/Orange	No Connection
3 <sup>1</sup>	Ring	White/Green	No Connection
4	Ring-1	Blue	TX and RX Audio
5	Tip-1	White/Blue	TX and RX Audio
6 <sup>1</sup>	Tip	Green	No Connection
7 <sup>1</sup>	E-Lead	White/Brown	No Connection
8 <sup>1</sup>	Signal Ground (SG)	Brown	No Connection

1. Not used in this configuration.

Configure the voice-class tone-signal groups for the tones that you want to use. The following example uses all ten available tones. You should use only the tones that you require. Also, configure the voice port for the tone panel. The configuration should be the same as the configuration that is described in the “[2-Wire Tone Control Configuration for Single Frequency](#)” section on page 3-40, except that you do not include the **voice-class tone-signal** command under the voice port. This command is used in the following section to generate multiple tone sequences from the same voice-port. The following example uses voice-port 0/2/0 for the tone panel connection.

```
ip multicast-routing
!
voice class codec 1
  codec preference 1 g729r8
  codec preference 2 g711ulaw
!
voice class permanent 1
  signal timing oos timeout disabled
  signal keepalive disabled
  signal sequence oos no-action
```

```
!  
voice class tone-signal 1950Hz  
  digital-filter 2175hz  
  inject tone 1 2175 3 120  
  inject tone 2 1950 -5 40  
  inject guard-tone 2175 -20  
!  
voice class tone-signal 1850Hz  
  digital-filter 2175hz  
  inject tone 1 2175 3 120  
  inject tone 2 1850 -5 40  
  inject guard-tone 2175 -20  
!  
voice class tone-signal 1750Hz  
  digital-filter 2175hz  
  inject tone 1 2175 3 120  
  inject tone 2 1750 -5 40  
  inject guard-tone 2175 -20  
!  
voice class tone-signal 1650Hz  
  digital-filter 2175hz  
  inject tone 1 2175 3 120  
  inject tone 2 1650 -5 40  
  inject guard-tone 2175 -20  
!  
voice class tone-signal 1550Hz  
  digital-filter 2175hz  
  inject tone 1 2175 3 120  
  inject tone 2 1550 -5 40  
  inject guard-tone 2175 -20  
!  
voice class tone-signal 1450Hz  
  digital-filter 2175hz  
  inject tone 1 2175 3 120  
  inject tone 2 1450 -5 40  
  inject guard-tone 2175 -20  
!  
voice class tone-signal 1350Hz  
  digital-filter 2175hz  
  inject tone 1 2175 3 120  
  inject tone 2 1350 -5 40  
  inject guard-tone 2175 -20  
!  
voice class tone-signal 1250Hz  
  digital-filter 2175hz  
  inject tone 1 2175 3 120  
  inject tone 2 1250 -5 40  
  inject guard-tone 2175 -20  
!  
voice class tone-signal 1150Hz  
  digital-filter 2175hz  
  inject tone 1 2175 3 120  
  inject tone 2 1150 -5 40  
  inject guard-tone 2175 -20  
!  
voice class tone-signal 1050Hz  
  digital-filter 2175hz  
  inject tone 1 2175 3 120  
  inject tone 2 1050 -5 40  
  inject guard-tone 2175 -20  
!  
interface Loopback0  
  ip address 192.168.4.6 255.255.255.255  
  ip pim sparse-dense-mode
```

```

!
interface Vif1
 ip address 192.168.3.5 255.255.255.252
 ip pim sparse-dense-mode
!
interface FastEthernet0/0
 description $ETH-LAN$$ETH-SW-LAUNCH$$INTF-INFO-FE 0/0$
 ip address 192.168.0.6 255.255.255.0
 ip pim sparse-dense-mode
 duplex auto
 speed auto
!
voice-port 0/2/0
 voice-class permanent 1
 auto-cut-through
 signal lmr
 lmr duplex half
 lmr led-on
 input gain 1
 output attenuation 1
 no echo-cancel enable
 no comfort-noise
 timeouts call-disconnect 3
 timeouts wait-release 3
 timing hookflash-in 0
 timing hangover 80
 timing delay-voice tdm 160
 connection trunk 101
 description 2-Wire Tone Controlled Radio
 threshold noise -40
!
dial-peer voice 101 voip
 destination-pattern 101
 session protocol multicast
 session target ipv4:239.193.1.1:21000
 codec g711ulaw

```

Configure a manual loopback in the RMS router to allow the voice-port to generate multiple tone sequences. This approach requires a DS0 manual loopback pair for each tone sequence that you entered as described earlier in this section. If you have four **voice-port tone-signal** commands, you need four DS0 bridges. If you have ten voice-port tone-signal commands, you need ten bridges. You can create bridges by manually defining the voice ports with dial peers. You will likely use a voice port pair that is part of one of your T1 loopbacks for the RMS. Make sure that the T1 loopback pair is not an available resource in the RMS by putting it in the Reserved state. (For information about putting an RMS in Reserved state, refer to the “Performing Cisco IPICS System Administrator Tasks” chapter in *Cisco IPICS Server Administration Guide, Release 4.0(2)*.)

After the channels are determined, you can use the following sample configuration and transpose the T1 voice ports as needed. This example assumes that the ten pairs of loopback ports of 1/0/0:1<->1/0/1:1 to 1/0/0:10<->1/0/1:10 have been marked as reserved in Cisco IPICS and will be used as the manual bridge for generating the required tone sequences.

One half of each T1 loopback pair is configured with **voice-port tone-signal** commands (for example, 1/0/0:1 with voice-port tone-signal 1,950 Hz) with the multicast address of 239.193.2.1:21000. By placing the command on this side of the bridge, the tone panel that is connected to the E&M port receives the tone sequence but the IDC and Cisco Unified IP Phone audio is filtered so that these devices do not receive the tones. There also is an individual dial peer with its own multicast address for each DS0. These addresses should be used as the Cisco IPICS channels. Continue with the additional T1 Loopback Left Side Half configurations as needed.

The following example shows one side of the T1 loopback tone control.

```

voice-port 1/0/0:1
 voice-class permanent 1
 voice-class tone-signal 1950Hz
 auto-cut-through
 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
 timing hangover 180
 timing delay-voice tdm 180
 connection trunk 1950101
 description Tone Control 1950 IDC Bridge (Disabled in Cisco IPICS)
!
voice-port 1/0/0:2
 voice-class permanent 1
 voice-class tone-signal 1850Hz
 auto-cut-through
 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
 timing hangover 180
 timing delay-voice tdm 180
 connection trunk 1850101
 description Tone Control 1850 IDC Bridge (Disabled in Cisco IPICS)
!
voice-port 1/0/0:3
 voice-class permanent 1
 voice-class tone-signal 1750Hz
 auto-cut-through
 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
 timing hangover 180
 timing delay-voice tdm 180
 connection trunk 1750101
 description Tone Control 1750 IDC Bridge (Disabled in Cisco IPICS)
!
voice-port 1/0/0:4
 voice-class permanent 1
 voice-class tone-signal 1650Hz
 auto-cut-through
 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
 timing hangover 180
 timing delay-voice tdm 180
 connection trunk 1650101
 description Tone Control 1650 IDC Bridge (Disabled in Cisco IPICS)
!
voice-port 1/0/0:5
 voice-class permanent 1
 voice-class tone-signal 1550Hz
 auto-cut-through

```

```
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
timing hangover 180
timing delay-voice tdm 180
connection trunk 1550101
description Tone Control 1550 IDC Bridge (Disabled in Cisco IPICS)
!
voice-port 1/0/0:6
voice-class permanent 1
voice-class tone-signal 1450Hz
auto-cut-through
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
timing hangover 180
timing delay-voice tdm 180
connection trunk 1450101
description Tone Control 1450 IDC Bridge (Disabled in Cisco IPICS)
!
voice-port 1/0/0:7
voice-class permanent 1
voice-class tone-signal 1350Hz
auto-cut-through
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
timing hangover 180
timing delay-voice tdm 180
connection trunk 1350101
description Tone Control 1350 IDC Bridge (Disabled in Cisco IPICS)
!
voice-port 1/0/0:8
voice-class permanent 1
voice-class tone-signal 1250Hz
auto-cut-through
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
timing hangover 180
timing delay-voice tdm 180
connection trunk 1250101
description Tone Control 1250 IDC Bridge (Disabled in Cisco IPICS)
!
voice-port 1/0/0:9
voice-class permanent 1
voice-class tone-signal 1150Hz
auto-cut-through
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
        timing hangover 180
        timing delay-voice tdm 180
        connection trunk 1150101
        description Tone Control 1150 IDC Bridge (Disabled in Cisco IPICS)
    !
voice-port 1/0/0:10
    voice-class permanent 1
    voice-class tone-signal 1050Hz
    auto-cut-through
    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
    timing hangover 180
    timing delay-voice tdm 180
    connection trunk 1050101
    description Tone Control 1050 IDC Bridge (Disabled in Cisco IPICS)
!
dial-peer voice 1950101 voip
    description Tone Control 1950 IDC Bridge
    destination-pattern 1950101
    session protocol multicast
    session target ipv4:239.193.2.1:21000
    codec g711ulaw
    no vad
!
dial-peer voice 1850101 voip
    description Tone Control 1850 IDC Bridge
    destination-pattern 1850101
    session protocol multicast
    session target ipv4:239.193.2.2:21000
    codec g711ulaw
    no vad
!
dial-peer voice 1750101 voip
    description Tone Control 1750 IDC Bridge
    destination-pattern 1750101
    session protocol multicast
    session target ipv4:239.193.2.3:21000
    codec g711ulaw
    no vad
!
dial-peer voice 1650101 voip
    description Tone Control 1650 IDC Bridge
    destination-pattern 1650101
    session protocol multicast
    session target ipv4:239.193.2.4:21000
    codec g711ulaw
    no vad
!
dial-peer voice 1550101 voip
    description Tone Control 1550 IDC Bridge
    destination-pattern 1550101
    session protocol multicast
    session target ipv4:239.193.2.5:21000
    codec g711ulaw
    no vad
!
dial-peer voice 1450101 voip
    description Tone Control 1450 IDC Bridge

```

```

destination-pattern 1450101
session protocol multicast
session target ipv4:239.193.2.6:21000
codec g711ulaw
no vad
!
dial-peer voice 1350101 voip
description Tone Control 1350 IDC Bridge
destination-pattern 1350101
session protocol multicast
session target ipv4:239.193.2.7:21000
codec g711ulaw
no vad
!
dial-peer voice 1250101 voip
description Tone Control 1250 IDC Bridge
destination-pattern 1250101
session protocol multicast
session target ipv4:239.193.2.8:21000
codec g711ulaw
no vad
!
dial-peer voice 1150101 voip
description Tone Control 1150 IDC Bridge
destination-pattern 1150101
session protocol multicast
session target ipv4:239.193.2.9:21000
codec g711ulaw
no vad
!
dial-peer voice 1050101 voip
description Tone Control 1050 IDC Bridge
destination-pattern 1050101
session protocol multicast
session target ipv4:239.193.2.10:21000
codec g711ulaw
no vad

```

To simplify the concept of a T1 loopback, which joins two T1 interface ports, we refer to the two sides as right and left. In the following example, the right side of each configured T1 loopback pair (for example, 1/0/1:1 to 1/0/1:10) are all configured with the same multicast address as the dial peer that is assigned to voice-port 0/2/0. In this example, the address is 239.193.1.1:21000.

```

voice-port 1/0/1:1
voice-class permanent 1
auto-cut-through
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
timing hangover 80
connection trunk 2101
description Tone Control 1950 Radio Bridge (Disabled in Cisco IPICS)
!
voice-port 1/0/1:2
voice-class permanent 1
auto-cut-through
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
        timing hangover 80
        connection trunk 2101
        description Tone Control 1850 Radio Bridge (Disabled in Cisco IPICS)
    !
voice-port 1/0/1:3
    voice-class permanent 1
    auto-cut-through
    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
    timing hangover 80
    connection trunk 2101
    description Tone Control 1750 Radio Bridge (Disabled in Cisco IPICS)
!
voice-port 1/0/1:4
    voice-class permanent 1
    auto-cut-through
    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
    timing hangover 80
    connection trunk 2101
    description Tone Control 1650 Radio Bridge (Disabled in Cisco IPICS)
!
voice-port 1/0/1:5
    voice-class permanent 1
    auto-cut-through
    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
    timing hangover 80
    connection trunk 2101
    description Tone Control 1550 Radio Bridge (Disabled in Cisco IPICS)
!
voice-port 1/0/1:6
    voice-class permanent 1
    auto-cut-through
    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
    timing hangover 80
    connection trunk 2101
    description Tone Control 1450 Radio Bridge (Disabled in Cisco IPICS)
!
voice-port 1/0/1:7
    voice-class permanent 1
    auto-cut-through
    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
timing hangover 80
connection trunk 2101
description Tone Control 1350 Radio Bridge (Disabled in Cisco IPICS)
!
voice-port 1/0/1:8
voice-class permanent 1
auto-cut-through
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
timing hangover 80
connection trunk 2101
description Tone Control 1250 Radio Bridge (Disabled in Cisco IPICS)
!
voice-port 1/0/1:9
voice-class permanent 1
auto-cut-through
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
timing hangover 80
connection trunk 2101
description Tone Control 1150 Radio Bridge (Disabled in Cisco IPICS)
!
voice-port 1/0/1:10
voice-class permanent 1
auto-cut-through
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
timing hangover 80
connection trunk 2101
description Tone Control 1050 Radio Bridge (Disabled in Cisco IPICS)
!
dial-peer voice 2101 voip
description Tone Control Bridge
destination-pattern 2101
session protocol multicast
session target ipv4:239.193.1.1:21000
codec g711ulaw
no vad

```

To complete the configuration, set up a channel in Cisco IPICS that is associated with each dial peer that is listed in [Table 3-11](#).

**Table 3-11** Cisco IPICS Tone Control Channel Configurations

Channel Label	Multicast Address
Channel 1 1950 Hz	239.193.2.1:21000

Table 3-11 Cisco IPICS Tone Control Channel Configurations (continued)

Channel Label	Multicast Address
Channel 2 1850 Hz	239.193.2.2:21000
Channel 7 1750 Hz	239.193.2.3:21000
Channel 8 1650 Hz	239.193.2.4:21000
Channel * 1550 Hz	239.193.2.5:21000
Channel * 1450 Hz	239.193.2.6:21000
Channel 3 1350 Hz	239.193.2.7:21000
Channel 4 1250 Hz	239.193.2.8:21000
Channel 5 1150 Hz	239.193.2.9:21000
Channel 6 1050 Hz	239.193.2.10:21000

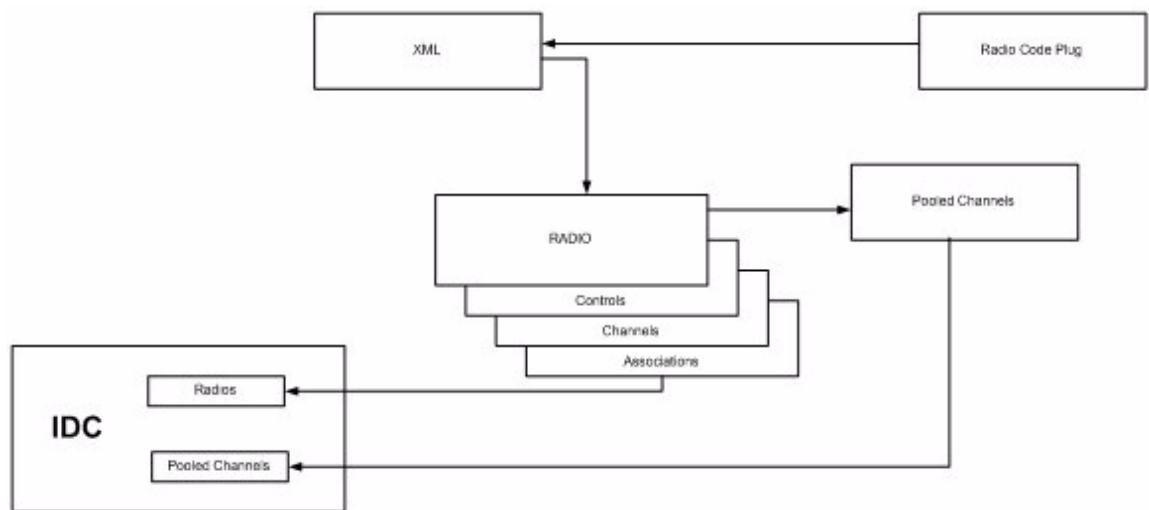
## Pooled Radios

A radio that is created in Cisco IPICS can be tone controlled or serial controlled via a router that serves as an LMR gateway. A serial controlled radio can be configured to be manually controlled by a Cisco IPICS user by directly assigning the radio to a user. Alternatively, a serial controlled radio can be configured as a pooled resource in the Radio Details page in the Cisco IPICS Administration Console.

When a serial controlled radio is marked as a pooled resource, it is no longer available to be directly assigned to a Cisco IPICS user as a media resource and therefore cannot be manually controlled. Instead, these radios are available to be allocated to a channel on demand. Upon channel activation, Cisco IPICS automatically selects a pooled radio, switches it to the desired channel selector and makes it available as a media resource.

Figure 3-26 illustrates the pooled radio to radio relationship.

Figure 3-26 Pooled Radio to Radio Relationship



Using pooled resources reduces the complexity of a system and the training required to use it, improves efficiency, and reduces conflicts when sharing resources between agencies or dispatchers. Using pooled resources also increase system reliability: if a radio in the pool fails, other radios remain available to access the desired resource and the system allocates these resources automatically.

Pooled radios provide a different way of addressing resources than a manually controlled shared radio. With shared radios, you first need to select a shared radio, then change the radio channel selector to the desired talk group. With pooled radios, you select the desired talk group, which comes from a pool of radios that have multiple channels and talk groups associated with them. The Cisco IPICS server automatically determines which radio is not busy, which has the resource available, and which has the highest priority for that use. With pooled radios, a system can be configured and tuned so that radios are automatically selected based on tower location, available bandwidth, and other criteria.

## Configuring and Allocating Pooled Resources

To use channels from multiple pooled radios, each radio must be defined with the same XML descriptor. The XML descriptor defines the channel name and which “Zone” and “Selector” are associated with the channel that is programmed into the radio. The channel is programmed into the radio via a configuration file, called a *code plug*, that is uploaded to the radio.

Pools of radios are not explicitly maintained within Cisco IPICS. All pooled radios that are associated with a specific radio descriptor are considered to implicitly belong to that pool. This approach eliminates the need to manage pools of radios. Radios with a similar set of channel selectors as determined by a radio descriptor have similar characteristics and therefore belong to the same pool. If you need to ensure separation of radios between pools, use a different radio descriptor for each pool.

When you create a channel in the Cisco IPICS Administration Console, the Pooled Radio media type is available. When adding a pooled radio media connection, you must select a radio descriptor and a channel selector. The radio descriptor defines the pool of radios, and the channel selector instructs Cisco IPICS to set the allocated pooled radio to this channel when the channel is activated.

A pooled radio is allocated to a channel when the channel is activated. Channel activation can occur when a channel with a pooled radio is a member of a VTG and the VTG is activated, or when a channel with a pooled radio is activated by an IDC user.

## Pooled Resource Allocation

When a channel that has a pooled radio assigned to it is activated, Cisco IPICS searches for a radio that is associated with the radio descriptor file in the media connection that is assigned to the channel. If Cisco IPICS finds a radio that is available and that meets these criteria, Cisco IPICS configures the radio to switch to the appropriate channel, group, or private call as described in the channel selector. After this process is completed, the radio is marked as allocated to the channel.

IPICS keeps track of a pooled radio allocation to a channel, including all channel activations that occurred via a VTG or an IDC user. When the last VTG or IDC deactivates the channel, IPICS automatically deallocates the pooled radio, and the radio becomes available for use for a future allocation. Until such a deallocation occurs, another activation of the same channel results in the use of the same pooled radio.



### Note

If a channel is created with a pooled radio connection and a multicast connection, Cisco IPICS always uses the cheaper media type. In this case, a multicast media connection is cheaper, therefore a pooled radio will never be allocated to this channel.

IP phone and dial-in users cannot activate a pooled resource in Cisco IPICS. Therefore, an IP phone or dial-in cannot join a pooled radio channel if the channel is not already active.

## Determining How many Pooled Radios to Configure

The main criteria to determine how many pooled radio resource to deploy for a given radio descriptor is the number of expected concurrent active channels. If the end user has 100 channel selectors available in a radio descriptor, but they don't expect to use more than say 10 channels at any given time, then they should deploy no less than 10 pooled radios for that radio descriptor.

### Troubleshooting Channel Activation Failures

When a channel containing a pooled radio media connection cannot be activated, it could be because of the following reasons:

- There are no pooled radios belonging to the selected radio descriptor.
- The desired channel selector for all remaining pooled radios belonging to the selected radio descriptor is not enabled.
- All remaining pooled radios that belong to the selected radio descriptor are disabled or not CONNECTED\_ONLINE.
- All pooled radios have already been allocated to other channels.

## Optimizing Priorities for Trunked Networks and Wide Area Systems

In a trunk system multisite deployment, there are always more talk groups defined than bearer channels available. To prevent a substantial number of collisions and busy conditions, a system design should attempt to optimize the trunk system utilization by allocating talk groups that are related geographically.

You perform the prioritization configuration process from the Cisco IPICS Administration Console by performing the following general steps. For related information, see the “Managing Radios and Radio Descriptors” chapter in *Cisco IPICS Server Administration Guide*.

1. To designate a radio as a pooled resource, choose the **Server** drawer, then choose **Configuration > Radios > radio\_name**, then check the **Pooled Resource** check box in the in the General tab.
2. To set priorities for each channel in the radio, choose the **Selectors** tab for the radio. This tab shows each channel that is defined in the descriptor file for the radio. Check the Enabled check box and set the priority for each channel in the radio based on the system design and donor radio placement in the network.

After you complete this configuration, the pooled resource is available for use in a VTG.

## Serial Radio Control

Cisco IPICS provides the serial radio control feature, which supports the following serially controlled radios:

- EF Johnson 5300 and 5300ES mobile radios
- Sprint Nextel (iDEN) i355 handsets

The serial radio control feature allows you to remotely control functions in a donor serial radio from the Cisco IPICS Administration Console or from the Cisco IPICS IDC. A donor radio allows sending and receiving audio between Cisco IPICS and a radio system. Functions that can be controlled include secure transmit mode, scan, monitor, channel/talkgroup change, and individual (unit-to-unit) calls and dynamic group calls, depending on the capabilities of the donor radio. Cisco IPICS also can detect changes in radio state, including talker ID and emergency “man down” alarms. This capability provides enhanced interoperability to Motorola SmartNet/SmartZone, P25, and Sprint Nextel (iDEN) radio networks.

When you set up serial control for a radio, you configure voice interoperability, which enables audio to pass between Cisco IPICS and a radio network via the E&M port on an LMR gateway. You also configure serial radio control for one of the following methods:

- Auxiliary port control—Used to control one radio that is attached an LMR gateway
- 8-port WAN interface card control—Used to control up to 8 radios that are attached an LMR gateway
- 16-port WAN interface card control—Used to control up to 16 radios that are attached an LMR gateway

This chapter includes these topics:

- [Setting up and Configuring Serial Control for EF Johnson Radios, page 3-55](#)
- [Setting up and Configuring Serial Control for Sprint Nextel \(iDEN\) Handsets, page 3-59](#)

## Setting up and Configuring Serial Control for EF Johnson Radios

The following sections explain how to connect and configure an EF Johnson 5300 or 5300ES mobile radio as a donor radio. This process involves these general steps:

1. Connect a donor radio. For detailed instructions, see the [“Connecting an EF Johnson Donor Radio to an LMR Gateway” procedure on page 3-56](#).
2. Configure the LMR gateway. For detailed instructions, see the [“Configuring the LMR Gateway for E&M Communications with EF Johnson Radios” section on page 3-57](#) and the [“Configuring the LMR Gateway for Serial Radio Control” section on page 3-58](#)

In addition, you must add the radio to Cisco IPICS and perform other tasks to allow serial control of the radio by Cisco IPICS. For detailed instructions, see *Cisco IPICS Server Administration Guide, Release 2.2*.

## Required Components

You need the following components to set up and configure serial control for EF Johnson radios:

- Donor Radio—EF Johnson model 5300 mobile radio running firmware version 04.14.03 or later or model 5300ES running firmware version 06.08.08 or later
- LMR gateway—Cisco 2811 or 3845 with E&M ports

### For voice interoperability:

- Cable for remote control head or fixed control station applications (EF Johnson part # 597-2002-249). One cable is required for each radio that you will connect.
- DB15 male to RJ-45 female adapter for connecting the control head cable to the LMR gateway E&M port (available from networked radio.com, part # REM-4496). One adapter is required for each radio that you will connect.

- E&M cable—Category 5 straight-through Ethernet cable.

**For serial radio control:**

- 5300 Series Remote Programming Interface (RPI)—Includes a ribbon cable with a Hirose connector, and a DB9 RS-232 connector (EF Johnson part # 023-5300-001). One RPE is required for each radio that you will connect.
- DB9 male to RJ-45 cable adapter (available from various third-party vendors). One adapter is required for each radio that you will connect.
- Category 5 straight-through Ethernet cable—Required only for auxiliary port control.
- Cisco “octopus” cable (Cisco part # 72-4023-01 or CAB-HD8-ASYNC)—One cable is required for 8-port WAN interface card control; two cables are required for 16-port WAN interface card control.
- Cisco 1800/2800/3800 series 8-port asynchronous high-speed WAN interface card model HWIC-8A—Required only for 8-port WAN interface card control.
- Cisco 1800/2800/3800 series 16-port asynchronous high-speed WAN interface card model HWIC-16A—Required only for 16-port WAN interface card control.

## Connecting an EF Johnson Donor Radio to an LMR Gateway

To connect an EF Johnson 5300 or 5300ES mobile radio to an LMR gateway, follow these steps:

### Procedure

- 
- Step 1** Make the connection for voice interoperability as follows:
- Connect the E&M cable from an available port on the LMR gateway to the DB15 male to RJ-45 cable adapter.
  - Connect the radio control head cable, which is attached to the radio, to this adapter.
- Step 2** Make the appropriate connections for serial radio control as follows:
- If you are setting up auxiliary port control, connect the category 5 straight-through Ethernet cable from the auxiliary port on the LMR gateway to the RJ-45 port on the RPI, using the DB9 male to RJ-45 data cable adapter.
  - If you are setting up 8-port WAN interface card control, take these actions:
    - Connect the octopus cable to the WAN interface card.
    - Connect one of the lines on the octopus cable to the DB9 to RJ-45 cable adapter.
  - If you are setting up 16-port WAN interface card control, take these actions:
    - Connect two octopus cables to the two ports on the WAN interface card.
    - Connect one of the lines on the octopus cable to the DB9 to RJ-45 cable adapter.
- Step 3** Connect the DB9 to RJ45 cable adapter to the DB9 port on the RPI.
- Step 4** Connect the ribbon cable from the RPI to the mic port on the radio.
-

## Configuring the LMR Gateway for E&M Communications with EF Johnson Radios

After you connect an EF Johnson radio to an LMR gateway as described in the [“Connecting an EF Johnson Donor Radio to an LMR Gateway”](#) section on page 3-56, configure the LMR gateway for E&M communications. This process involves configuring voice ports and creating associated dial peers.

To configure the LMR gateway, perform the following steps for each radio that is to be serially controlled:

### Procedure

- 
- Step 1** Log in to the LMR gateway and enter the following command to start configuration mode:
- ```
router-2811# configure terminal
```
- Step 2** Enter the following commands to configure the LMR gateway voice port to which the radio is connected, where
- *<x>* is the network module on the LMR gateway that contains the voice cards
  - *<y>* is the slot on the network module that contains the voice card that you are connecting to
  - *<z>* is the port on the voice card that you are using on the voice card that you are connecting to
  - *<connection trunk number>* is a unique number that you assign to the connection trunk
- ```
router-2811(config)# voice-port <x>/<y>/<z>
router-2811(config-voiceport)# voice-class permanent 1
router-2811(config-voiceport)# auto-cut-through
router-2811(config-voiceport)# operation 4-wire
router-2811(config-voiceport)# type 3
router-2811(config-voiceport)# signal lmr
router-2811(config-voiceport)# lmr e-lead voice
router-2811(config-voiceport)# lmr led-on
router-2811(config-voiceport)# input gain -10
router-2811(config-voiceport)# output attenuation 10
router-2811(config-voiceport)# no echo-cancel enable
router-2811(config-voiceport)# no comfort-noise
router-2811(config-voiceport)# timeouts call-disconnect 3
router-2811(config-voiceport)# timing hookflash-in 0
router-2811(config-voiceport)# timing hangover 80
router-2811(config-voiceport)# bootup e-lead off
router-2811(config-voiceport)# connection trunk <connection trunk number>
router-2811(config-voiceport)# description EFJ 5300
```
- Step 3** Enter the following command to exit voice port configuration mode:
- ```
router-2811(config-voiceport)# exit
```
- Step 4** Enter the following commands to create a dial peer for the connection trunk number that you configured in [Step 2](#), where

- *<connection trunk number>* is the number of the connection trunk.
- *<multicast>* is the multicast IP address and port number for voice traffic, in a.c.b.d:port format. Make note of this multicast address. You will use it when add the radio in the Cisco IPICS Administration Console.
- *<description>* is a description that you enter for the voice port and dial peer.

```

router-2811(config)# dial-peer voice <connection trunk number> voip
router-2811(config)# description <description>
router-2811(config)# destination-pattern <connection trunk number>
router-2811(config)# session protocol multicast
router-2811(config)# session target ipv4:<multicast>
router-2811(config)# codec g711ulaw
router-2811(config)# ip qos dscp cs5 media
router-2811(config)# no vad

```

**Step 5** Enter the following command to exit configuration mode:

```

router-2811(config-voiceport)# end

```

## Configuring the LMR Gateway for Serial Radio Control

After you configure the an LMR gateway as described in the [“Configuring the LMR Gateway for E&M Communications with EF Johnson Radios”](#) section on page 3-57, you are ready to configure the LMR gateway for serial control. This process involves configuring an asynchronous high-speed WAN interface card or an auxiliary port, depending on the serial radio control method that you are using.

To configure an LMR gateway for serial radio control, follow these steps:

### Procedure

**Step 1** Log in to the LMR gateway and enter the following command to start configuration mode:

```

router-2811# configure terminal

```

**Step 2** Enter the following command to create an AAA policy that does not require authentication:

```

router-2811(config)# aaa authentication login NO-AUTHEN none

```

**Step 3** Take one of these actions:

- If you are configuring for auxiliary port control, enter the following command:  

```

router-2811(config)# line aux 0

```
- If you are configuring for 8-port or 16-port WAN interface card control and want to configure one line at a time, enter the following command for each line that you are configuring:  

```

router-2811(config)# line <x>/<y>/<z>

```

  - *<x>* is the network module on the LMR gateway that contains the voice cards
  - *<y>* is the slot on the network module that contains the voice card that you are connecting to
  - *<z>* is the port on the voice card that you are using on the voice card that you are connecting to



- If you are configuring for 8-port or 16-port WAN interface card control and want to configure a range of contiguous lines on the WAN card, enter the following command:  
router-2811(config)# **line** <x>/<y>/<a> <x>/<y>/<b>  
  - <x> is the network module on the LMR gateway that contains the voice cards
  - <y> is the slot on the network module that contains the voice card that you are connecting to
  - <a> is the beginning port of the port range on the voice card that you are using on the voice card that you are connecting to
  - <b> is the ending port of the port range on the voice card that you are using on the voice card that you are connecting to

**Step 4** Enter the following commands to set the transport parameters:

```
router-2811(config-line)# transport preferred none  
router-2811(config-line)# transport input all  
router-2811(config-line)# speed 19200  
router-2811(config-line)# no exec-banner  
router-2811(config-line)# exec-timeout 0 0  
router-2811(config-line)# privilege level 0  
router-2811(config-line)# login authentication NO-AUTHEN  
router-2811(config-line)# no activation-character  
router-2811(config-line)# no exec  
router-2811(config-line)# transport output none  
router-2811(config-line)# escape-character NONE
```

**Step 5** Enter the following command to exit configuration mode:

```
router-2811(config-line)# end
```

---

## Setting up and Configuring Serial Control for Sprint Nextel (iDEN) Handsets

This section explains how to connect and configure a Sprint Nextel (iDEN) handset as a donor radio. This process involves these general steps:

1. Connect a donor radio. For detailed instructions, see the [“Connecting a Sprint Nextel \(iDEN\) Handset to an LMR Gateway”](#) section on page 3-60.
2. Configuring the Sprint Nextel (iDEN) handset. For detailed instructions, see the [“Configuring a Sprint Nextel \(iDEN\) Handset”](#) section on page 3-61
3. Configure the LMR gateway. For detailed instructions, see the [“Configuring the LMR Gateway for E&M Communication with Sprint Nextel \(iDEN\) Handsets”](#) section on page 3-61 and the [“Configuring the LMR Gateway for Serial Radio Control”](#) section on page 3-63.

In addition, you must add a radio to Cisco IPICS and perform other tasks to allow serial control of the radio by Cisco IPICS. For detailed instructions, see *Cisco IPICS Server Administration Guide, Release 2.2*.

## Required Components

You need the following components to set up and configure serial control for Sprint Nextel (iDEN) i355 handsets:

- Donor Radio—Sprint Nextel (iDEN) i355 handset
- LMR gateway—Cisco 2811 or 3845 with E&M ports

**For voice interoperability:**

- E&M cable—Nextel Falcon series E&M interface cable (available from networkedradio.com, part # REM-4327)
- Attenuator for E&M cable (available from networkedradio.com, part # REM-621)

**For serial radio control:**

- Motorola iDen data cable (available from networkedradio.com, part # REM-4527)
- Category 5 straight-through Ethernet cable—Required only for auxiliary port control
- Cisco “octopus” cable (Cisco part # 72-4023-01 or CAB-HD8-ASYNC)—One cable is required for 8-port WAN interface card control; two cables are required for 16-port WAN interface card control
- Cisco 1800/2800/3800 series 8-port asynchronous high-speed WAN interface card model HWIC-8A—Required only for 8-port WAN interface card control
- Cisco 1800/2800/3800 series 16-port asynchronous high-speed WAN interface card model HWIC-16A—Required only for 16-port WAN interface card control

## Connecting a Sprint Nextel (iDEN) Handset to an LMR Gateway

To connect a Sprint Nextel (iDEN) i355 handset to an LMR gateway, follow these steps:

### Procedure

- 
- Step 1** Make the connection for voice interoperability as follows:
- a. Connect the E&M cable to the attenuator.
  - b. Connect the E&M cable to the speaker/mic port on the handset.
  - c. Connect the attenuator to one of the E&M ports on the LMR gateway.
- Step 2** Make the appropriate connections for serial radio control as follows:
- If you are setting up auxiliary port control, connect the Category 5 straight-through Ethernet cable from the LMR gateway aux port to the RJ-45 jack on the Motorola iDen data cable, and connect the Motorola iDen data cable to the data port on the bottom of the handset.
  - If you are setting up 8-port WAN interface card control, take these actions:
    - a. Connect the octopus cable to up to the WAN interface card.
    - b. Connect one of the lines on the octopus cable to the RJ-45 jack on the Motorola iDen data cable.
    - c. Connect the Motorola iDen data cable to the data port on the bottom of the handset.
  - If you are setting up 16-port WAN interface card control, take these actions:
    - a. Connect two octopus cables to the two ports on the WAN interface card.
    - b. Connect one of the lines on the octopus cable to the RJ-45 jack on the Motorola iDen data cable.

- c. Connect the Motorola iDen data cable to the data port on the bottom of the handset.
- 

## Configuring a Sprint Nextel (iDEN) Handset

After connecting a handset to an LMR gateway as described in the [“Connecting a Sprint Nextel \(iDEN\) Handset to an LMR Gateway”](#) section on page 3-60, follow these steps to configure the handset:

### Procedure

---

- Step 1** Take these actions to set the handset to always talk back on the last call type:
- a. Press the **Menu** button on the handset.  
The Menu button has an icon of a page.
  - b. Use the right-arrow button to navigate to the **Settings** option and press **OK**.
  - c. Use the down-arrow button to navigate to **DC/GC Options** and press **OK**.
  - d. Use the down-arrow button to navigate to **One Touch DC** and press **OK**.
  - e. Make sure that **Last Call** is selected.  
If it is not, use the arrow-buttons to highlight **Last Call** and press **OK**.
  - f. Press the **Back** button to return to the NEXTEL main page.
- Step 2** Take these actions to set the handset data baud rate to 19200:
- a. Press the **Menu** button on the handset.
  - b. Use the right-arrow button to navigate to the **Settings** option and press **OK**.
  - c. Use the down-arrow button to navigate to **Advanced** and press **OK**.
  - d. Use the down-arrow button to navigate to **Baud Rate** and press **OK**.
  - e. Make sure that **19200** is selected.  
If it is not, use the arrow-buttons to highlight **19200** and press **OK**.
- 

## Configuring the LMR Gateway for E&M Communication with Sprint Nextel (iDEN) Handsets

After you configure a handset as described in the [“Configuring a Sprint Nextel \(iDEN\) Handset”](#) section on page 3-61, configure the LMR gateway for E&M communication. This process involves configuring voice ports and creating associated dial peers.

To configure the LMR gateway, perform the following steps for each radio that is to be serially controlled:

### Procedure

---

- Step 1** Log in to the LMR gateway and enter the following command to start configuration mode:
- ```
router-2811# configure terminal
```
- Step 2** Enter the following commands to configure the LMR gateway voice port to which the radio is connected, where

- *<x>* is the network module on the LMR gateway that contains the voice cards
- *<y>* is the slot on the network module that contains the voice card that you are connecting to
- *<z>* is the port on the voice card that you are using on the voice card that you are connecting to
- *<connection trunk number>* is a unique number that you assign to the connection trunk

```

router-2811(config)# voice-port <x>/<y>/<z>
router-2811(config-voiceport)# voice-class permanent 1
router-2811(config-voiceport)# auto-cut-through
router-2811(config-voiceport)# operation 4-wire
router-2811(config-voiceport)# type 5
router-2811(config-voiceport)# signal lmr
router-2811(config-voiceport)# lmr e-lead voice
router-2811(config-voiceport)# lmr duplex half
router-2811(config-voiceport)# lmr led-on
router-2811(config-voiceport)# input gain -10
router-2811(config-voiceport)# output attenuation 17
router-2811(config-voiceport)# no echo-cancel enable
router-2811(config-voiceport)# no comfort-noise
router-2811(config-voiceport)# timeouts call-disconnect 3
router-2811(config-voiceport)# timing hookflash-in 0
router-2811(config-voiceport)# timing hangover 530
router-2811(config-voiceport)# timing delay-voice tdm 250
router-2811(config-voiceport)# timing ignore m-lead 300
router-2811(config-voiceport)# connection trunk <connection trunk number>
router-2811(config-voiceport)# description Nextel

```

**Step 3** Enter the following command to exit voice port configuration mode:

```
router-2811(config-voiceport)# exit
```

**Step 4** Enter the following commands to create a dial peer for the connection trunk number that you configured in [Step 2](#), where

- *<connection trunk number>* is the number of the connection trunk.
- *<multicast>* is the multicast IP address and port number for voice traffic, in a.c.b.d:port format. Make of note of this multicast address. You will use it when add the radio in the Cisco IPICS Administration Console.
- *<description>* is an description that you enter for the voice port and dial peer

```

router-2811(config)# dial-peer voice <connection trunk number> voip
router-2811(config)# description <description>
router-2811(config)# destination-pattern <connection trunk number>
router-2811(config)# session protocol multicast
router-2811(config)# session target ipv4:<multicast port number>

```

```

router-2811(config)# codec g711ulaw
router-2811(config)# ip qos dscp cs5 media
router-2811(config)# vad aggressive

```

**Step 5** Enter the following command to exit configuration mode:

```

router-2811(config-voiceport)# end

```

## Configuring the LMR Gateway for Serial Radio Control

After you configure the an LMR gateway for E&M communications as described in the [“Configuring the LMR Gateway for E&M Communication with Sprint Nextel \(iDEN\) Handsets”](#) section on page 3-61, you are ready to configure the LMR gateway for serial radio control. This process involves configuring an asynchronous high-speed WAN interface card or an auxiliary port, depending on the serial radio control method that you are using.

To configure an LMR gateway for serial radio control, follow these steps:

### Procedure

**Step 1** Log in to the LMR gateway and enter the following command to start configuration mode:

```

router-2811# configure terminal

```

**Step 2** Enter the following to create an AAA policy that does not require authentication:

```

router-2811(config)# aaa authentication login NO-AUTHEN none

```

**Step 3** Take one of these actions:

- If you are configuring for auxiliary port control, enter the following command:  

```

router-2811(config)# line aux 0

```
- If you are configuring for 8-port or 16-port WAN interface card control and want to configure one line at a time, enter the following command for each line that you are configuring:  

```

router-2811(config)# line <x>/<y>/<z>

```

  - <x> is the network module on the LMR gateway that contains the voice cards
  - <y> is the slot on the network module that contains the voice card that you are connecting to
  - <z> is the port on the voice card that you are using on the voice card that you are connecting to
- If you are configuring for 8-port or 16-port WAN interface card control and want to configure a range of multiple contiguous lines on the WAN card, enter the following command:  

```

router-2811(config)# line <x>/<y>/<a> <x>/<y>/<b>

```

  - <x> is the network module on the LMR gateway that contains the voice cards
  - <y> is the slot on the network module that contains the voice card that you are connecting to
  - <a> is the beginning port of the port range on the voice card that you are using on the voice card that you are connecting to
  - <b> is the ending port of the port range on the voice card that you are using on the voice card that you are connecting to

**Step 4** Enter the following commands to set the transport parameters:

```

router-2811(config-line)# transport preferred none
router-2811(config-line)# transport input all
router-2811(config-line)# speed 19200
router-2811(config-line)# no exec-banner
router-2811(config-line)# exec-timeout 0 0
router-2811(config-line)# privilege level 0
router-2811(config-line)# login authentication NO-AUTHEN
router-2811(config-line)# no activation-character
router-2811(config-line)# no exec
router-2811(config-line)# transport output none
router-2811(config-line)# escape-character NONE

```

**Step 5** Enter the following command to exit configuration mode:

```

router-2811(config-line)# end

```

## Trunked Radio Optional Workaround

The following sections describes the issue that is referred to as the ping-pong effect and provides a hybrid configuration procedure to solve this issue:

- [Trunked Radio Feedback Tones, page 3-64](#)
- [Trunked Radio Hybrid Configuration, page 3-65](#)

## Trunked Radio Feedback Tones

Trunked radios often provide a radio user with beeps and bonks during the beginning and end of transmissions. These beeps and bonks provide feedback about the status of user requests to access a channel, group, or radio. If Cisco IPICS IDC users do not receive this audio feedback information, they may think that they are transmitting when they have been denied channel access to the system because it is busy or because the radio that they are trying to contact is not available. An IDC must operate in a full duplex mode to receive these tones. However, if you add a full duplex enabled channel to a VTG, you risk obtaining a ping pong audio effect when the trailing burst of audio is received at the VTG after the PTT key is released on a PTT device.



### Note

Only the IDC endpoint can operate in a full duplex mode. The Cisco Unified IP Phone XML application continues to be half duplex.

A goal is to deal with these conflicting requirements:

- Full duplex is required for IDC endpoints to hear beeps and bonks.
- Half duplex is required to prevent ping ponging with trunked radios that provide a trailing burst of audio when they disconnect.

- Half duplex is required when two or more trunked radios are added to VTGs.
- Additional timing is required to prevent the loss of the beginning of transmissions because of channel access time when two or more trunked radios are added to VTGs.

## Trunked Radio Hybrid Configuration

To allow for beeps and bonks and to prevent ping ponging, you must deploy a hybrid solution that creates two separate channels for each trunked radio as follows:

- Channel 1 IDC = 239.193.1.4. The multicast address that is assigned to channel 1 is the same address that is assigned to the voice port and dial peer for a radio. Channel 1 is a full duplex channel that can be assigned to IDC users who want to use the trunked channel and obtain the feedback beeps and bonks. It is important that this full duplex channel not accidentally be placed into a VTG or an extreme ping pong effect will occur. You can prevent this channel from being placed in a VTG by unchecking the **Allow Use in VTGs** check box in the **Configuration > Channels > General** tab in the Cisco IPICS Administration Console.
- Channel 2 VTG = 239.193.1.0 This half duplex channel can be put in a VTG if you want the trunked radio to be in a patch. Channel 2 has a multicast address, which is different than the address of channel 1, and which is assigned to its own dial-peer that is separate from the voice port and dial peer for the radio. The goal of this channel is to prevent the feedback beeps and bonks from getting into the VTG audio patch.

Now, as you can see, you have an extra “dummy” channel (Channel 2 VTG) that is used to create the hybrid solution.



### Note

This solution consumes two LMR licenses for each physical trunk radio. Make sure that you have enough LMR licenses to deploy this solution.

The following steps describe how to configure the voice port for a trunked radio. The voice port must be configured to match the radio that is being used. The choices are described in the [“Cisco IOS LMR Gateway Configurations” section on page 3-7](#). Typically, you use the configuration that is shown in the following example for a “VAD Operated Signaling Configuration” for any trunked radio, even if the COR/COS lead is available. In this way, when the donor radio that is connected to the Cisco IPICS voice port presents the feedback beeps and bonks, it does not activate the COR/COS lead. Unless you can verify that the COR/COS lead is activated during any audio (not just during receive audio), the “VAD Operated Signaling Configuration” should be used for the voice-port with the trunk radio hybrid configuration so that the IDC receives the beeps and bonks.

The following example shows the E&M voice-port and dial peer configuration that is used for the full duplex trunked radio in the hybrid configuration solution for Cisco IPICS.

In this example, type { 2 | 3 | 5 } typically is type 3, but see [Figure 3-3 on page 3-5](#), [Figure 3-4 on page 3-6](#), and [Figure 3-5 on page 3-7](#) to select the type that best matches your radio requirements. Input gain { -27 - 16 } typically is 10, but adjust this value as needed to best receive audio on Cisco IPICS endpoints. Output attenuation { -16 - 27 } typically is 10, but adjust this value as needed to best receive audio on radios. When connecting a radio to a voice port in an LMR gateway, you may need to make adjustments to properly balance the audio levels. A radio typically provides gain adjustments, and the level of the signal from the radio to the voice port and the level of the signal from the voice port to the radio may require some adjustments on the radio and the voice port. When using a tone controlled radio, it is important to note that the tones that are sent from the LMR gateway to the radio also are affected by

the voice ports output attenuation settings. When optimizing these settings to achieve the desired audio levels, take care to ensure that the voice port adjustments do not have an adverse effect on the level and quality of the tone signals.

```
! Full Duplex E&M Port for Trunked Radio
!
voice-port 0/3/1
  voice-class permanent 1
  auto-cut-through
  operation 4-wire
  type {2 | 3 | 5 } ! Typically type 3.
  signal lmr
  lmr e-lead voice
  lmr led-on
  input gain { -27 - 16 }
  output attenuation { -16 - 27 }
  no echo-cancel enable
  no comfort-noise
  timeouts call-disconnect 3
  timeouts wait-release 3
  timing hookflash-in 0
  timing hangover 80
  connection trunk 104
  description Trunked Radio Port
!
! VAD Dial-Peer For Above Trunked Radio
!
dial-peer voice 104 voip
  destination-pattern 104
  session protocol multicast
  session target ipv4:239.193.1.4:21000
  codec g711ulaw
  vad ! Do not use vad aggressive.
```

So that the traffic that is associated to 239.193.1.4 is routed to the dummy channel, you must next set up a manual loopback in the RMS router. To do so, manually define the voice ports with dial peers to create the manual “bridge.” You will likely use a voice port pair that is part of one of your T1 loopbacks for the RMS. Make sure that the T1 loopback pair (DS0 resource) is not an available resource in the RMS by putting it in the Reserved state. (For information about putting an RMS in Reserved state, refer to the “Performing Cisco IPICS System Administrator Tasks” chapter in *Cisco IPICS Server Administration Guide, Release 4.0(2).*)

When the DSO channel that you want to use is determined, you can use the following sample configuration and transpose the T1 DS0 voice ports as needed. This example assumes that a loopback port of 1/0/0:0 (VTG Half Duplex Left Side) <-> 1/0/1:0 (IDC Full Duplex Right Side) has been marked as reserved in Cisco IPICS and is used for the trunk radio hybrid configuration bridge.

T1 Loopback Left Side VTG half is set to lmr duplex half (for example, 1/0/0:0) with the multicast address of channel 2 VTG 239.193.1.0:21000. This channel is made available to VTGs. For proper operation, all voice ports that are associated with the T1 loopback should be configured with **lmr m-lead audio-gate-in** and the associated dial-peers should be configured with **no vad**. If you use VAD anywhere in the T1 loopback ports, you may lose the beginning of audio transmissions when the trunked radio is used in VTGs.



This portion of the bridge may require tuning to match the trunked radio systems that are in use. However, the following recommended settings should be sufficient for the majority of applications:

- **timing delay-voice tdm** command

Typically timing delay-voice tdm 600 gives good results. But if you know or can measure the actual trunkin radio channel access setup time and then add 100 ms to that value, you will obtain optimal performance.

- **timing hangover** command

Typically, timing hangover 620 provides good results when timing delay-voice tdm 600 is used. But if a new calculated value was used for timing delay-voice tdm, the new timing hangover value should be slightly longer.

- **timing ignore m-lead** command

Typically, timing ignore m-lead 100 provides good results. But if extra access tones are heard when trunked radios are in VTGs, you may want to increase this value. If this value is set too high, the tail end of the audio transmission may be chopped when the trunked radio is in a VTG.

The following example shows the voice port and dial-peer configuration for the half duplex side of the T1 loopback that is used for the trunked radio hybrid configuration solution for Cisco IPICS.

```
! Half Duplex Left Side DSO Port for VTG Use
!
voice-port 1/0/0:0
  voice-class permanent 1
  auto-cut-through
  lmr m-lead audio-gate-in
  lmr e-lead voice
  lmr duplex half
  no echo-cancel enable
  no comfort-noise
  timeouts call-disconnect 3
  timeouts wait-release 3
  timing hookflash-in 0
  timing hangover { 0 - 1000 } ! Typically {620}. Should be longer than timing
delay-voice tdm value.
  timing delay-voice tdm { 0 - 1500 } ! Typically {600}. Channel access time +100 mSec.
  timing ignore m-lead { 0 - 1000 } ! Typically {100}. If set to high you may chop the
tail end of audio.
  connection trunk 3104
  description Trunked Radio VTG Half Duplex Bridge(Disabled in Cisco IPICS)
!
! T1 Loopback Left Side VTG Half Duplex Dial Peer.
!
dial-peer voice 3104 voip
  description Trunked Radio VTG Half Duplex Channel
  destination-pattern 3104
  session protocol multicast
  session target ipv4:239.193.1.0:21000
  codec g711ulaw
  no vad ! Do not use any type of vad.
```

T1 Loopback Right Side IDC half should be set to no lmr duplex half (for example, 1/0/1:0) with the multicast address of channel 1 IDC 239.193.1.4:21000. This channel is made available to IDCs and allows users to hear the beeps and bonks that are specific to trunked radio systems. For proper operation, all voice ports that are associated with the T1 loopback should be configured with lmr **m-lead audio-gate-in** and the associated dial-peers should be configured with **no vad**. If you use VAD anywhere in the T1 loopback ports, you may lose of the beginning of audio transmissions when the trunk radio is used in VTGs.

The following example shows the voice port and dial-peer configuration for the full duplex side of the T1 loopback that is used for the trunked radio hybrid configuration solution for Cisco IPICS.

```
voice-port 1/0/1:0
  voice-class permanent 1
  auto-cut-through
  lmr m-lead audio-gate-in
  lmr e-lead voice
  no echo-cancel enable
  no comfort-noise
  timeouts call-disconnect 3
  timeouts wait-release 3
  timing hookflash-in 0
  timing hangover 80
  connection trunk 2104
  description Trunked Radio IDC Full Duplex Bridge (Disabled in Cisco IPICS)
!
! T1 Loopback Right Side Dial Peer (Do not use any type of vad).
!
dial-peer voice 2104 voip
  description Trunked Radio IDC Full Duplex Channel
  destination-pattern 2104
  session protocol multicast
  session target ipv4:239.193.1.4:21000
  codec g711ulaw
  no vad
```

This bridge allows you to use channel 1 IDC for endpoints and channel 2 VTG any time that you need to place this trunked radio into a VTG. Because channel 1 IDC is full duplex, endpoints hear the beeps and bonks. Because channel 1 VTG is half duplex, it allows for multiple half duplex radio channels (or their dummy partners) to be in VTGs without passing the splash tones back and forth, preventing ping ponging and other trunked radio issues.

Table 3-12 Cisco IPICS Trunked Channel Configurations

IPICS Trunked Channel Configurations	
Channel Label	Multicast Address
Channel 1 IDC	239.193.1.4:21000
Channel 2 VTG	239.193.1.0:21000



Note

The end user must also configure the IDC to not mute the received audio during PTT communication on the trunked channel to ensure that beeps and bonks are heard.

# Analog Tap Recording Configuration

The following sections provide information about recording multicast LMR traffic:

- [Recording Multicast LMR Traffic, page 3-69](#)
- [Recording Tap Cisco IOS Configuration, page 3-69](#)

## Recording Multicast LMR Traffic

Recording the traffic of radios that are connected to the Cisco IPICS network can be accomplished with readily available third-party recording solutions.

The [“Recording Tap Cisco IOS Configuration” section on page 3-69](#) explains how to configure an E&M port that is dedicated to providing an analog audio output to an external recording device. Typically, each radio channel should be recorded on its own recording track so that when the recording plays back, the end user hears only the radio traffic for the channel that was selected. If that radio channel was a member of a Cisco IPICS virtual talk group, the audio from all the members of that talk group would also be heard. To accomplish this type of channel-only recording, an E&M port is required for each radio channel that needs to be recorded. For example, if there are four radios, each connected to its own E&M port as the interface to the Cisco IPICS network, an additional four E&M ports are required if each channel needs to be recorded. In this case, eight E&M ports are required. If the recording device is in a location other than the radios, it may require a dedicated ISR to provide the analog taps for the recording device.

## Recording Tap Cisco IOS Configuration

When the configuration that is described in this section is used, the router captures the multicast traffic for a particular channel and converts it to an analog signal that can be sent to a recording device. If the recorder requires a signal to indicate when to start recording, the E-lead pin 7 can be employed. The E-lead corresponds to the PTT signal of the radio system, which indicates audio activity on the LMR system. If the recording device is continuous or triggered by the presence of audio, only pins 4 and 5 should be required. Typically four of the eight wires are employed.

[Table 3-13](#) shows the configuration for four of the eight wires.

**Table 3-13 Physical Connections For Recording Device**

Router RJ-45 Pin No.	Router Function	Category 5 Color Code	Router Function
1 <sup>1</sup>	Signal Battery (SB)	Orange	No Connection
2 <sup>1</sup>	M-Lead	White/Orange	No Connection
3 <sup>1</sup>	Ring	White/Green	No Connection
4	Ring-1	Blue	TX & RX Audio
5	Tip-1	White/Blue	TX & RX Audio
6 <sup>1</sup>	Tip	Green	No Connection
7	E-Lead	White/Brown	Start Recording
8	Signal Ground (SG)	Brown	Ground

1. Not used in this configuration.

The following example shows the E&M Voice-Port & Dial Peer configurations that are required for recording multicast traffic on an analog recording device.

In this example, type { 2 | 3 | 5 } typically is type 3, but see [Figure 3-3 on page 3-5](#), [Figure 3-4 on page 3-6](#), and [Figure 3-5 on page 3-7](#) to select the type that best matches your radio requirements. Input gain { -27 - 16 } typically is 10, but adjust this value as needed to best receive audio on Cisco IPICS endpoints. Output attenuation { -16 - 27 } typically is 10, but adjust this value as needed to best receive audio on radios. When connecting a radio to a voice port in an LMR gateway, you may need to make

adjustments to properly balance the audio levels. A radio typically provides gain adjustments, and the level of the signal from the radio to the voice port and the level of the signal from the voice port to the radio may require some adjustments on the radio and the voice port. When using a tone controlled radio, it is important to note that the tones that are sent from the LMR gateway to the radio also are affected by the voice ports output attenuation settings. When optimizing these settings to achieve the desired audio levels, take care to ensure that the voice port adjustments do not have an adverse effect on the level and quality of the tone signals.

```
ip multicast-routing
!
voice class codec 1
  codec preference 1 g729r8
  codec preference 2 g711ulaw
!
voice class permanent 1
  signal timing oos timeout disabled
  signal keepalive disabled
  signal sequence oos no-action
!
voice-port 0/2/0
  voice-class permanent 1
  auto-cut-through
  operation 4-wire
  type { 2 | 3 | 5 }
  signal lmr
  lmr m-lead audio-gate-in
  lmr e-lead voice
  bootup e-lead off
lmr duplex half
lmr led-on
output attenuation { -16 - 27 }
no echo-cancel enable
no comfort-noise
timeouts call-disconnect 3
timeouts wait-release 3
timing hookflash-in 10
timing hangover 80
connection trunk 11101
description Recording Tap Radio 0/2/0
threshold noise -40
!
dial-peer voice 11101 voip
  destination-pattern 11101
  session protocol multicast
  session target ipv4: { Multicast address of radio channel to be recorded }
  codec g711ulaw
  vad aggressive
```

## Cisco IPICS Integration with ISSI Gateways

The Cisco Instant Connect ISSI Gateway (ISSIG) is an optional Cisco Instant Connect component that enables voice interoperability between radio frequency subsystems that support the Inter-RF Subsystem Interface (ISSI).

The ISSIG includes the following components:

- P25 Gateway—Handles the transcoding between the G.711 codec of a multicast stream and the Improved Multi-Band Excitation (IMBE) codec.

- RFSS Gateway—Handles the ISSI between the ISSI Gateway and a remote radio frequency subsystem (RFSS).

Cisco IPICS is itself an RFSS in the ISSI.

The ISSIG provides these interoperability modes:

- Proxy mode—Enables any Cisco Instant Connect endpoint to interoperate with a P25 device and provides transcoding between G.711 and the IMBE codecs.
- Native mode—Enables the IDC to communicate directly to a P25 endpoint. Transcoding is not performed. Allows optional end-to-end encryption for this communication

For related information, see *Configure ISSI Gateway in IPICS Environment*, which is available at <https://www.cisco.com/c/en/us/support/unified-communications/instant-connect/products-technical-reference-list.html>.

## Cisco IPICS Integration with DFSI Gateways

The Cisco Digital Fixed Station Interface Gateway (DFSIG) is an optional Cisco Instant Connect component that enables voice interoperability between radio frequency subsystems that support conventional P25 radio systems.

The DFSIG provide provides several interoperability modes and includes the following components:

- P25 Gateway—Handles the transcoding between the G.711 codec of a multicast stream and the Improved Multi-Band Excitation (IMBE) codec
- Console Arbitrator (CAR)—Handles the implementation of the DFSI standard and interoperability with DFSI-capable fixed stations

For related information, see *Using a DFSI Gateway on IPICS*, which is available at <https://www.cisco.com/c/en/us/support/unified-communications/instant-connect/products-technical-reference-list.html>.

## Feature Support for Radios

Table 3-14 provides information about features that various radio models support. A dash (—) indicates that a feature is not supported. To determine additional information about supported radio models, contact your Cisco representative.

Table 3-14 Feature Support for Radios

	<b>Motorola: i355/i365</b>	<b>EF Johnson: 5300 series</b>	<b>ICOM: FR5000, F5062</b>	<b>TAIT: TM 8200 Series, TM 91XX, TM 94XX, MPT 1327 DIP</b>	<b>Sepura: SRG 3900</b>	<b>Cassidian / EADS/ Airbus: TMR880i</b>	<b>Selex: FC 3000</b>	<b>Jotron: TR-7750/ 25/10</b>	<b>Harris: CS 7000</b>
P25 Trunking	—	Supported	—	Supported on TM91xx and TM94xx	—	—	—	—	Supported
P25 Conventional	—	Supported	—	Supported on TM 91xx and TM 94xx	—	—	—	—	Supported
Analog Conventional	—	Supported	Supported	Supported on TM 8200 Series, TM 91xx, and TM 94xx	—	—	—	Supported	Supported
EDACS/ OpenSky	—	—	—	—	—	—	—	—	Supported
dPMR	—	—	Supported	—	—	—	—	—	—
Smartnet/ Smartzone trunking	—	Supported	—	—	—	—	—	—	—
iDEN	Supported	—	—	—	—	—	—	—	—
Tetra	—	—	—	—	Supported	Supported	Supported	—	—
MPT1327	—	—	—	Supported on MPT 1327 DIP	—	—	—	—	—
Talker ID Rx	Supported	Supported	Supported	Supported	Supported	Supported	Supported	—	—
Channels/ groups	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported	Supported
Private call	Supported	—	Supported	Supported on MPT 1327 DIP	Supported on MPT 1327 DIP	—	Supported on MPT 1327 DIP	—	—
Call alert	Supported	—	—	—	—	—	—	—	—

Table 3-14 Feature Support for Radios (continued)

	<b>Motorola: i355/i365</b>	<b>EF Johnson: 5300 series</b>	<b>ICOM: FR5000, F5062</b>	<b>TAIT: TM 8200 Series, TM 91XX, TM 94XX, MPT 1327 DIP</b>	<b>Sepura: SRG 3900</b>	<b>Cassidian / EADS/ Airbus: TMR880i</b>	<b>Selex: FC 3000</b>	<b>Jotron: TR-7750/ 25/10</b>	<b>Harris: CS 7000</b>
Short data	—	—	—	Supported on MPT 1327 DIP	—	—	—	—	—
Console Preemption	—	—	—	Supported on MPT 1327 DIP	—	—	—	—	—
Emergency Rx	—	Supported	Supported	Supported on MPT 1327 DIP	Supported	—	—	—	—
Secure/clear	—	Supported	Supported	—	Supported	—	—	—	—
Repeater/direct	—	Supported	—	—	—	—	—	—	—
Tx power	—	Supported	—	—	—	—	—	—	—
Scan	—	Supported	—	—	—	—	—	—	—
Monitor	—	Supported	—	—	—	—	—	—	—
Volume	—	—	—	—	—	—	—	—	—
Squelch	—	—	—	—	—	—	—	—	—
Key selection	—	—	—	—	—	—	—	—	—
Frequency entry	—	—	—	—	—	—	—	—	—







## Cisco IPICS Infrastructure Considerations

---

This chapter contains information about infrastructure issues that you must be aware of when you deploy Cisco IPICS.

For related information, see the following documents:

- IP multicast—See *Cisco IOS IP Multicast Configuration Guide, Release 12.4*:  
[http://www.cisco.com/en/US/products/ps6350/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6350/products_installation_and_configuration_guides_list.html)
- Quality of Service—See *Cisco IOS Quality of Service Solutions Configuration Guide, Release 12.4*:  
[http://www.cisco.com/en/US/products/ps6350/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6350/products_installation_and_configuration_guides_list.html)
- Voice Configuration—See *Cisco IOS Voice Configuration Library*:  
[http://www.cisco.com/en/US/products/ps6350/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6350/products_installation_and_configuration_guides_list.html)
- Hoot ‘n’ Holler—See *Hoot ‘n’ Holler Solution*:  
[http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns70/networking\\_solutions\\_package.html](http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns70/networking_solutions_package.html)

This chapter includes these topics:

- [WAN Considerations, page 4-1](#)
- [Multicast Routing](#)
- [Bandwidth Planning](#)
- [Quality of Service, page 4-8](#)
- [VPN in Deployment Scenarios, page 4-14](#)
- [Securing the Cisco IPICS Infrastructure, page 4-14](#)
- [Cisco IPICS Network Management System, page 4-15](#)

## WAN Considerations

To ensure the successful deployment of Cisco IPICS over a WAN, you must carefully plan, design, and implement the WAN. Make sure to consider the following factors:

- Delay—Propagation delay between two sites introduces 6 milliseconds (ms) per kilometer. Other network delays may also be present.

- **Quality of Service**—The network infrastructure relies on QoS engineering to provide consistent and predictable end-to-end levels of service for traffic. QoS-enabled bandwidth must be engineered into the network infrastructure.
- **Jitter**—Varying delay that packets incur through the network as a result of processing, queue, buffer, congestion, or path variation delay. Jitter for the multicast voice traffic must be minimized by using Quality of Service (QoS) features. For related information, see the [“Quality of Service” section on page 4-8](#).
- **Packet loss and errors**—The network should be engineered to provide sufficient prioritized bandwidth for all voice traffic. Standard QoS mechanisms must be implemented to avoid congestion and packet loss. For related information, see the [“Quality of Service” section on page 4-8](#).
- **Bandwidth**—Provision the correct amount of bandwidth between each site for the expected call volume. This bandwidth is in addition to bandwidth for other applications and traffic that share the network. The provisioned bandwidth must have QoS enabled to provide prioritization and scheduling for the different classes of traffic. In general, the bandwidth should be over-provisioned and under-subscribed.

## Multicast Routing

Cisco supports the Protocol Independent Multicast (PIM) routing protocol for both sparse mode (SM) and dense mode (DM). However, because of its periodic broadcast and prune mechanism, DM PIM is not recommended for production networks.

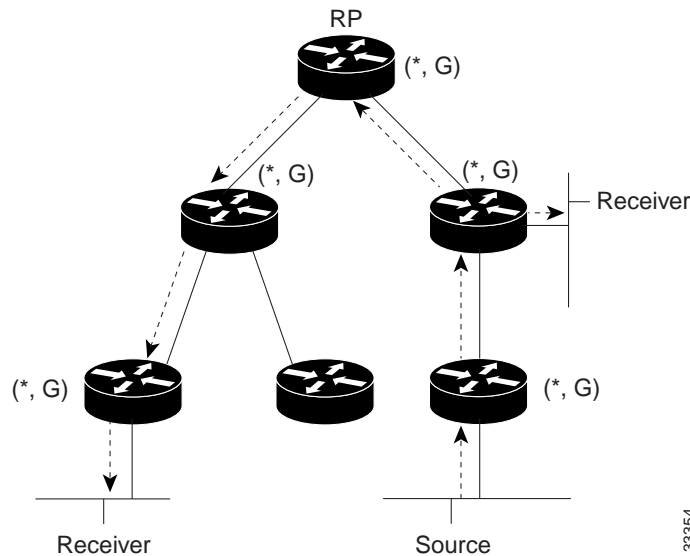
Cisco recommends using bidirectional PIM for Cisco IPICS. Bidirectional PIM is an extension of the PIM suite of protocols that implements shared sparse trees with bidirectional data flow. In contrast to PIM-sparse mode, bidirectional PIM avoids keeping source-specific states in a router and allows trees to scale to an arbitrary number of sources while requiring only minimal additional overhead.

The shared trees that are created in PIM SM are unidirectional. Therefore, a source tree must be created to bring a data stream to the rendezvous point (RP), which is the root of the shared tree. Then the data can be forwarded down the branches to receivers. In the unidirectional mode, source data cannot flow up the shared tree toward the RP.

In bidirectional mode, traffic is routed only along a bidirectional shared tree that is rooted at the RP for the group. In bidirectional PIM, the IP address of the RP acts as the key to having all routers establish a loop-free spanning tree topology rooted in that IP address. This IP address does not need to be a router. It can be any unassigned IP address on a network that is reachable throughout the PIM domain.

[Figure 4-1](#) shows a bidirectional shared tree. In this example, data from the source can flow up the shared tree (\*, G) toward the RP, and then down the shared tree to the receiver. There is no registration process so source tree (S, G) is created.

Figure 4-1 Bidirectional Shared Tree



Bidirectional PIM is derived from the mechanisms of PIM SM and has many of the same shared tree operations. Bidirectional PIM also has unconditional forwarding of source traffic toward the RP upstream on the shared tree, but no registering process for sources, as provided by PIM SM. These modifications are necessary and sufficient to allow forwarding of traffic to all routers based only on the (\*, G) multicast routing entries. Bidirectional PIM eliminates any source-specific state and allows scaling to an arbitrary number of sources.

In a Cisco IPICS deployment, bidirectional PIM solves the problem of scalability in the following ways:

- Forwarding traffic based on the shared tree (\*, G)—This functionality helps scale the multicast routing table by creating a single routing entry per channel. In SM, a routing entry is created per group and per source. So, for example, if a channel has 100 participants, it will have 101 multicast routing entries in the routing table. With bidirectional PIM, only a single multicast routing entry in the routing table is created, regardless of the number of participants.
- Basing the Reverse Path Forwarding (RPF) decision on the route to the RP—In SM, RPF decisions about (S, G) entries are based on the source address of the flow, and for bidirectional (\*, G), RPF decisions are based on the RP. This functionality eliminates the need to configure hundreds of ip mroute entries to force multicast traffic on the Cisco IPICS Permanent Virtual Circuit (PVC). With bidirection, forcing the multicast traffic on the Cisco IPICS PVC is achieved by tuning the unicast routing protocol to prefer the Cisco IPICS PVC as the best route to reach the RP.

If you are using Auto-RP and a Cisco IOS release earlier than 12.2(7), sparse dense mode is required. If you are using Auto-RP and Cisco IOS release 12.2(7) or later, use the **sparse mode** and **ip pim auto rp listener** commands. Multicast types other than auto-rp can use sparse mode.



#### Note

Cisco recommends that static RPs be used in a large deployment. This approach helps with control of the multicast tree and provides a stable and a deterministic path for Cisco IPICS traffic.

# Bandwidth Planning

To ensure sufficient bandwidth for the operation of Cisco IPICS, consider the following issues as you plan and deploy your network. These issues include:

- Codec used for VoIP—See the [“Codecs” section on page 4-4](#)
- The number of voice streams that will be mixed—See the [“Mixing Voice Streams” section on page 4-8](#)

In addition, consider the guaranteed bandwidth that is available on the VoIP network. Make sure to take into account both LAN and WAN bandwidth, and to consider factors such as Frame Relay, Committed Information Rate (CIR) or Asynchronous Transfer Mode Peak Cell Rate (ATM PCR), Sustained Cell Rate, and burst. For additional information see the [“Quality of Service” section on page 4-8](#).

## Codecs

Cisco IPICS uses either the G.711 or G.729a codec. This section provides the following information about codecs:

- [Choosing a Codec, page 4-4](#)
- [Calculating Codec Bandwidth Use, page 4-5](#)



**Note**

The Cisco IPICS policy engine supports only the G.711 u-law codec.

## Choosing a Codec

When choosing a codec for Cisco IPICS, consider the issues that [Table 4-1](#) describes.

**Table 4-1** *Codec Considerations*

	G.711	G.729a	iLBC
Voice Quality	<ul style="list-style-type: none"> <li>• Assuming that good VoIP conditions exist, delivers a mean opinion score (MOS) of 4.1 with a high degree of consistency.</li> <li>• Does tandem well, so no voice quality degradation results from transcoding.</li> </ul>	<ul style="list-style-type: none"> <li>• Assuming that good VoIP conditions exist, typically delivers a Mean Opinion Score (MOS) of 3.7 and can cause more unpredictable results than G.711.</li> <li>• Does not perform as well as G.711 under packet loss conditions. For example, a 3% packet loss rate can have a larger effect on voice quality than a similar packet loss rate under G.711.</li> <li>• Does not tandem as well as G.711.</li> <li>• Transcoding decreases voice quality from a MOS of 3.7 to 3.2.</li> </ul>	<ul style="list-style-type: none"> <li>• The iLBC (internet Low Bitrate Codec) is a standard high-complexity speech codec with built-in error correction functionality that helps the codec perform in networks with high-packet loss.</li> <li>• This codec suitable for robust voice communication over IP.</li> </ul>

Table 4-1 Codec Considerations (continued)

	<b>G.711</b>	<b>G.729a</b>	<b>iLBC</b>
Bandwidth	<ul style="list-style-type: none"> <li>Typically consumes 3 times more bandwidth than G.729a.</li> </ul>	<ul style="list-style-type: none"> <li>Offers bandwidth savings over G.711.</li> <li>A Cisco IPICS deployment that connects sites via a WAN link may use G.729a to reduce WAN bandwidth use, which also may reduce WAN costs.</li> </ul>	Designed for narrow band speech and results in a payload bit rate of 15.20 kbps with an encoding length of 20 ms.

## Calculating Codec Bandwidth Use

This section explains how to calculate bandwidth use for codecs.

By default, Cisco IOS sends all VoIP traffic (that is, media traffic that uses RTP) at a rate of 50 packets/second. In addition to the voice sample, each packet includes an IP, UDP, and RTP header, which adds 40 bytes to the packet. Layer 2 headers (such as Frame Relay, Point-to-Point Protocol, and Ethernet) also add bytes to each packet.

The amount of bandwidth that is consumed by a VoIP call depends on the codec that is used, and can be calculated as follows. Make sure to also add the appropriate number of bytes for the layer 2 header to determine the actual bandwidth that is consumed.

### **G.729a (8 KB CS-ACELP)**

50 packets/second

20 ms samples / packet = 20 bytes

AP/UDP/RTP headers/packet = 40 bytes

(20 bytes [payload] + 40 bytes [headers]) \* 50 packets/second = 3,000 bytes \* 8 bits = 24 kbps

### **G.711 (64 KB PCM)**

50 packets/second

20 ms samples / packet = 160 bytes

AP/UDP/RTP headers/packet = 40 bytes

(160 bytes [payload] + 40 bytes [headers]) \* 50 packets/second = 10,000 bytes \* 8 bits = 80 kbps

Table 4-2 shows sample bandwidth consumption. In this table:

- The examples assume a payload size (bytes) of 20 ms samples per packet with 50 packets per second.
- The value *n* is equal to the number of voice streams in a session.
- The encompassed bandwidth includes IP/UDP/RTP headers (40 bytes) in the bandwidth calculation.
- Compressed RTP (cRTP) reduces the IP/UDP/RTP headers to between 2 and 4 bytes per packet. The calculation of compressed bandwidth uses 4 bytes for a compressed IP/UDP/RTP headers per packet.
- Make sure to add the appropriate number of bytes for the layer 2 header to determine the actual bandwidth consumed.

Table 4-2 Sample Bandwidth Usage

Codec	Payload Size (bytes)	Bandwidth/Voice Stream (kbps)		RTCP Bandwidth per Cisco IPICS Session (kbps)	Example: 1 Voice Stream in a Session (kbps)	
		Uncompressed	Compressed		Uncompressed	Compressed
G.729a	20	24	9.6	3.6	27.6	13.2
G.711	160	80	65.6	12.0	92.0	77.6

According to RFC 1889 (*RTP: A Transport Protocol for Real-Time Applications*), the RTCP traffic for any RTP stream is limited to a maximum of 5% of the voice stream (RTP + RTCP). This limitation applies to the three streams that participate in a Cisco IPICS session. Therefore, the RTCP Bandwidth per Cisco IPICS Session is calculated by multiplying the bandwidth per voice stream by 3 and then multiplying that product by 0.05.

When you design a Cisco IPICS network within a campus network, you should not run into any bandwidth-related issues because IP multicast is used to replicate a voice stream and map it to an IP multicast group, in which UMS resources are not used. When remote users connect over a WAN link that is not multicast enabled, the UMS converts a multicast stream to an IP unicast stream, which conserves bandwidth on the WAN. When the IP unicast voice stream arrives, the UMS converts the IP unicast stream back to a multicast stream. When the voice streams traverse a WAN, the UMS resources are used.

**Note**

Each Cisco IPICS dial engine port uses the G.711 codec. Bandwidth calculations must consider the G.711 connectivity between the Cisco IPICS server and connected endpoints.

## cRTP, Variable-Payload Sizes and Aggressive VAD

There are several methods that you can use to modify the bandwidth consumed by a call. These methods include the following:

- [RTP Header Compression, page 4-6](#)
- [Adjustable Byte Size of the Voice Payload, page 4-7](#)
- [Aggressive Voice Activity Detection, page 4-7](#)

### RTP Header Compression

As described in the “Codecs” section on page 4-4, IP/UDP/RTP headers add 40 bytes to each packet. However, a packet header is typically unchanged throughout a call. You can enable cRTP for VoIP calls, which reduces the size of IP/UDP/RTP headers to 2 to 4 bytes per packet.

For detailed information about cRTP, see *Understanding Compression (Including cRTP) and Quality of Service*, which is available at this URL:

[http://www.cisco.com/en/US/tech/tk543/tk762/technologies\\_tech\\_note09186a0080108e2c.shtml](http://www.cisco.com/en/US/tech/tk543/tk762/technologies_tech_note09186a0080108e2c.shtml)

## Adjustable Byte Size of the Voice Payload

You can control the size of the voice payload that is included in each Cisco IPICS voice packet. To do so, use the bytes parameter in a VoIP dial peer. For example:

```
dial-peer voice 1 voip
destination-pattern 4085551234
codec g729r8 bytes 40
session protocol multicast
session target ipv4:239.192.1.1:21000
```

Modifying the number of bytes per packet changes the number of packets that are sent per second.

For a G.729 call with voice payload size per packet of 20 bytes (160 bits), 50 packets need to be transmitted every second ( $50 \text{ pps} = (8 \text{ Kbps}) / (160 \text{ bits per packet})$ ), that is:

$8 * 1000 \text{ bits per second} / 160 \text{ bits per packet} (20 \text{ bytes} * 8 \text{ bits per byte}) = 50 \text{ pps}$



**Note**

Increasing payload size increases the delay per sample by the same amount. For example, increasing payload size from 20 ms to 40 ms increases the delay per sample by 20 ms.

## Aggressive Voice Activity Detection

Voice Activation Detection (VAD) is a mechanism that allows a DSP to dynamically sense pauses in conversation. When such pauses occur, no VoIP packets are sent into the network. VAD can reduce the amount of bandwidth used for a VoIP call.

Although VAD conserves bandwidth in VoIP, it disrupts and marginalizes Cisco IPICS signaling, which is used for LMR and PTT packet streams. Be aware of this issue if you use VAD in a Cisco IPICS deployment.

When configuring LMR gateway ports, VAD should not be used if the radio supports Carrier Operated Relay (COR) or Carrier Operated Signal (COS) signaling. Radios that support COR/COS signaling can provide hardwired signaling to the LMR port to start generating packets. Using COR/COS gating is an efficient way to control the audio input and to avoid the possibility of dropping short bursts of voice data that may fall below the VAD activation values.

Each voice port has different environmental noises and different users, which can cause a wide variation in noise and speech levels. Conventional VAD can manage these variations, but it is designed for unicast. Conventional VAD usually prefers over-detection to under-detection, as good voice quality is typically given precedence over bandwidth conservation. But in a multicast environment, over-detection and under-detection are not desirable because they degrade voice quality.

Aggressive VAD can be used in a multicast environment to avoid over-detection. With aggressive VAD, when a DSP detects signals with an unknown signal-to-noise ratio (SNR), the DSP does not transmit any spurious packets. With conventional VAD, when the DSP detects signals with an unknown SNR, the DSP continues to transmit packets, which can cause unwanted traffic to take over all slots that are available for voice streams.

You can enable aggressive VAD by enabling the `vad aggressive` configuration setting under a dial peer as follows:

```
dial-peer voice 10 voip
destination-pattern 111
session protocol multicast
session target ipv4:239.192.1.1:21000
vad aggressive
```

## Mixing Voice Streams

As described in the [“Virtual Talk Groups” section on page 2-15](#), the DSPs in a Cisco IPICS deployment can mix up to three voice streams. However, the DSPs do not perform a summation function. So, for example, if three G.729a streams (24 KB each with headers) are received by a router or gateway, the mixed stream would consume 72 KB bandwidth. Even though each user in a VTG or a channel in the VTG receives a single mixed audio stream, the DSP does not send a single 24 KB stream.

It is important to consider this issue when you plan bandwidth requirements in a Cisco IPICS network. It is especially important when planning WAN bandwidth requirements, which can be more expensive and less available than LAN bandwidth.

Because the Cisco Hoot ‘n’ Holler feature mixes up to three voice streams at a time, you do not need to provision voice bandwidth for more than three times the per-call bandwidth for each WAN site that includes routers with the Cisco Hoot ‘n’ Holler feature.

**Note**

---

An audio channel that is mixed through a VTG experiences an additional 60 ms of delay.

---

## Quality of Service

There are several QoS features that should be enabled so that a Cisco IPICS deployment can deliver toll-quality voice. This section provides an overview of these features for Point-to-Point Protocol (PPP) and Frame Relay WAN topologies and for deployments on LAN media.

This section includes these topics:

- [QoS Overview, page 4-8](#)
- [Cisco IOS Queuing Techniques, page 4-9](#)
- [QoS for a LAN, page 4-10](#)
- [QoS at the WAN Edge, page 4-11](#)
- [Policing, page 4-11](#)
- [Queuing, page 4-11](#)
- [Trust Boundaries, page 4-12](#)

## QoS Overview

QoS provides consistent voice latency and minimal packet loss. The following recommendations apply to QoS in campus LAN and WAN environments:

- Classify voice RTP streams as expedited forwarding (EF) or IP precedence 5 and place them into a priority queue on all network elements
- Classify voice control traffic as assured forwarding 31 (AF31) or IP precedence 3 and place it into a second queue on all network elements

As you design a VoIP network to deploy real-time applications such as Cisco IPICS, consider the following issues, which can affect voice quality:



- **Packet loss**—Causes voice clipping and skips. The industry-standard codec algorithms that are used in DSPs can correct for up to 30 ms of lost voice. Cisco VoIP technology uses 20 ms samples of voice payload per VoIP stream. Therefore, for the codec correction algorithms to be effective, only a single packet can be lost during any time. Packet loss can be a significant problem for real-time applications because they are not designed to retransmit packets.
- **Delay**—Causes either voice quality degradation due to the end-to-end voice latency or packet loss if the delay is variable. If the delay is variable, such as queue delay in bursty data environments, there is a risk of jitter buffer overruns at the receiving end. Longer delays can cause buffer overflow and underflow, and unnatural pauses in human conversations. Because Cisco IPICS supports a PTT service, the typical one-way delay requirement of 150 ms as recommended in the International Telecommunication Union (ITU) G.114 specification does not directly apply. PTT users are aware of radio protocol, so a more reasonable delay is 400 ms as outlined in the ITU G.173 specification.
- **Jitter**—Variable delay. While some delay is acceptable, delay that constantly changes can cause inconsistent and inefficient DSP buffering. It also can cause inconsistent voice quality.
- **Ability to Prioritize VoIP traffic**—Involves the use of queuing techniques, such as IP RTP Priority and Low-Latency Queuing, that are available in Cisco IOS.
- **Ability to make VoIP traffic best fit the LAN or WAN network**—Involves making sure that small VoIP packets do not get delayed behind large data packets (an event called *serialization*).

If networks are designed and built to provide low delay, limited jitter, and limited packet loss, real-time applications such as Cisco IPICS solution can be successful.

## Cisco IOS Queuing Techniques

Cisco IOS provides a wide variety of QoS features. The following features are particularly useful for a Cisco IPICS deployment:

- [IP RTP Priority, page 4-9](#)
- [Low Latency Queuing, page 4-10](#)

For more detailed documentation about IP RTP Priority, see the “Congestion Management Overview” chapter in *Cisco IOS Quality of Service Solutions Configuration Guide*, which is available at this URL:

[http://www.cisco.com/en/US/products/ps6350/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6350/products_installation_and_configuration_guides_list.html)

### IP RTP Priority

IP RTP Priority can be applied to point-to-point links and to Frame Relay PVCs. It allows you to provision a fixed amount of bandwidth (in KB) that is always available for Cisco IPICS packets. If there are no Cisco IPICS packets present in the network (that is, nobody is speaking), the bandwidth is available to other data applications. This predefined amount of bandwidth is serviced as a strict priority-queue within the overall structure of Weighted-Fair Queuing (WFQ). The entrance criteria to this priority queue is a range of UDP ports that are used by Cisco IPICS to send IP packets.

Cisco IPICS uses the UDP port that is selected on the VoIP dial peer, and the next sequential port. The ports can range from 21000 through 65534. The first port must be an even number within this range.

The following example shows the UDP port (24100) defined in the VoIP dial-peer, so the range for the IP RTP Priority is 24100-24101:

```
dial-peer voice 1 voip
destination-pattern 1111
session protocol multicast
```

```

codec g711ulaw
session target ipv4:239.10.0.100:24100
!
interface serial 0/0
ip address 10.1.1.1
ip rtp priority 24100 2 64

```

## Low Latency Queuing

Low-Latency Queuing (LLQ) applies to point-to-point links and to Frame Relay PVCs. LLQ creates a strict priority queue, as does IP RTP Priority, but LLQ applies the strict priority queue as a service-class within Class-Based Weighted Fair Queueing (CBWFQ). The functionality of fixed allocation but dynamic usage is again similar to IP RTP Priority.

A primary difference between IP RTP Priority and LLQ is that LLQ allows the usage of access control lists (ACLs) as the entrance criteria to the priority queue. This capability provides you with flexibility in determining what types of traffic are allowed into the priority queue.

The following example shows how LLQ is used to prioritize Cisco IPICS traffic:

```

access-list 102 permit udp host 10.1.1.1 host 239.10.0.100 range 24100 24101
!
class-map voice
match access-group 102
!
policy-map policy1
class voice
priority 50
!
multilink virtual-template 1
!
interface virtual-template 1
ip address 172.17.254.161 255.255.255.248
no ip directed-broadcast
no ip mroute-cache
service-policy output policy1
ppp multilink
ppp multilink fragment-delay 20
ppp multilink interleave
!
interface serial 2/0
bandwidth 256
no ip address
no ip directed-broadcast
encapsulation ppp
no fair-queue
clockrate 256000
ppp multilink
multilink-group 1

```

## QoS for a LAN

When you deploy QoS in a LAN, classify and mark applications as close to their sources as possible. For example, implement QoS in a Cisco Layer 2 switch for Cisco Unified IP Phones that connect to the Cisco IPICS server via multicast. For LMRs, implement QoS in the dial peer that is configured for the E&M port that connects to the radios.

To classify and mark applications, follow these recommendations:

- Use Differentiated Services Code Point (DSCP) markings whenever possible.

- Follow standards-based DSCP per-hop behaviors (PHB) to ensure interoperability and provide for future expansion. These standards include:
  - RFC 2474 Class Selector Codepoints
  - RFC 2597 Assured Forwarding Classes
  - RFC 3246 Expedited Forwarding.

## QoS at the WAN Edge

QoS should be configured at the WAN edge so that QoS settings are forwarded to the next-hop router. When you configure QoS at the WAN edge, follow these recommendations:

- If the combined WAN circuit-rate is significantly below 100 Mbps, enable egress shaping on the Cisco Layer 2 switches (when supported)
- If the combined WAN circuit-rate is significantly below 100 Mbps and the Cisco Layer 2 switch does not support shaping, enable egress policing (when supported)

## Policing

Policing is configured so that traffic of a certain class that exceeds the allocated bandwidth is marked as discard eligible (DE) or is dropped, so it prevents denial of service (DoS) or a virus attacks. When you configure policing, follow these recommendations.

- Police traffic as close to their sources as possible.
- Perform markdown according to standards-based rules, whenever supported.
- RFC 2597 specifies how Assured Forwarding traffic classes should be marked down (AF11 > AF12 > AF13). You should follow this specification when DSCP-Based WRED is supported on egress queues.
- Non-AF classes do not have a markdown scheme defined in standards, so Scavenger-class remarking is a viable option.
- Profile applications to determine what constitutes “normal” or “abnormal” flows (within a 95% confidence interval).
- Deploy campus access-edge policers to remark abnormal traffic to Scavenger.
- Deploy a second-line of defense at the distribution-layer via per-user microflow policing.
- Provision end-to-end “less-than-best-Effort” scavenger-class queuing policies.

## Queuing

Queuing is a method of buffering traffic so that the traffic does not overflow the allocated bandwidth on a WAN link. To provide service guarantees, enable queuing at any node that has the potential for congestion.

When you enable queuing, follow these recommendations:

- Reserve at least 25% of the bandwidth of a link for the default best effort class.
- Limit the amount of strict-priority queuing to 33% of the capacity of a link.
- Whenever a Scavenger queuing class is enabled, assigned to it a minimal amount of bandwidth.

- To ensure consistent per-hop behavior (PHB), configure consistent queuing policies in the campus, WAN, and VPN, according to platform capabilities.
- Enable WRED on all TCP flows, if supported. DSCP-based WRED is recommended.

## Trust Boundaries

The Cisco IPICS QoS infrastructure is defined by using a trust boundary. For detailed information about trust boundary concepts, see *Cisco Collaboration System 11.x Solution Reference Network Designs (SRND)*, which is available at this URL:

[http://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/cucm/srnd/collab11/collab11.html](http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11.html)

A trust boundary can include LMRs, and Cisco Unified IP Phones. IP precedence should be marked for Cisco Unified IP Phones, with a suggested value of 5 for voice traffic (such as RTP) and 3 for voice signaling (such as SIP or SCCP).

For a LMR PTT client, an LMR gateway marks the traffic coming from E&M ports to IP precedence 5 as follows:

```
voice-port 1/0/0
 voice class permanent 1
 connection trunk 111
 operation 4-wire
!
dial-peer voice 111 voip
 destination-pattern 111
 session protocol multicast
 session target ipv4:239.111.0.111:21000
 ip precedence 5
!
```

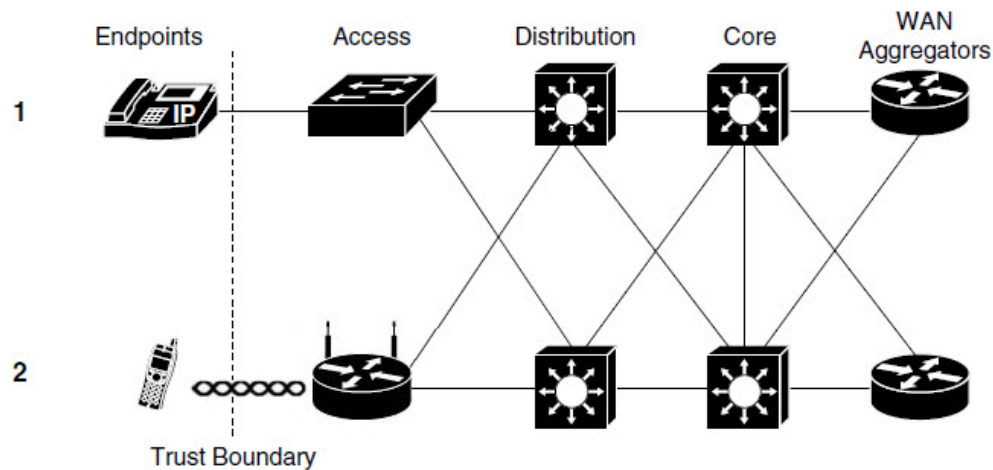
Cisco IPICS traffic that flows from an LMR or Cisco Unified IP Phone aggregates on an access switch, and QoS configuration is applied on this switch. Once marked, these values for IP precedence are honored throughout out the network.

If one of the Cisco IPICS trusted endpoint is located in the PSTN, these endpoints are connected through a voice gateway. Cisco voice gateways can set IP precedence and DSCP values for voice control and bearer traffic to 3 (AF31/SC3) and 5 (EF/CS5) respectively.

VoIP bearer traffic is placed in a strict priority queue, when possible. The boundary nodes police at the ingress level to rate-limit the VoIP traffic to avoid potential bandwidth exhaustion and the possibility of DoS attack through priority queues.

Figure 4-2 shows a trust boundary.

Figure 4-2 Trust Boundary



1 Trusted IP Phone PTT Endpoint

2 Trusted Mobile Client Endpoint

The following example shows access layer QoS configuration for a Cisco Catalyst 3550. This example also applies to later Cisco Catalyst 3xxx switch models.

```
CAT3550(config)#mls qos map policed-dscp 0 24 46 to 8
! Excess traffic marked 0 or CS3 or EF will be remarked to CS1
CAT3550(config)#
CAT3550(config)#class-map match-all IPICS-VOICE
CAT3550(config-cmap)# match access-group name IPICS-VOICE
CAT3550(config)#policy-map IPICS-PTTC
CAT3550(config-pmap)#class IPICS-VOICE
CAT3550(config-pmap-c)# set ip dscp 46
! VoIP is marked to DSCP EF
CAT3550(config-pmap-c)# police 128000 8000 exceed-action policed-dscp-transmit
! Out-of-profile IPICS VoIP (G711) is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)#class IPICS-SIGNALING
CAT3550(config-pmap-c)# set ip dscp 24
! Signalling is marked to DSCP CS3
CAT3550(config-pmap-c)# police 32000 8000 exceed-action policed-dscp-transmit
! Out-of-profile Signalling is marked down to Scavenger (CS1)
CAT3550(config-pmap-c)#class class-default
CAT3550(config-pmap-c)# set ip dscp 0
CAT3550(config-pmap-c)# police 5000000 8000 exceed-action policed-dscp-transmit
! Out-of-profile data traffic is marked down to Scavenger (CS1) 50000 (Depends on per
customer design and requirements)
CAT3550(config-pmap-c)# exit
CAT3550(config-pmap)#exit
CAT3550(config)#
CAT3550(config)#interface range FastEthernet0/1 - 48
CAT3550(config-if)# service-policy input IPICS-PTTC
! Attaching the policy map IPICS-PTTC to the interface range
CAT3550(config-if)#exit
CAT3550(config)#
CAT3550(config)#ip access-list extended IPICS-VOICE
! Extended ACL for the IPICS Address/Port ranges
CAT3550(config-ext-nacl)#
permit udp 233.0.0.0 0.255.255.255 233.0.0.0 0.255.255.255 range 21000 65534
```

```

permit udp 233.0.0.0 0.255.255.255 239.0.0.0 0.255.255.255 range 21000 65534
permit udp 239.0.0.0 0.255.255.255 233.0.0.0 0.255.255.255 range 21000 65534
permit udp 239.0.0.0 0.255.255.255 239.0.0.0 0.255.255.255 range 21000 65534
CAT3550(config-ext-nacl)#ip access-list extended IPICS-SIGNALING
! Extended ACL for the remote IDC clients
CAT3550(config-ext-nacl)# permit udp <RMS IP Address> <Any > eq 5060
! Extended ACL for the PSTN clients
CAT3550(config-ext-nacl)# permit udp <VoiceGW IP Address> <Any > eq 5060
CAT3550(config-ext-nacl)# permit tcp <Voice GW IP Address> <Any > eq 1720
CAT3550(config-ext-nacl)#end
CAT3550#

```

## VPN in Deployment Scenarios

A Cisco IPICS deployment can include a VPN implementation for mobile clients.

For the mobile client, audio cannot be transmitted bidirectionally on a 3G, 4G, or LTE network because certain providers block the audio on their data networks. Implementing a VPN tunnel between the Cisco IPICS server and the mobile client allows bidirectional transmission of audio. (Bidirectional audio quality depends on the service provider.)

In addition, if a IPICS server typically resides in an enterprise network, the mobile client must be able to reach it over a public network. There two methods by which the mobile client can reach the Cisco IPICS server over a wireless network or a 3G network. For a wireless connect, ensure that the wireless network can access the CISCO IPICS Server. If this connectivity is not available, the mobile client should be able to use its own VPN client and create a tunnel to the Cisco IPICS server. For a 3G network connection, a VPN client is required on the mobile client to for access to the Cisco IPICS server.

To allow the mobile client to contact the Cisco IPICS server, the server must have its domain name resolve to an IP address. The mobile client must be able to contact a DNS server that is supplied by a service provider or by the VPN configuration.

For related information about VPNs, see the following documentation:

- *Cisco AnyConnect Secure Mobility Solution Guide:*  
[http://www.cisco.com/c/dam/en/us/td/docs/security/wsa/wsa7-0/user\\_guide/AnyConnect\\_Secure\\_Mobility\\_SolutionGuide.pdf](http://www.cisco.com/c/dam/en/us/td/docs/security/wsa/wsa7-0/user_guide/AnyConnect_Secure_Mobility_SolutionGuide.pdf)
- “General VPN Setup” chapter in *Cisco ASA 5500 Series Configuration Guide using ASDM:*  
[http://www.cisco.com/c/en/us/td/docs/security/asa/asa83/asdm63/configuration\\_guide/config/vpn\\_gen.html](http://www.cisco.com/c/en/us/td/docs/security/asa/asa83/asdm63/configuration_guide/config/vpn_gen.html)

## Securing the Cisco IPICS Infrastructure

The following sections provide information about providing system security for Cisco IPICS:

- [Secure Socket Layer, page 4-15](#)
- [Firewalls and Access Control Lists, page 4-15](#)
- [Other Security Recommendations, page 4-15](#)

## Secure Socket Layer

Cisco IPICS uses Secure Socket Layer (SSL) to encrypt communications with the Cisco IPICS server. The browser with which you access the Cisco IPICS Administration Console uses HTTPS. To enforce SSL, you must install a certificate on the Cisco IPICS server. You can use a self-signed certificate or, to impose additional security, you can purchase and set up a digitally-signed certificate.

For additional information, see the “Installing Third Party Certificates on the Cisco IPICS Server” section in *Cisco IPICS Server Installation and Upgrade Guide, Release 4.10(2)*.

## Firewalls and Access Control Lists

Use a firewall and access control lists (ACLs) in front of the Cisco IPICS server and other Cisco IPICS components to add an extra layer of security. For example, you can use a firewall or an ACL to allow only call control and management packets to reach the Cisco IPICS server, and block unnecessary traffic such as Telnet or TFTP traffic. You can use ACLs to allow only the source addresses that are supposed to access your network.

When you use a firewall, it must support state-full inspection of voice signaling protocol. Cisco IPICS and a firewall must only open the ports needed to support for this application. In addition, make sure that the firewall supports application layer gateway (ALG) capabilities. ALG inspects signaling packets to discover what UDP port an RTP stream is going to use and dynamically opens a pinhole for that UDP port.

## Other Security Recommendations

For additional security in a Cisco IPICS network, follow these recommendations:

- Use Terminal Access Controller Access-Control System+ (TACACS+) and Remote Authentication Dial In User Service (RADIUS) to provide highly secure access in your network.
- Do not rely only on VLANs for separation; also provide layer 3 filtering at the access layer of your network.
- Use VLANs and IP filters between your voice and data network.
- Use out of band management switches and routers with SSH, HTTPS, out-of-band (OOB), permit lists, and so on to control who is accessing your network devices.
- Disable unused switch ports on the LAN switches and place them in an unused VLAN so that they are not misused.
- Use spanning tree (STP) attack mitigation tools such as Bridge Protocol Data Unit (BPDU) Guard and Root Guard.
- Disperse critical resources to provide redundancy.
- Provide limited and controlled access to power switches.

## Cisco IPICS Network Management System

When you plan for managing and monitoring a Cisco IPICS network, define the parameters that can be operatively monitored in the Cisco IPICS environment. You can use the outputs from these parameters to establish a set of alarms for spontaneous problems, and to establish a proactive, early warning system.

As you develop a management and monitoring policy for your network, take these actions:

- For each component in the network, define the parameters that must be monitored on the component
- Select the network management and monitoring tools that are appropriate for monitoring the parameters that you defined

## Managing the Overall Network

The Cisco Multicast Manager (CMM) is a web-based network management application that is designed to aid in the monitoring and troubleshooting of multicast networks. Cisco Multicast Manager includes the following features and benefits:

- Early warning of problems in multicast networks
- In-depth troubleshooting and analysis capabilities
- On demand, real time and historical reporting capabilities
- Optimization of network utilization and enhancement of services delivery over multicast enabled networks

CMM can monitor all multicast-capable devices that are running Cisco IOS, including Layer 2 switches. For more detailed information about CMM, see this URL:

<http://www.cisco.com/en/US/products/ps6337/index.html>

If you use Cisco Unified IP Phones as PTT clients in your Cisco IPICS network, you can use various IP Telephony (IPT) management tools to manage these devices. For example, you can use Cisco Unified Operations Manager (CUOM) to provide real-time, detailed fault analysis specifically designed for Cisco IPT devices. This tool evaluates the health of IPT implementations and provides alerting and notification of problems and areas that should be addressed to help minimize IPT service interruption. IPT management solution also identifies the underutilized or imbalanced gateway resources, and provides historical trending and forecasting of capacity requirements.

Other items to monitor in a Cisco IPICS network include the following:

- Cisco IPICS server health
- Cisco IPICS services health
- IP gateway health
- Cisco Unified Communications Manager functionality
- QoS monitoring
- L2/L3 switches and applications





## Understanding Dial Peers

Dial peers identify call source and destination endpoints and define the characteristics that are applied to each call leg in a call connection. Understanding the principles behind dial peers can increase your understanding of how Cisco IPICS works.

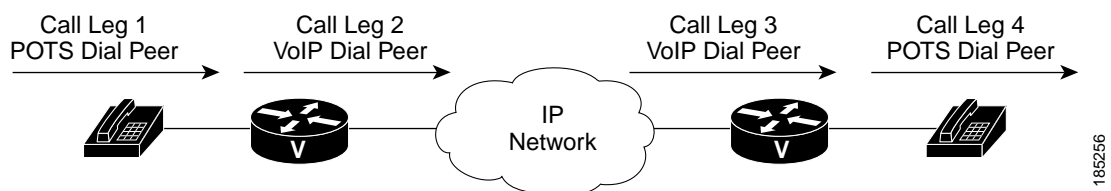
This chapter includes these topics:

- [Dial Peer Call Legs, page 5-1](#)
- [Inbound and Outbound Dial Peers, page 5-2](#)
- [Destination Pattern, page 5-3](#)
- [Session Target, page 5-3](#)
- [Configuring Dial Peers for Call Legs, page 5-3](#)
- [Matching Inbound and Outbound Dial Peers, page 5-3](#)

### Dial Peer Call Legs

A traditional voice call over the Public Switched Telephone Network (PSTN) uses a dedicated 64 KB circuit end-to-end. In contrast, a voice call over the packet network is made up of discrete segments, or *call legs*. A call leg is a logical connection between two routers or between a router and a telephony device. A voice call comprises four call legs, two from the perspective of the originating router and two from the perspective of the terminating router, as shown in [Figure 5-1](#).

**Figure 5-1** *Dial Peer Call Legs*



A dial peer is associated with each call leg. Attributes that are defined in a dial peer and applied to the call leg include codec, Quality of Service (QoS), and Voice Activation Detection (VAD). To complete a voice call, you must configure a dial peer for each of the four call legs in the call connection.

Depending on the call leg, a call is routed by using one of these dial peer types:

- **POTS (Plain Old Telephone Service)**—Dial peer that defines the characteristics of a traditional telephony network connection. POTS dial peers map a dialed string to a specific voice port on the local router, normally the voice port connecting the router to the local PSTN, private branch exchange (PBX), or telephone.
- **Voice-network**—Dial peer that defines the characteristics of a packet network connection. Voice-network dial peers map a dialed string to a remote network device, such as the destination router that is connected to the remote telephony device.

In a VoIP network, dial peer points to the IP address of the destination router that terminates the call.

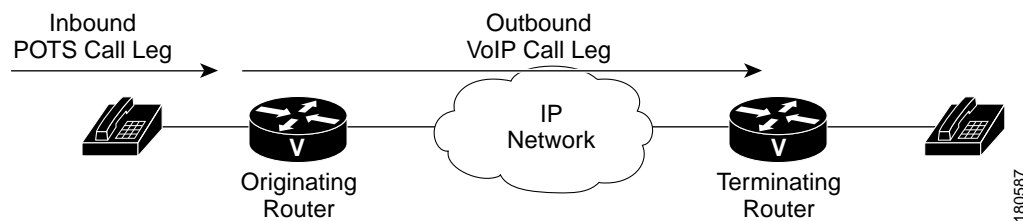
POTS and voice-network dial peers are needed to establish either voice connections over a packet network or a unicast connection trunk.

## Inbound and Outbound Dial Peers

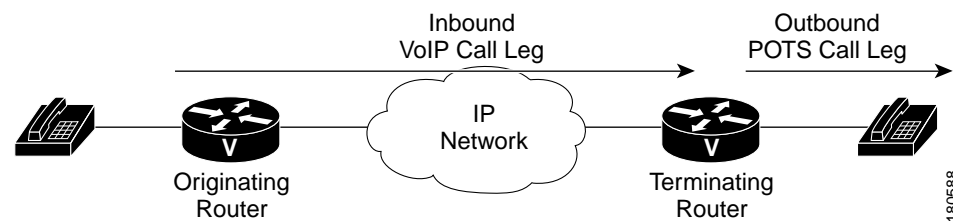
Dial peers are used for inbound and outbound call legs. It is important to understand that these terms are defined from the perspective of the router. An inbound call leg originates when an incoming call comes in to the router. An outbound call leg originates when an outgoing call is placed from the router.

[Figure 5-2](#) illustrates call legs from the perspective of the originating router. [Figure 5-3](#) illustrates call legs from the perspective of the terminating router.

**Figure 5-2** *Originating Router Call Legs*



**Figure 5-3** *Terminating Router Call Legs*



For inbound calls from a POTS interface that are destined for the VoIP network, the router matches a POTS dial peer for the inbound call leg and a VoIP dial peer for the outbound leg. For inbound calls from the packet network, the router matches a POTS dial peer to terminate the call and a VoIP dial peer to apply features such as codec or QoS.

The following examples show basic configurations for POTS and VoIP dial peers:

```
dial-peer voice 1 pots
destination-pattern 555....
port 1/0:1
```

```
dial-peer voice 2 voip
 destination-pattern 555...
 session target ipv4:192.168.1.1
```

The router selects a dial peer for a call leg by matching the string that is defined by using the **answer-address**, **destination-pattern**, or **incoming called-number** command in the dial peer configuration. For Cisco IPICS, the destination-pattern is used in the dial peer configurations.

## Destination Pattern

Cisco IPICS configurations use the destination pattern, which associates a string with a specific device. You configure a destination pattern in a dial peer by using the **destination-pattern** command. If the string matches the destination pattern, the call is routed according to the voice port in POTS dial peers, or the session target in VoIP dial peers. For outbound voice-network dial peers, the destination pattern may also determine the dialed digits that the router collects and then forwards to the remote telephony interface. You must configure a destination pattern for each POTS and voice-network dial peer that you define on the router.

## Session Target

The session target is the network address of the remote router to which you want to send a call once a local voice-network dial peer is matched. It is configured in VoIP dial peers by using the **session target** command. For outbound dial peers, the destination pattern is the telephone number of the remote voice device that you want to reach. The session target represents the path to the remote router that is connected to that voice device.

Establishing voice communication over a packet network is similar to configuring a static route; you are establishing a specific voice connection between two defined endpoints. Call legs define the discrete segments that lie between two points in the call connection. A voice call over the packet network comprises four call legs, two on the originating router and two on the terminating router. A dial peer is associated with each of these four call legs.

## Configuring Dial Peers for Call Legs

When a voice call comes into the router, the router must match dial peers to route the call. For inbound calls from a POTS interface that are being sent over the packet network, the router matches a POTS dial peer for the inbound call leg and a VoIP dial peer for the outbound call leg. For calls coming into the router from the VoIP, the router matches an outbound POTS dial peer to terminate the call and an inbound VoIP dial peer for features such as codec, VAD, and QoS.

## Matching Inbound and Outbound Dial Peers

To match inbound call legs to dial peers, the router uses three information elements in the call setup message and four configurable dial peer attributes. The call setup elements are:

- Called number or dialed number identification service (DNIS)—Set of numbers representing the destination

- Calling number or automatic number identification (ANI)—Set of numbers representing the origin
- Voice port—Voice port carrying the call.

The configurable dial peer attributes are:

- Incoming called-number—String representing the called number or DNIS. It is configured by using the **incoming called-number dial-peer configuration** command in POTS and VoIP dial peers.
- Answer address—String representing the calling number or ANI. It is configured by using the **answer-address dial-peer configuration** command in POTS or VoIP dial peers and is used only for inbound calls from the IP network.
- Destination pattern—String representing the called number or ANI. It is configured by using the **destination-pattern dial-peer configuration** command in POTS or VoIP dial peers.
- Port—Voice port through which calls to this dial peer are placed.

The router selects an inbound dial peer by matching the information elements in the setup message with the dial peer attributes. The router attempts to match these items in the following order:

1. Called number with incoming called-number.
2. Calling number with answer-address.
3. Calling number with destination-pattern.
4. Incoming voice port with configured voice port.

The router must match only one of these conditions to select a dial peer. It is not necessary for all the attributes to be configured in the dial peer or that every attribute match the call setup information. The router stops searching as soon as one dial peer is matched and the call is routed according to the configured dial peer attributes. Even if there are other dial peers that would match, only the first match is used.

The router selects an outbound dial peer based on the dial string. If the dial string matches a configured dial peer, the router places the call by using the configured attributes in the matching dial peer.



## Cisco IPICS Licensing and Sizing Guidelines

---

This chapter provides information about how Cisco IPICS uses licensable features. It also provides information about resource usage and system sizing. Use this information to help plan your Cisco IPICS deployment.

This chapter includes these topics:

- [Resource and License Usage, page 6-1](#)
- [UMS Usage, page 6-1](#)
- [Additional Planning and Sizing Guidelines, page 6-2](#)
- [Dial Port Licensing Details, page 6-2](#)

### Resource and License Usage

To properly design a Cisco IPICS deployment, it is important to understand how resources are licensed and used. The Cisco IPICS license determines the number of concurrent land mobile radio (LMR) ports, multicast ports, IP phone users, dial users, and ops views that are available for your system. The total number of LMR and multicast ports, IP phone, dial users, and ops views cannot exceed the number that is specified in the license or licenses that you purchased. See the “Managing Licenses” section in “Chapter 2 Performing Cisco IPICS System Administrator Tasks” in *Cisco IPICS Server Administration Guide* for this release.

### UMS Usage

A single UMS license is used in the following situations:

- For each channel in an active VTG
- For each instance of an active VTG that is accessed by a dial-in or dial-out user, regardless of the number of users who are connected to the VTG
- For each mobile client

## Additional Planning and Sizing Guidelines

Each channel that is associated with a mobile client user ID consumes one UMS resource when a user logs in with that ID. For example, if a user ID has 10 associated channels, 10 UMS resources are used when a user logs in with this ID. If a mobile client user has several associated channels but does not require all of these channels when logging in from the Remote location, you can conserve system resources by creating an alternate login ID for the user. Configure this alternate login ID with only the resources that the user needs when connecting to Cisco IPICS, and instruct the user to log in with this alternate ID when connecting from a mobile client.

## Dial Port Licensing Details

A Cisco IPICS license for the policy engine includes licenses for the purchased number of Cisco IPICS dial ports. These licenses determine the total number of dial users (incoming and outgoing) who can be connected simultaneously.

Dial port usage can be partitioned per ops view. This way, a Cisco IPICS administrator can limit the number of Cisco IPICS dial port licenses in groups that are segmented by ops views.

Dial ports from the available dial pool are used by the currently executing policy notification or invite actions. If there are fewer dial ports available than what is needed, other policy actions will wait for a dial port to become available.

The recipient of a call must authenticate properly for the call to succeed. Otherwise, the call is considered unsuccessful and the system moves on to the next number that is configured in the dial preferences for the recipient. If you want the system to retry the same number, enter the same number again as a dial preference. The system attempts one call to each number in the dial preferences. It stops attempting calls when the recipient authenticates properly or when the system has tried all numbers.

Dial pool configurations are made in the Administration Console Ops View window. For detailed information, see the “Configuring and Managing Cisco IPICS Operational Views” chapter in *Cisco IPICS Server Administration* Guide for this release.



## Cisco IPICS Deployment Models

---

This chapter describes Cisco IPICS deployment models. You can use these models as guides when you design your Cisco IPICS deployment.

This chapter includes these topics:

- [Single Site Model, page 7-1](#)
- [Multiple Site Model, page 7-2](#)

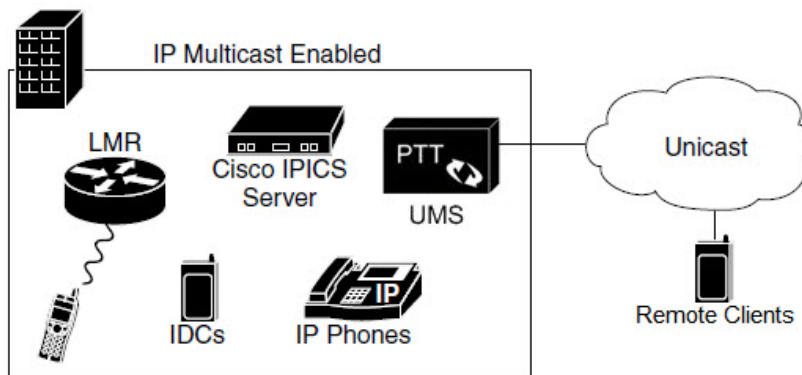
### Single Site Model

The Cisco IPICS single site model represents a deployment in a single multicast domain. Cisco IPICS components are located at one multicast-enabled site or campus, with no Cisco IPICS multicast services provided over an IP WAN. The single site model typically is deployed over a LAN or metropolitan area network (MAN), either of which carries the multicast voice traffic within the site. Calls from beyond the LAN or MAN connect to the Cisco IPICS domain via a SIP-based unicast call.

The single site model has the following design characteristics:

- Cisco IPICS server
- UMS
- Cisco Unified IP Phones
- LMR gateways (optional)
- Multicast-enabled network using PIM Sparse mode.

[Figure 7-1](#) illustrates the Cisco IPICS single site model.

**Figure 7-1 Single Site Model**

## Benefits of the Single Site Model

A single infrastructure for a converged network solution provides significant cost benefits, and it enables Cisco IPICS to take advantage of the IP-based applications in an enterprise. In addition, a single site deployment allows a site to be completely self-contained. There is no dependency on an IP WAN, and a WAN failure or insufficient bandwidth will not cause loss of Cisco IPICS service or functionality.

## Best Practices for the Single Site Model

When you implement a Cisco IPICS single site model, follow these guidelines:

- Provide a highly available, fault-tolerant infrastructure. A sound infrastructure is important for the installation of Cisco IPICS and makes it easier to change to a multiple site deployment, if you choose to do so.
- Use the G.711 codec for all local endpoints. This practice eliminates the consumption of DSP resources for transcoding.
- Implement the recommended network infrastructure for high availability, connectivity options for phones (inline power), QoS mechanisms, multicast, and security. (For more information, see [Chapter 4, “Cisco IPICS Infrastructure Considerations.”](#))

## Multiple Site Model

The Cisco IPICS multiple site model consists of a single Cisco IPICS server that provides services for two or more sites and that uses the IP WAN to transport multicast IP voice traffic between the sites. The IP WAN also carries call control signaling between the central site and the remote sites.

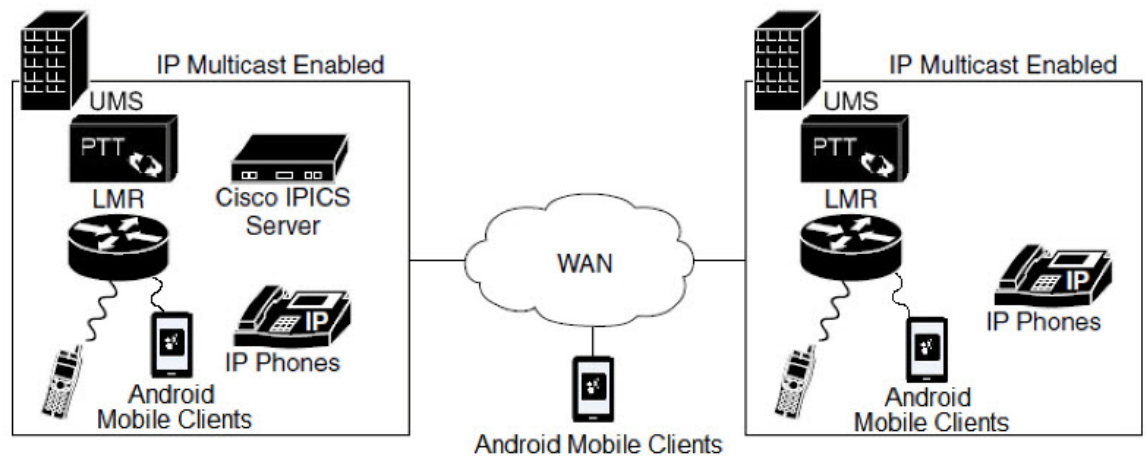
Multicast be enabled between sites, but it is not required. Multiple sites connected by a multicast-enabled WAN are in effect a topologically different case of the single site model, because there is only one multicast domain. The main difference between multiple site model deployments is whether the connecting core network is a service provider network that employs Multiprotocol Label Switching (MPLS). If it is, MPLS with multicast VPNs is deployed to produce a single multicast domain between



sites. Multiple sites with no native multicast support between sites can either employ Multicast over Generic Routing Encapsulation (GRE). IPsec VPNs can also be configured between sites to secure inter-site traffic.

Figure 7-2 illustrates a typical Cisco IPICS multiple site deployment, with a Cisco IPICS server at the central site and an IP WAN to connect all the sites.

Figure 7-2 Multiple Site Model



In the multiple site model, connectivity options for the IP WAN include the following:

- Leased lines
- MPLS Virtual Private Network
- Voice and Video Enabled IP Security Protocol (IPsec) VPN (V3PN)

Routers that reside at the edges of the WAN require Quality of Service (QoS) mechanisms, such as priority queuing and traffic shaping, to protect the voice traffic from the data traffic across the WAN, where bandwidth is typically scarce.

This section includes these topics:

- [MPLS with Multicast VPNs, page 7-3](#)
- [Multicast Islands, page 7-10](#)
- [VPN Termination for Mobile Clients, page 7-15](#)

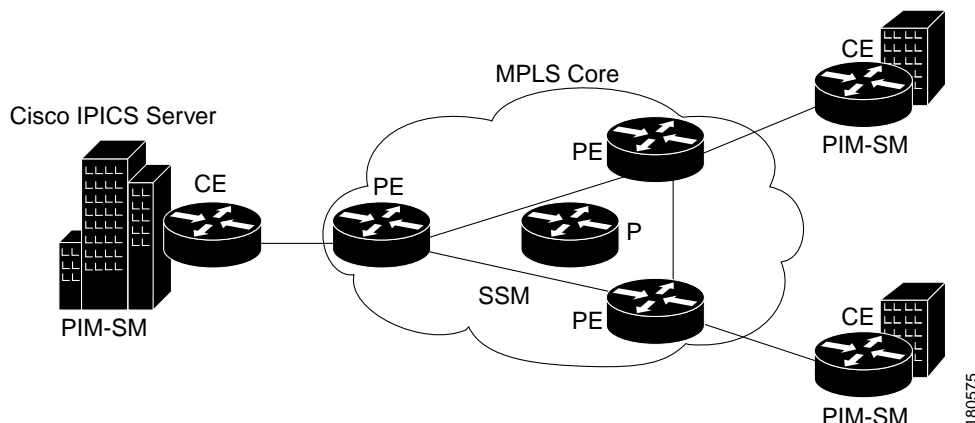
## MPLS with Multicast VPNs

MPLS does not support native multicast in an MPLS VPN. This section discusses a technique for enabling multicast across an MPLS core. This section assumes that the unicast PLS core and the VPN have been configured and are operating properly, and it assumes that you are familiar with IP multicast and MPLS. For additional information about these topics, see the documentation at this URL:

[http://www.cisco.com/en/US/products/ps6552/products\\_ios\\_technology\\_home.html](http://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html)

Figure 7-3 illustrates the topology that is discussed in this section.

Figure 7-3 MPLS with Multicast VPNs



## MPLS Terminology

The following terms apply to MPLS:

- Customer Edge Router (CE)—Router at the edge of a network and that has interfaces to at least one Provider Edge (PE) router.
- Data Multicast Distribution Tree (MDT)—Tree created dynamically by the existence of active sources in the network and that is sent to active receivers located behind separate PE routers. Data MDT connects only to PE routers that are attached to CE routers with active sources or receivers of traffic from active sources or that are directly attached to active sources or receivers of traffic.
- Default-MDT—Tree created by the multicast virtual private network (MVPN) configuration. The Default-MDT is used for customer Control Plane and low rate Data Plane traffic. It uses Routing and Forwarding (MVRFs) to connect all of the PE routers in a particular multicast domain (MD). One Default-MD exists in every MD whether there is any active source in the respective customer network.
- LEAF—Describes the recipient of multicast data. The source is thought of as the root and the destination is the leaf.
- Multicast domain (MD)—Collection of MVRFs that can exchange multicast traffic
- Multicast Virtual Route Forwarding (MVRF)—Used by a PE router to determine how to forward multicast traffic across an MPLS core.
- Provider Router (P)—Router in the core of the provider network that has interfaces only to other P routers and other PE routers
- Provider Edge Router (PE)—Router at the edge of the provider network that has interfaces to other P and PE routers and to at least one CE router
- PIM-SSM—PIM Source Specific Multicast

## MVPN Basic Concepts

The following basic concepts are key to understanding MVPN:

- A service provider has an IP network with its own unique IP multicast domain (P-Network).
- The MVPN customer has an IP network with its own unique IP multicast domain (C-Network).

- The Service Provider MVPN network forwards the customer IP multicast data to remote customer sites. To do so, the service provider encapsulates customer traffic (C-packets) inside P-packets at the service provider PE. The encapsulated P-packet is then forwarded to remote PE sites as native multicast inside the P-Network
- During the process of forwarding encapsulated P-packets, the P-Network has no knowledge of the C-Network traffic. The PE is the device that participates in both networks. (There may be more than one Customer Network per PE.)

## VPN Multicast Routing

A PE router in an MVPN network has several routing tables. There is one global unicast/multicast routing table and a unicast/multicast routing table for each directly connected MVRF.

Multicast domains are based on the principle of encapsulating multicast packets from a VPN in multicast packets to be routed in the core. As multicast is used in the core network, PIM must be configured in the core. PIM-SM, PIM-SSM, and PIM-BIDIR are supported inside the provider core for MVPN. PIM-SM or PIM-SSM is the recommended PIM option in the provider core, because PIM-BIDIR is not supported on all platforms. PIM-SM, PIM-SSM, PIM-BIDIR and PIM-DENSE-MODE are supported inside the MVPN. MVPN leverages Multicast Distribution Trees (MDTs). An MDT is sourced by a PE router and has a multicast destination address. PE routers that have sites for the same MVPN source to a default MDT and join to receive traffic on it.

In addition, a Default-MDT is a tree that is always-on and that transports PIM control-traffic, dense-mode traffic, and rp-tree (\*,G) traffic. All PE routers configured with the same default-MDT receive this traffic.

Data MDTs are trees that are created on demand and that will only be joined by the PE routers that have interested receivers for the traffic. Data MDTs can be created either by a traffic rate threshold or a source-group pair. Default-MDTs must have the same group address for all VPN Routing and Forwarding (VRFs) that make up a MVPN. Data MDTs may have the same group address if PIM-SSM is used. If PIM-SM is used, they must have a different group address, because providing the same one could result in the PE router receiving unwanted traffic.

## Configuring the Provider Network for MVPN

This section provides an example of how to configure a provider network for MVPN.

The steps required to enable a MVPN in the provider network see the topology illustrated in [Figure 7-3 on page 7-4](#). In these steps, the customer VPN is called “ipics.”

### Procedure

---

**Step 1** Choose the PIM mode for the provider network.

Cisco recommends PIM-SSM as the protocol in the core. No additional source-discovery BGP configuration is required with the source-discovery attribute. A route distinguisher (RD) type is used to advertise the source of the MDT with the MDT group address. PIM-SM has been the most widely deployed multicast protocol and has been used for both sparsely and densely populated application requirements. PIM SSM is based upon PIM SM. Without the initial Shared Tree and the subsequent cutover to the Shortest Path Tree, either PIM SSM or PIM SM is suitable for the default MDT.

When bidirectional PIM support becomes available on all relevant hardware, it will be the recommendation for the default MDT. For the Data MDT, either PIM SM or PIM SSM is suitable. PIM SSM is simpler to deploy than PIM SM. It does not require a Rendezvous point, and the Provider network is a known and stable group of multicast devices. Cisco recommends the use of PIM SSM for Provider core deployment. This configuration example uses PIM-SSM in the core.

**Step 2** Choose the VPN group addresses used inside the provider network:

The default PIM-SSM range is 232/8. However, this address range is designed for global use in the Internet. For use within a private domain, you should use an address outside of this administratively scoped multicast range (as recommended in RFC2365). Using a private address range makes it simpler to filter on boundary routers. Cisco recommends using 239.232/16, because addresses in this range are easily recognizable as both private addresses and SSM addresses by using 232 in the second octet. In the design discussed in this document, the range is divided for default-MDT and data MDT. (Data MDT is discussed elsewhere in the [“VPN Multicast Routing” section on page 7-5](#). Default-MDTs uses 239.232.0.0-239.232.0.255 and Data MDTs uses 239.232.1.0-239.232.1.255. This address range provides support for up to 255 MVRFs per PE router.

**Step 3** Configure the provider network for PIM-SSM.

The following commands enable a basic PIM-SSM service.

- On all P and PE routers, configure these commands globally:

```
ip multicast-routing
ip pim ssm range multicast_ssm_range
ip access-list standard multicast_ssm_range
permit 239.232.0.0 0.0.1.255
```

- On all P interfaces and PE interfaces that face the core, configure this command:

```
ip pim sparse-mode
```

- On each PE router, configure this command on the loopback interface that is used to source the BGP session:

```
ip pim sparse-mode
```

**Step 4** Configure the MDT on the VRF.

- To configure multicast routing on the VRF, configure these commands on all PE routers for the VRF ipics:

```
ip vrf ipics
mdt default 239.232.0.0
```

- To enable multicast routing for the VRF, configure this command:

```
ip multicast-routing vrf ipics
```

**Step 5** Configure the PIM mode inside the VPN.

The PIM mode inside the VPN depends on what type of PIM the VPN customer is using. Cisco provides automatic discovery of the group-mode used inside the VPN via auto-rp or bootstrap router (BSR), which requires no additional configuration. Optionally, a provider may choose to provide the RP for the customer by configuring the PE router as an RP inside the VPN. In the topology discussed in this section, the VPN customer provides the RP service and the PE routers will automatically learn the group-to-rendezvous point (RP) via auto-rp.

Configure all PE-CE interfaces for sparse-dense-mode, which ensures that either auto-rp or BSR messages are received and forwarded, and which allows the PE to learn the group-to-rendezvous point (RP) inside the VPN. To do so, configure the following on all customer facing interfaces:

```
ip pim sparse-mode
```

## Verifying the Provider Network for MVPN

After you complete the configuration as described in the [“Configuring the Provider Network for MVPN” section on page 7-5](#), use the following procedure to verify that the configuration is correct:

### Procedure

#### Step 1 Verify BGP updates.

BGP provides for source discovery when SSM is used, which is known as a BGP-MDT update. To verify that all BGP-MDT updates have been received correctly on the PE routers, take either of these actions:

- Use the **show ip pim mdt bgp** command:

```
PE1#show ip pim mdt bgp
Peer (Route Distinguisher + IPv4)           Next Hop
MDT group 239.232.0.0
  2:65019:1:10.32.73.248                     10.32.73.248 (PE-2 Loopback)
  2:65019:1:10.32.73.250                     10.32.73.250 (PE-3 Loopback)
```

2:65019:1 indicates the RD-type (2) and RD (65019:1) that is associated with this update.

The remaining output is the address that is used to source the BGP session.

- Use the **show ip bgp vpnv4 all** command:

```
PE1#show ip bgp vpnv4 all
BGP table version is 204, local router ID is 10.32.73.247
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
               r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop        Metric LocPrf Weight Path
Route Distinguisher: 65019:1 (default for vrf ipics)
*>i10.32.72.48/28    10.32.73.248             0    100        0 ?
... (output omitted)
Route Distinguisher: 2:65019:1
*> 10.32.73.247/32   0.0.0.0                  0    100        0 ?
*>i10.32.73.248/32   10.32.73.248             0    100        0 ?
*>i10.32.73.250/32   10.32.73.250             0    100        0 ?
```

#### Step 2 Verify the global mroute table

Use the **show ip mroute mdt-group-address** command to verify that there is a (Source, Group) entry for each PE router. Because PIM-SSM is used, the source is the loopback address used to source the BGP session and the Group is the MDT address configured. Without traffic, only default-MDT entries are visible.

```
PE1#show ip mroute 239.232.0.0
IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
```

```

    U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel
    Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags: H - Hardware switched
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(10.32.73.247, 239.232.0.0), 1w0d/00:03:26, flags: sTZ
  Incoming interface: Loopback0, RPF nbr 0.0.0.0
  Outgoing interface list:
    FastEthernet0/0, Forward/Sparse, 1w0d/00:02:47

(10.32.73.248, 239.232.0.0), 1w0d/00:02:56, flags: sTIZ
  Incoming interface: FastEthernet0/0, RPF nbr 10.32.73.2
  Outgoing interface list:
    MVRF ipics, Forward/Sparse, 1w0d/00:01:30

(10.32.73.250, 239.232.0.0), 1w0d/00:02:55, flags: sTIZ
  Incoming interface: FastEthernet0/0, RPF nbr 10.32.73.2
  Outgoing interface list:
    MVRF ipics, Forward/Sparse, 1w0d/00:01:29

```

Verify that the s flag is set on each (S,G) entry, which indicates that this group is used in ssm mode. Verify that the z flag is set, which indicates that this PE router is a leaf of the multicast tunnel. When the router is a leaf of a multicast tunnel, it has to do additional lookups to determine which MVRF to forward this traffic to, as it is basically a receiver for this traffic. Verify the T flag is set for the remote PE(S,G) entry. This flag indicates that the router understands it is joining an SSM group. It is as though an IGMPv3 host had requested to join that particular channel.

### Step 3 Verify PIM neighbors in the global table.

Use the **show ip pim neighbors** command on all PE and P routers to verify that the pim neighbors are setup properly in the global table.

```

PE1#show ip pim neighbor
PIM Neighbor Table
Neighbor      Interface      Uptime/Expires   Ver   DR
Address
10.32.73.2    FastEthernet0/0  1w4d/00:01:21    v2    1 / DR
10.32.73.70   Serial0/2        1w4d/00:01:29    v2    1 / S

```

### Step 4 Verify PIM neighbors inside the VPN

Use the **show ip pim vrf ipics neighbors** command on all PE routers to verify that the CE router is seen as a PIM neighbor and that the remote-PE routers are seen as pim neighbors over the tunnel.

```

PE1#show ip pim vrf ipics neighbor
PIM Neighbor Table
Neighbor      Interface      Uptime/Expires   Ver   DR
Address
10.32.73.66   Serial0/0       1w3d/00:01:18    v2    1 / S
10.32.73.248  Tunnel0         3d17h/00:01:43    v2    1 / S
10.32.73.250  Tunnel0         1w0d/00:01:42    v2    1 / DR S

```

### Step 5 Verify the VPN group-to-rendezvous point (RP).

The main customer site has been configured to use auto-rp within the VPN. VPN IPICS is using the multicast range 239.192.21.64 - 79 for channels and VTGs.

```

ip pim send-rp-announce Loopback0 scope 16 group-multicast_range
ip pim send-rp-discovery scope 16
ip access-list standard multicast_range
permit 239.192.21.64 0.0.0.15

```

Use the **show ip pim vrf ipics rp mapping** command to verify that the PE router correctly learned the RP mapping information from the VPN.

```
PE1#show ip pim vrf ipics rp map
PIM Group-to-RP Mappings

Group(s) 239.192.21.64/28
  RP 10.32.72.248 (?), v2v1
    Info source: 10.32.73.62 (?), elected via Auto-RP
    Uptime: 1w3d, expires: 00:02:54
```

This output shows that the PE router has correctly learned the group-to-rendezvous point (RP), which is used inside the VPN. The default-MDT reaches all PE routers in the core of the provide network in which the multicast replication is performed. With only a default-MDT configured, traffic goes to all PE routers, regardless of whether they want to receive the traffic.

## Optimizing Traffic Forwarding: Data MDT

Data MDT is designed to optimize traffic forwarding. Data MDT is a multicast tree that is constructed on demand. The conditions to create a data MDT are based upon traffic-load threshold measured in kbps or on an access-list that specifies certain sources inside the VPN. A data MDT is created only by the PE that has the source connected to its site. The data MDT conditions do not have to be configured. However, when there are no conditions set for each (S,G) inside the VPN, a data MDT is created. This data MDT requires resources from the router, so it is recommended that you not create one just because a source exists. A non-zero threshold is recommended, because this value requires an active source to trigger the creation of the Data MDT. The maximum number of multi-VPN Routing/Forwarding (MVRF) entries is 256.

To configure the data MDT under the VRF, use one of the ranges that is described in [Step 2](#) in the “Configuring the Provider Network for MVPN” section on [page 7-5](#). A maximum of 256 addresses is allowed per VRF. This limitation is an implementation choice, not a protocol limitation. Because SSM is used, the data MDT address-range may be the same on all PE routers for the same VPN. Use an inverse-mask to specify the number of addresses used for the data MDT, as shown in the following command:

```
ip vrf ipics
mdt data 239.232.1.0 0.0.0.255 threshold 1
```

## Verifying Correct Data MDT Operation

Data MDTs create mroute entries in the global table. There also are specific commands for verifying functionality of the sending and receiving PE router. To verify the data MDT operation, there must be multicast traffic between sites that exceeds the configured threshold. An easy way to test the data MDT is to statically join a multicast group in one site and then ping that group from another site, as shown in the following example:

```
CE1
interface Loopback0
 ip address 10.32.72.248 255.255.255.255
 ip pim sparse-mode
 ip igmp join-group 239.192.21.68

CE2
ping 239.192.21.68 size 500 repeat 100
```

To verify the data MDT operation, perform the following procedure:

**Step 1** Verify the sending PE router.

Use the **show ip pim vrf ipics mdt send** command on the sending PE router (PE2) to verify the setup of a data mdt.

```
PE2#show ip pim vrf ipics mdt send
MDT-data send list for VRF: ipics
  (source, group)                MDT-data group    ref_count
  (10.32.72.244, 239.192.21.68)  239.232.1.0       1
  (10.32.73.74, 239.192.21.68)  239.232.1.1       1
```

**Step 2** Verify the receiving PE router.

Use the **show ip pim vrf ipics mdt receive detail** command on the receiving PE (PE1) router to verify that this router is receiving on a data mdt.

```
PE1#show ip pim vrf ipics mdt receive

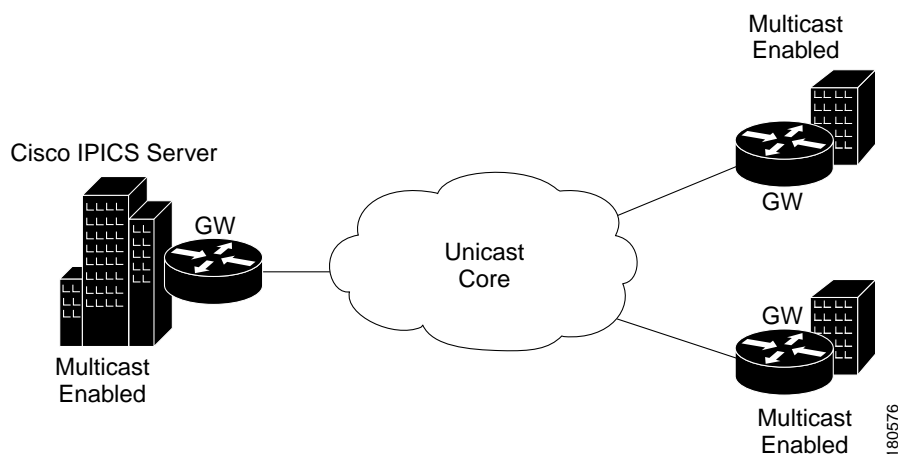
Joined MDT-data [group : source] for VRF: ipics
[239.232.1.0 : 10.32.73.248] ref_count: 1
[239.232.1.1 : 10.32.73.248] ref_count: 1
```

At this point, if everything is correctly configured, the sites in VPN IPICS can transfer multicast traffic by using the MPVN and all sites are now in the same multicast domain. Therefore, all channels and users on the Cisco IPICS server can be configured with the same location.

## Multicast Islands

A multicast island is a site in which multicast is enabled. A multi-site deployment can consist of several multicast islands that connect to each other over unicast-only connections. See [Figure 7-4](#).

**Figure 7-4** Multicast Islands

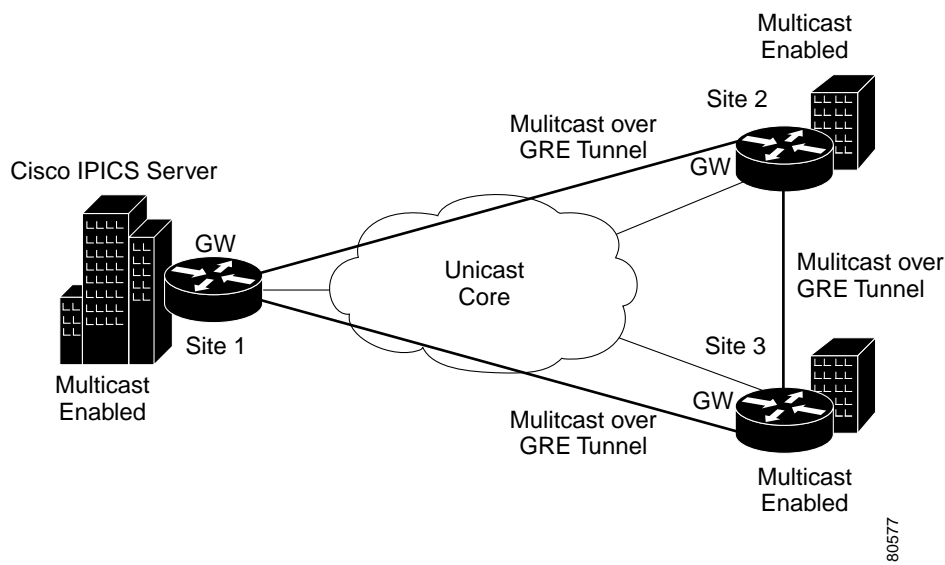




## Multicast over GRE

Multicast over GRE provides multicast support between islands. This section provides an overview of how to configure multicast over GRE. Figure 7-5 illustrates a Cisco IPICS deployment with multicast over GRE.

Figure 7-5 Multicast over a GRE Tunnel



A tunnel is configured between the gateway in Site 1 and the gateway in Site 2, which is sourced with their respective loopback0 interfaces. The **ip pim sparse-dense mode** command is configured on tunnel interfaces and multicast routing is enabled on the gateway routers. Sparse-dense mode configuration on the tunnel interfaces allows sparse-mode or dense-mode packets to be forwarded over the tunnel depending on the RP configuration for the group.

The following examples show the configuration that is required to implement multicast over GRE between Site 1 and Site 2. Use the same approach between Site 1 and Site 3, and between Sites 2 and Site 3.

```
interface loopback 0
 ip address 1.1.1.1 255.255.255.255

interface Tunnel0
 ip address 192.168.3.1 255.255.255.252
 ip pim sparse-mode
 tunnel source Loopback0
 tunnel destination 2.2.2.2
```

### Site 2

```
ip multicast-routing

interface loopback 0
 ip address 2.2.2.2 255.255.255.255

interface Tunnel0
 ip address 192.168.3.2 255.255.255.252
 ip pim sparse-mode
 tunnel source Loopback0
```

```
tunnel destination 1.1.1.1
```

When you configure PIM sparse mode over a tunnel, make sure to follow these guidelines:

- For successful RPF verification of multicast traffic flowing over the shared tree (\*,G) from the RP, configure the **ip mroute rp-address nexthop** command for the RP address, pointing to the tunnel interface.

For example, assume that Site 1 has the RP (RP address 10.1.1.254). In this case, the mroute on the gateway in Site 2 would be the **ip mroute 10.1.1.254 255.255.255.255 tunnel 0** command, which ensures a successful RPF check for traffic flowing over the shared tree.

- For successful RPF verification of multicast (S,G) traffic flowing over the Shortest Path Tree (SPT), configure the **ip mroute source-address nexthop** command for the multicast sources, pointing to the tunnel interface on each gateway router.

In this case, when SPT traffic flows over the tunnel interface, an **ip mroute 10.1.1.0 255.255.255.0 tunnel 0** command is configured on the Site 2 gateway and **ip mroute 10.1.2.0 255.255.255.0 tunnel 0** command is configured on the Site 1 gateway. This configuration ensures successful RPF verification for incoming multicast packets over the Tu0 interface.

## Bandwidth Considerations when using Multicast over GRE

Cisco IPICS can operate with either the G.711 or the G.729 codec. [Table 7-1](#) lists the bandwidth requirements for a voice call over unicast connection trunks, based on the codec used, the payload size, and whether cRTP, VAD, or both are configured.

**Table 7-1** Bandwidth Considerations for Unicast Connection Trunks

Compression Technique	Payload Size (Bytes)	Full Rate Bandwidth (kbps)	Bandwidth with cRTP (kbps)	Bandwidth with VAD (kbps)	Bandwidth with cRTP and VAD (kbps)
G.711	240	76	66	50	43
G.711	160	83	68	54	44
G.729	40	17.2	9.6	11.2	6.3
G.729	29	26.4	11.2	17.2	7.3

Bandwidth consumption across a tunnel depends on the number of active channels and VTG users that are communicating between the sites.

The following cases are examples how to calculate bandwidth use across a tunnel.

### Case 1: Active channel in Site 1 and Site 2.

All users in Site 1 are using one channel, and all users in Site 2 are using another channel. No multicast voice flows across the tunnel.

### Case 2: Active channel has n users in site 1 and m users in site 2.

In the following example, Call bandwidth is the bandwidth value from [Table 4-2 on page 4-6](#).

Bandwidth 1 = Call bandwidth \* n (Flow from site 1 to site 2)

Bandwidth 2 = Call bandwidth \* m (Flow from site 2 to site 1)

Total bandwidth = Bandwidth 1 + Bandwidth 2

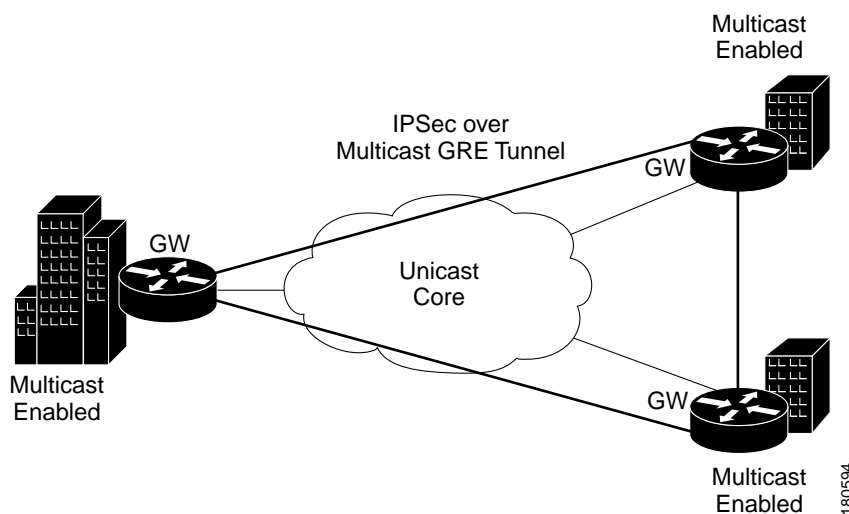
(Call bandwidth is the value from Table 3-1.)

Depending on the number of active channels, the number of active users per channel, and whether the channel spans multiple sites, the bandwidth usage could be significant.

## IPSec VPNs

IPSec VPNs can be implemented over multicast GRE tunnels. See [Figure 7-6](#).

**Figure 7-6** *IPSec over Multicast GRE Tunnels*

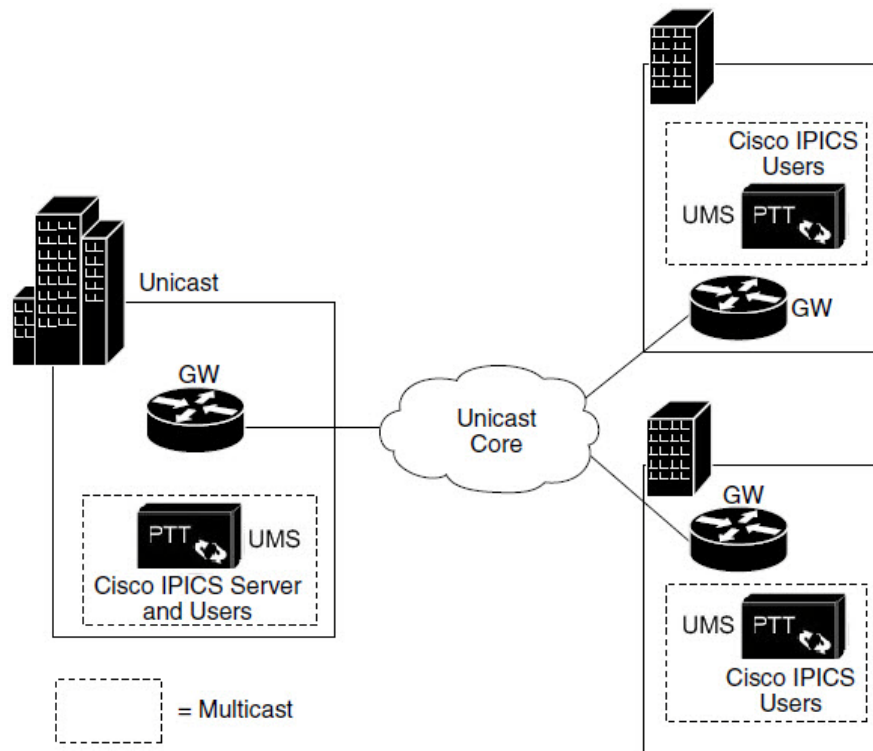


There are a number of ways to configure IPSec over GRE tunnels. See the appropriate Cisco documentation.

## Multicast Singularities

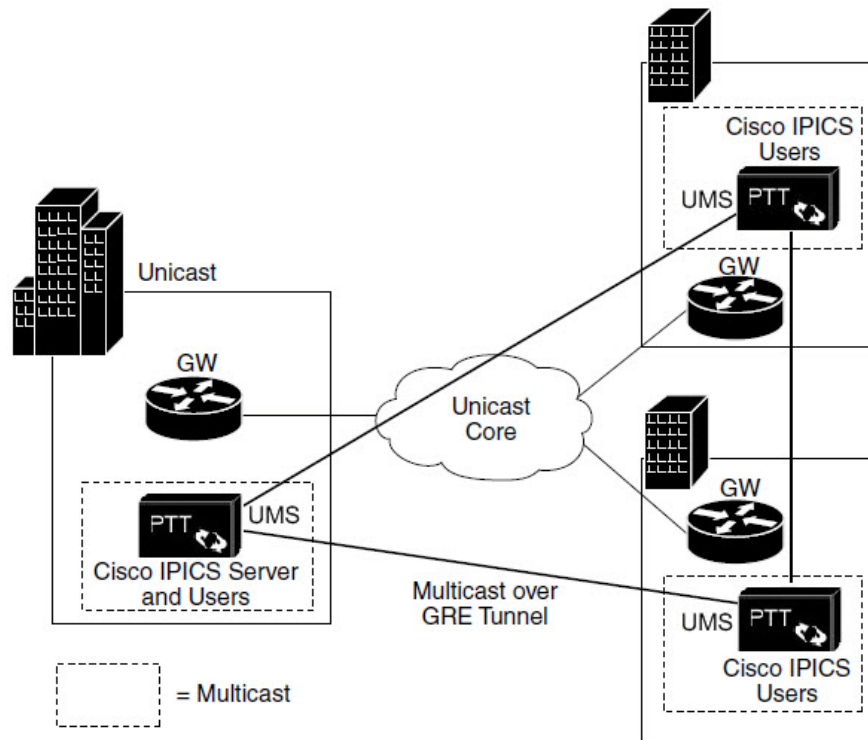
A multicast singularity is a restrictive case of the multicast island scenario. Between sites, multicast routing is not enabled. Within a site, multicast is enabled only on Cisco IPICS specific devices: UMS, LMR gateways, and Cisco Unified IP Phones. These Cisco IPICS devices reside in a multicast singularity, as shown in [Figure 7-7](#).

Figure 7-7 Multicast Singularities



The singularities can be connected by using multicast over GRE tunnels (as shown in [Figure 7-8](#)).

Figure 7-8 Multicast Singularities with GRE Tunnels



The configuration of a multicast over GRE tunnel is identical to the multicast island scenario except the tunnel must be configured between the routers and not the gateway routers because the gateway routers are not enabled for multicast.

The following rules apply to a multicast singularity:

1. All UMSs and LMR gateways must reside in a multicast singularity. That is, these devices must be on directly connected multicast enabled LANs.
2. All users within the multicast singularity can use a Cisco Unified IP Phone because they are in the multicast enabled zone.
3. Users outside the multicast singularity can use the mobile client.
4. Users outside the multicast singularity cannot use the Cisco Unified IP Phone because this device supports only multicast.

It would be possible to have multiple multicast singularities within the same site and the singularities could be connected with multicast over GRE tunnels. This solution depends on the policies of the organization.

## VPN Termination for Mobile Clients

Cisco IPICS Mobile Clients expand the types of devices that can access the network and provide access to the network from virtually anywhere on the Internet.

For information about the ports and transport protocols that Cisco IPICS mobile clients, use see [Table 2-4 on page 2-39](#).

In a secure campus network, mobile clients work over WiFi. As the network expands and access shifts to 3G/4G and LTE, an additional level of protection is required. Cisco offers that protection by using the Cisco AnyConnect Mobile VPN Client and Cisco Adaptive Security Appliance (ASA) platforms to create a VPN tunnel between the endpoints and Cisco IPICS.

The VPN tunnel encapsulates and encrypts the traffic and provides the added advantage of overcoming issues with NAT traversal through the carrier network. A Cisco IPICS session that runs over a VPN tunnel is viewed by the service provider as a data call, not a voice call, because the tunneled payload is a data service running on the mobile client.



---

## A

<b>action</b>	A discrete function that is performed through a policy. Discrete functions include activate VTG, notification, VTG add participant, dial-out, and invite to VTG.
<b>activate VTG</b>	An action that activates a preconfigured VTG; can also specify a duration. At the end of the specified duration, the VTG is deactivated. If no duration is specified, the VTG must be manually deactivated by the dispatcher from the VTG Management drawer in the Cisco IPICS administration console.
<b>activated</b>	A state that indicates that the SIP (unicast) or multicast channel is fully operational.
<b>active virtual talk group</b>	A virtual talk group (VTG) becomes active when Cisco IPICS commits global resources, such as a multicast address and any necessary dial-in peers, so that the participants in the VTG can communicate with each other.
<b>Administration Console</b>	The graphical user interface (GUI) in the Cisco IPICS server software through which authorized Cisco IPICS users can manage and configure Cisco IPICS resources, events and VTGs.
<b>autonomous system</b>	A radio system under one administrative control; also known as a management domain. This system is usually mapped to an agency.

---

## B

<b>backward compatibility</b>	The ability of newer radio equipment to operate within an older system infrastructure or to directly intercommunicate with an older radio unit. The term usually applies to digital radios that are also capable of analog signal transmission.
<b>bandwidth</b>	The difference between the highest and lowest frequencies that are available for network signals. The term also describes the rated throughput capacity of a specific network medium or protocol. Bandwidth specifies the frequency range that is 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.
<b>base station</b>	A land station in the land mobile radio service. In the personal communication service, the common name for all the radio equipment that is located at one fixed location and used for serving one or several calls.

---

C

<b>call</b>	Radio terminology that defines a call as beginning at the moment that you press the transmit key and concluding when you release the transmit key. The term “per call” implies that some form of control causes the radio to select a specific frequency before it transmits audio. Some radios may be configured to automatically return to a predefined RF channel when the call ends.
<b>call delay</b>	The delay that occurs when there is no idle channel or facility available to immediately process a call that arrives at an automatic switching device.
<b>call setup time</b>	The time that is required to establish a circuit-switched call between users or terminals.
<b>carrier</b>	A wave that is suitable for modulation by an information-bearing signal.
<b>CAS</b>	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.
<b>channel</b>	A communication path that is wide enough to permit a single RF transmission. Multiple channels can be multiplexed over a single cable in certain environments. There are many different types of channels in Cisco IPICS, including direct dial, 2-way, VTGs, and radio channels. Channels can be dynamically or statically allocated. Channels may have one or more channel connections that define the source for the channel. <i>See</i> PTT channel.
<b>channel capacity</b>	The maximum possible information transfer rate through a channel, subject to specified constraints.
<b>channel connection</b>	One or more methods by which a content stream can be obtained. For instance, a particular channel may be found on several different multicast addresses in different locations and also on several different radios at different locations.
<b>channel group</b>	A logical grouping of channels
<b>channel spacing</b>	The distance from the center of one channel to the center of the next-adjacent-channel. Typically measured in kilohertz.
<b>Cisco Unified Communications Manager (CallManager)</b>	The software-based call-processing component of the Cisco IP telephony solution. Cisco Unified Communications Manager (CallManager) extends enterprise telephony features and functions to packet telephony network devices, such as Cisco Unified IP Phones, media processing devices, VoIP gateways, and multimedia applications.
<b>Cisco IPICS</b>	Cisco IP Interoperability and Collaboration System. The Cisco IPICS system provides an IP standards-based solution for voice interoperability by interconnecting voice channels, talk groups, and VTGs to bridge communications amongst disparate systems.
<b>Cisco IPICS policy engine</b>	Integrated with the Cisco IPICS server, this component enables telephony dial functionality and is responsible for the management and execution of policies and user notifications.
<b>Cisco IPICS server</b>	Provides the core functionality of the Cisco IPICS system. The Cisco IPICS server software runs on the Linux operating system on selected performs. The server software includes an incident management framework administration GUI that enables dynamic resource management for users, channels, and VTGs. The server also includes the Cisco IPICS policy engine, which enables telephony dial functionality and is responsible for the management and execution of policies and user notifications.



<b>Cisco Unified IP Phone</b>	A full-featured telephone that provides voice communication over an IP network. A user can participate in a PTT channel or VTG by using a Cisco Unified IP Phone as a PTT device.
<b>CLI</b>	command-line interface. An interface that allows the user to interact with the operating system by entering commands and optional arguments.
<b>codec</b>	<p>coder-decoder.</p> <ol style="list-style-type: none"> <li>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.</li> <li>2. In Voice over IP, Voice over Frame Relay, and Voice over ATM, a DSP software algorithm that is used to compress/decompress speech or audio signals.</li> </ol>
<b>conference of conferences</b>	A conference that consists of two or more VTGs.
<b>conventional radio system</b>	A non-trunked system that is similar to telephone party-line in that the user determines availability by listening for an open channel.
<b>COR</b>	carrier operated relay. An electrical signal that is used to signal when a radio is receiving traffic.
<b>coverage</b>	In radio communications, the geographical area that is within the range of, or that is covered by, a wireless radio system to enable service for radio communications. Also referred to as service delivery area.
<hr/>	
<b>D</b>	
<b>delay time</b>	The sum of waiting time and service time in a queue.
<b>decrypt</b>	Cryptographically restore ciphertext to the plaintext form it had before encryption.
<b>decryption</b>	Reverse application of an encryption algorithm to encrypted data, thereby restoring that data to its original, unencrypted state.
<b>dial engine scripts</b>	Scripts that the Cisco IPICS dial engine executes to provide the telephony user interface (TUI) for interaction with incoming and outgoing phone calls.
<b>dial-in</b>	A phone call that is dialed in to the policy engine.
<b>dial-in floor control</b>	A feature that allows one dial-in user, at a time, to talk in a VTG or a channel. The telephony user interface provides this dial-in floor control feature to support dial-in users. It does not provide support for floor control for other PTT users.
<b>dial number</b>	The phone number that is used by the policy engine and the SIP provider and configured in the Dial Information pane in the Ops Views window. Dialing this number provides user access to the telephony user interface.
<b>dial out invite</b>	<p>An action that invites selected user(s) to the selected VTG.</p> <p>A phone call that is dialed out by the policy engine to a phone user to invite the user in to a talk group.</p>
<b>dial peer</b>	Addressable call endpoint. In Voice over IP, there are two kinds of dial peers: POTS and VoIP.

<b>digit ID</b>	A numeric identifier that is chosen by a Cisco IPICS user and stored in the user profile. Cisco IPICS uses this ID and a numeric password to authenticate a Cisco Unified IP Phone user.
<b>digital modulation technique</b>	A technique for placing a digital data sequence on a carrier signal for subsequent transmission through a channel.
<b>discrete tone</b>	Any tone that is sent without any summed or added tone. For example, adding a function tone with a low level guard tone may impact the recognition of the function tone. Contrast with mixed tones.
<b>dispatcher</b>	The Cisco IPICS dispatcher is responsible for setting up the VTGs, activating the VTGs to begin conferences, and adding and/or removing participants in inactive VTG and active VTGs. The dispatcher also monitors the active VTGs and events, can mute and unmute IDC users, as necessary, and manages policies, which activate/deactivate VTGs based on specific criteria and designated intervals. Policy management activities include create/modify/delete policies, view policies, execute policies, and activate privileges.
<b>DS0</b>	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.
<b>DTMF</b>	dual tone multi-frequency. The signal to the phone company that you generate when you press keys on a telephone keypad. With DTMF, each key that you press on your phone (0 through 9, ‘*’ and ‘#’) generates two tones of specific frequencies; one tone is generated from a high frequency group of tones and the other from a low frequency group. Voice gateways often strip these inband tones and present them out-of-band in SIP, H.323, or other messages.
<b>dynamic radio channel (dynamic control)</b>	The controls that are used to preset radio characteristics so that channels are available to clients.
<b>dynamic regrouping</b>	A trunking system feature that allows multiple radios to be placed upon a specific talk group without manual manipulation of the programming of the radios. Dynamic regrouping is initiated through a system control console and transmitted to the radio via the trunking systems control channel.

---

## E

<b>E &amp; M</b>	<p>recEive and transMit (or ear and mouth). As the analog interface between a radio and the LMR gateway, the E&amp;M interface provides voice signals from radio channels, which are then mapped to IP multicast or unicast. The E&amp;M interface provides the most common form of analog trunking.</p> <ol style="list-style-type: none"> <li>1. Trunking arrangement that is generally used for two-way switch-to-switch or switch-to-network connections. Cisco's analog E&amp;M interface is an RJ-48 connector that allows connections to PBX trunk lines (tie lines). E&amp;M also is available on E1 and T1 digital interfaces.</li> <li>2. A type of signaling that is traditionally used in the telecommunications industry. Indicates the use of a handset that corresponds to the ear (receiving) and mouth (transmitting) component of a telephone.</li> </ol>
<b>e-lead</b>	The ear portion of the E & M interface. The e-lead is the receive path of the LMR gateway.
<b>encipher</b>	To convert plain text into an unintelligible form by using a cipher.
<b>encode</b>	To modify information into the required transmission format.

<b>encryption</b>	Application of a specific algorithm so as to alter the appearance of data and make it incomprehensible to unauthorized users.
<b>event</b>	An active VTG in the Cisco IPICS solution.
<hr/>	
<b>F</b>	
<b>FDM</b>	frequency-division multiplexing. Technique whereby information from multiple channels can be allocated bandwidth on a single wire based on frequency.
<b>FDMA</b>	frequency-division multiple access. A channel access method in which different conversations are separated onto different frequencies. FDMA is employed in narrowest bandwidth and multiple-licensed channel operations.
<b>FLEXlm</b>	Cisco software that enforces licensing on certain systems; FLEXlm ensures that Cisco IPICS software will work only on the supported and licensed hardware.
<b>floor control</b>	The standard mechanism for Push-to-Talk speaker arbitration.
<b>frame</b>	A 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 describe logical information groupings at various layers of the OSI reference model.
<b>frequency</b>	For a periodic function, frequency represents the number of cycles or events per unit of time. Frequency is used in several different contexts. For example, transmission frequency (the band on which the radio sends signals) or the frequency of an audible signal measured in hertz (Hz). All tone control operations require audible tones that fall within a narrow band of a specific frequency and at a specific volume (amplitude).
<b>frequency assignment</b>	Assignment that is given to a radio station to use a radio frequency or radio frequency channel under specified conditions.
<b>frequency hopping</b>	The repeated switching of frequencies during radio transmission according to a specified algorithm, intended to minimize unauthorized interception or jamming of telecommunications.
<b>frequency modulation</b>	Modulation technique in which signals of different frequencies represent different data values.
<b>frequency sharing</b>	The assignment to or use of the same radio frequency by two or more stations that are separated geographically or that use the frequency at different times.
<b>function tone</b>	A tone that follows the high level guard tone and causes the radio to perform a specific function, such as selecting a new transmit frequency. Function tones are often referred to as F1, F2, F3, and so on. <i>See</i> preamble and high level guard tone.

---

**G**

<b>gateway</b>	Device that performs an application-layer conversion of information from one protocol stack to another. In Cisco IPICS, the gateway component includes LMR gateways, which functionality is usually installed as an additional feature in a supported Cisco router. LMR gateways provide voice interoperability between radio and non-radio networks by bridging radio frequencies to IP multicast streams.
<b>GRE</b>	generic routing encapsulation. Tunneling protocol that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling that uses GRE allows network expansion across a single-protocol backbone environment. GRE is generally used to route multicast traffic between routers.
<b>guard tone</b>	The most common guard tones are the high level guard tone (HLGT) and the low level guard tone (LLGT). The HLGT is used to alert the radio that a function tone follows. The LLGT is used as a hold tone or keying tone. <i>See</i> tone keyed.

---

**H**

<b>H.323</b>	Defines a common set of codecs, call setup and negotiating procedures, and basic data transport methods to allow dissimilar communication devices to communicate with each other by using a standardized communication protocol.
<b>high-band frequency</b>	Refers to the higher frequency levels in the VHF band, typically 138-222 MHz.
<b>HLGT</b>	high level guard done. Also known as awake tone. This tone is set at high volume and is usually the first tone in a preamble. It is used to alert the radio that another tone, usually a function tone, will follow. <i>See</i> guard tone.
<b>Hoot 'n' Holler (Hootie)</b>	A communications system where the loudest and most recent talker or talkers are mixed into one multicast output stream. Also known as hootie, these networks provide “always on” multiuser conferences without requiring that users dial in to a conference.  Cisco enables the Cisco Hoot 'n' Holler feature in specific Cisco IOS versions.

---

**I**

<b>idle tone</b>	The tone that a radio may deliver on the m-lead to signal the LMR gateway that there is no incoming traffic. When the idle tone is removed, the LMR gateway deems all signals to be valid voice traffic.
<b>inband</b>	Traffic that is sent inband is included in the same stream as the real-time traffic protocol (RTP). Inband signals can be encoded signals and RFC 2833 signals.
<b>incident</b>	An event that you create in the IDC and for which various users can coordinate responses by using the IDC.
<b>incident VTG</b>	A temporary talk group for an incident.

<b>informix linux group</b>	Members of this group have full permission to Cisco IPICS server folders, files, and scripts that are related to the Informix database application. Members of this group include the informix and ipicsdba users.
<b>informix user ID</b>	<p>The Cisco IPICS Linux user that belongs to both the informix linux group, which includes full permission to the Cisco IPICS database server folders, files, and scripts, and the ipics linux group, which includes permission to Cisco IPICS application-related folders, files, and scripts. In addition, this user has full administrative permission to the Informix database instance. Cisco IPICS creates this Linux system user ID and generates the password during the software installation process. The password for this user ID never expires.</p> <p>To access the informix user, log in to the Cisco IPICS server by using the root user ID; then, enter <b>su - informix</b> (superuser from root).</p>
<b>interference</b>	The effect of unwanted energy due to one or a combination of emissions, radiation, or inductions upon reception in a radio communication system, manifested by any performance degradation, misinterpretation, or loss of information, which could be extracted in the absence of such unwanted energy.
<b>interoperability</b>	The capability of equipment manufactured by different vendors to communicate with each other successfully over a network.
<b>invitation policy</b>	A policy that can be invoked only through the telephony user interface and can include only the invite to VTG action. After joining a talk group, a user can access the breakout menu and invoke invitation policies. The talk group that this user has joined is the talk group that the invited users join.
<b>invite to VTG</b>	A version of the dial out invite action where users to be invited are preconfigured but the VTG that they are invited to depends on which VTG the invoker of the policy is dialed into.
<b>ipicsadmin user ID</b>	The Cisco IPICS Linux user that, as part of the ipics linux group, has full permission to the Cisco IPICS server folders, files, and scripts that are related to the Cisco IPICS application and database backup and restore operations. In addition, the ipicsadmin user has permission to read and write data from and/or to the Informix database. Cisco IPICS creates this Linux system user ID during the software installation process. The password for this user ID never expires.
<b>ipicsdba user ID</b>	<p>The Cisco IPICS Linux user that belongs to both the informix linux group, which includes full permission to the Cisco IPICS database server folders, files, and scripts, and the ipics linux group, which includes permission to Cisco IPICS application-related folders, files, and scripts. In addition, the ipicsdba user has permission to read data, write data, create tables, and create databases in the Informix database instance. Cisco IPICS creates this Linux system user ID and generates the password during the software installation process. The password for this user ID never expires.</p> <p>To access the ipicsdba user, log in to the Cisco IPICS server by using the root user ID; then, enter <b>su - ipicsdba</b> (superuser from root).</p>
<b>ipics linux group</b>	Members of this group have full permission to Cisco IPICS server folders, files, and scripts that are related to the Cisco IPICS application and database backup and restore operations. Members of this group include the ipicsadmin, ipicsdba, and informix users.

<b>ipics user ID</b>	The Cisco IPICS application-level user ID that can perform all administration-related tasks via the Cisco IPICS Administration Console. Cisco IPICS creates this web-based user ID during the software installation process.
<b>IPSec</b>	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

<b>keepalive</b>	A message that is sent by one network device to inform another network device that the virtual circuit between the two devices is still active.
<b>key</b>	<p>The parameter that defines an encryption code or method.</p> <p>Key (a radio) causes the radio to transmit. <i>See</i> tone keyed.</p>
<b>kilohertz (kHz)</b>	A unit of frequency that denotes one thousand Hz.

---

## L

<b>linear modulation</b>	A radio frequency transmission technique that provides the physical transport layer of a radio system. This technology is compatible in digital and analog system environments and supports channel bandwidths of 5 kHz to 50 kHz.
<b>LLGT</b>	low level guard tone. This tone is used as a hold tone or keying tone. <i>See</i> guard tone.
<b>LMR</b>	<p>Land Mobile Radio. A Land Mobile Radio (LMR) system is a collection of portable and stationary radio units that are 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.</p> <p>This term is often used interchangeably between a handheld or vehicle-mounted device and a stationary transmitter. Stationary devices are typically referred to as base stations.</p> <p>Cisco IPICS leverages the Cisco Hoot 'n' Holler feature, which is enabled in specific Cisco IOS versions, to provide radio integration into the Cisco IPICS solution. LMR is integrated by providing an ear and mouth (E&amp;M) interface to a radio or other PTT devices, such as Nextel phones. Configured as a voice port, this interface provides the appropriate electrical interface to the radio. You configure this voice port with a connection trunk entry that corresponds to a voip dial peer, which in turn associates the connection to a multicast address. This configuration allows you to configure a corresponding channel in Cisco IPICS, using the same multicast address, which enables Cisco IPICS to provide communication paths between the desired endpoints.</p>
<b>LMR gateway</b>	Land Mobile Radio gateway. Refers to the router E&M interface that converts IP traffic from digital to analog for use by radios.

**location** In Cisco IPICS, location signifies reachability; meaning, channels or users who are associated with the same location can communicate with each other without additional network configuration. Location may refer to a physical or virtual location, as defined in the server.

**low-band frequency** Lower frequency levels in the VHF band, typically 25–50 MHz.

---

## M

**megahertz (MHz)** A unit of frequency denoting one million Hz.

**mixed tone** Two tones that are mixed together. DTMF is an example of a mixed tone. To be transmitted properly, tone signals must be mixed with the LLGT. *See* DTMF.

**m-lead** The mouth portion of the E&M interface. The m-lead is the transmit path of the LMR gateway.

**modulation** The process, or result of the process, of varying a characteristic of a carrier in accordance with an information-bearing signal.

**multicast** Single packets that are copied by the network and sent to a specific subset of network addresses. Multicast refers to communications that are sent between a single sender and multiple recipients on a network.

**multicast address** A single address that may refer to multiple network devices.

**multicast address/port** Cisco IPICS uses this type of connection to enable the IDC to directly tune in to the multicast channel. Multicast address/port combinations are also used by gateways and UMS components.

**multicast pool** Multicast IP addresses that are defined as part of a multicast pool. Cisco IPICS allocates a multicast address from this pool of resources when a dispatcher activates a VTG.

**multiplexing** The combination of two or more information channels on to a common transmission medium. In electrical communications, the two basic forms of multiplexing are time-division multiplexing (TDM) and frequency-division multiplexing (FDM).

**multipurpose policy** A policy that can include any of the supported actions; may be invoked through the telephony user interface or the Cisco IPICS administration console.

**mutual aid channel** A national or regional channel that has been set aside for use only in mutual aid interoperability situations. Restrictions and guidelines governing usage usually apply.

---

## N

**narrowband channels** Channels that occupy less than 20 kHz.

**National Public Safety Planning Advisory Committee** The committee that was established to conduct nationwide planning and allocation for the 821–824 MHz and 866–869 MHz bands.

<b>National Telecommunication and Information Administration</b>	The United States executive branch agency that serves as the principal advisor to the president on telecommunications and information policies and that is responsible for managing the federal government's use of the radio spectrum.
<b>near end</b>	The device or devices that are physically connected to the Ethernet or an RS-232 link. Compare with far end, which refers to devices on the other side of the broadcast. A base station that is connected to an LMR gateway is a near end device while a handheld radio that receives over-the-air signals from the base station is a far end device.
<b>network</b>	An interconnection of communications entities.
<b>NAT</b>	Network Address Translation. Provides a mechanism for translating addresses that are not globally unique into globally routable addresses for connection to the Internet.
<b>not activated</b>	A VTG state that becomes effective when the Activate button is clicked a second time (to deactivate the channel) or if the connection terminates. No IDC buttons appear highlighted.
<b>notification</b>	<p>An action that notifies selected user(s) via email, SMS, pager, or phone. The necessary IDs and phone numbers are configured in the communication preferences for each user. Notifications that are sent via the phone require user authentication before the notification prompt is heard.</p> <p>An email, SMS, pager, or phone call that is placed to a user for the purpose of sending a notification message.</p>

---

**O**

<b>operator</b>	The Cisco IPICS operator is responsible for setting up and managing users, configuring access privileges, and assigning user roles and ops views.
<b>ops view</b>	operational view. A Cisco IPICS feature that provides the ability to organize users, user groups, channels, channel groups, VTGs, and policies into different user-definable views across multiple organizations or agencies that normally would not share resources. While ops views are maintained separately by the Cisco IPICS system administrator and/or ops view administrator, this functionality also allows multiple entities to use one Cisco IPICS server to enable resource sharing across multiple ops views, according to business need.
<b>ops view administrator</b>	The ops view administrator capabilities include managing and monitoring the activity logs that are filtered by ops views and accessible in the Administration Console ( <b>Administration &gt; Activity Log Management</b> ) window.
<b>OTAR</b>	over-the-air re-keying. Provides the ability to update or modify over radio frequency the encryption keys that are programmed in a mobile or portable radio.

---

**P**

<b>packet</b>	A logical grouping of information that includes a header that contains control information. Usually also includes user data.
---------------	--



<b>packet switching</b>	The process of routing and transferring data by using addressed packets so that a channel is occupied during the transmission of the packet only. Upon completion of the transmission, the channel is made available for the transfer of other traffic.
<b>PIM</b>	Protocol Independent Multicast. Multicast routing architecture that allows the addition of IP multicast routing on existing IP networks. PIM is unicast routing protocol independent and can be operated in two modes: PIM dense mode and PIM sparse mode.
<b>PIM dense mode</b>	One of the two PIM operational modes. PIM dense mode is data-driven and resembles typical multicast routing protocols. Packets are forwarded on all outgoing interfaces until pruning and truncation occurs. In dense mode, receivers are densely populated, and it is assumed that the downstream networks want to receive and will probably use the datagrams that are forwarded to them. The cost of using dense mode is its default flooding behavior. Sometimes called dense mode PIM or PIM DM.
<b>PIM sparse mode</b>	One of the two PIM operational modes. PIM sparse mode tries to constrain data distribution so that a minimal number of routers in the network receive it. Packets are sent only if they are explicitly requested at the RP (rendezvous point). In sparse mode, receivers are widely distributed, and the assumption is that downstream networks will not necessarily use the datagrams that are sent to them. The cost of using sparse mode is its reliance on the periodic refreshing of explicit join messages and its need for RPs. Sometimes called sparse mode PIM or PIM SM.
<b>policy</b>	Policies include one or more actions that execute sequentially and can be manually activated via the Cisco IPICS administration console or the telephony user interface. Cisco IPICS provides support for multiple policy types.
<b>policy execution status</b>	An indicator of policy execution success or failure. The Cisco IPICS administration console provides a status for each action under a policy.
<b>portalization</b>	A web programming paradigm for customizing the interface and functionality of a client application.
<b>preamble</b>	The sequence of tones that precede a transmission. The preamble generally includes the HLGT and the function tone.
<b>protocol</b>	A set of unique rules that specify a sequence of actions that are necessary to perform a communications function.
<b>PTT</b>	Push-to-talk. A signal to a radio transmitter that causes the transmission of radio frequency energy.  The action that keys a radio or causes the radio to transmit. On the Cisco router, the e-lead, or key tone, is used to signal the radio to transmit.
<b>PTT channel</b>	A channel consists of a single unidirectional or bidirectional path for sending and/or receiving signals. In the Cisco IPICS solution, a channel represents one LMR gateway port that maps to a conventional radio physical radio frequency (RF) channel.
<b>PTT channel button</b>	The button on the IDC that you click with your mouse, or push, and hold to talk. You can use the latch functionality on this button to talk on one or more channels at the same time.
<b>PTT channel group</b>	A logical grouping of available PTT channels that can be used for categorization.

---

Q

<b>QoS</b>	quality of service. A measurement of performance for a transmission system, including transmission quality and service availability.
<b>queue</b>	Represents a set of items that are arranged in sequence. Queues are used to store events occurring at random times and to service them according to a prescribed discipline that may be fixed or adaptive.
<b>queuing delay</b>	In a radio communication system, the queuing delay specifies the time between the completion of signaling by the call originator and the arrival of a permission to transmit to the call originator.

---

R

<b>radio channel</b>	Represents an assigned band of frequencies sufficient for radio communication. The bandwidth of a radio channel depends upon the type of transmission and its frequency tolerance.
<b>radio control service</b>	The logical element in the Cisco IPICS system that can tune a radio to the desired channel without manual intervention. Refers to a serial control entity.
<b>radio equipment</b>	Any equipment or interconnected system or subsystem of equipment (both transmission and reception) that is used to communicate over a distance by modulating and radiating electromagnetic waves in space without artificial guide. This equipment does not include microwave, satellite, or cellular telephone equipment.
<b>remote connection</b>	Cisco IPICS uses this type of connection to provide SIP-based trunking into the UMS component, which is directly tuned into the multicast channel.
<b>RF</b>	radio frequency. Any frequency within the electromagnetic spectrum that is normally associated with radio wave propagation. RF generally refers to wireless communications with frequencies below 300 GHz.
<b>RFC 2833</b>	The Internet Engineering Task Force (IETF) specification that describes how to carry DTMF signaling, other tone signals, and telephony events in RTP packets. Using RFC 2833 a packet can be compactly composed to play a series of tones, including DTMF, in a specific sequence that includes specified durations and volume levels.
<b>RF repeater</b>	An analog device that amplifies an input signal regardless of its nature (analog or digital). Also, a digital device that amplifies, reshapes, retimes, or performs a combination of any of these functions on a digital input signal for retransmission.
<b>root user ID</b>	The Cisco IPICS Linux user that has access to all files in the Cisco IPICS server. Strong passwords are enforced and Linux operating system password expiration rules apply to this user ID.
<b>RTP</b>	Real-Time Transport Protocol. Commonly used with IP networks to provide end-to-end network transport functions for applications that transmit real-time data, such as audio, video, or simulation data, over multicast or unicast network services.
<b>RTCP</b>	Real-time Transport Control Protocol. The standard for notifying senders and receivers of important events or transmission statistics. The most common forms of RTCP are the sender report and the receiver report.

## S

<b>scanning</b>	A subscriber unit feature that automatically allows a radio to change channels or talk groups to enable a user to listen to conversations that are occurring on different channels or talk groups.
<b>script prompts</b>	The audio prompts that the dial engine scripts play out during execution and which callers hear when they are interacting with the telephony user interface.
<b>secure channel</b>	<p>A channel that is connected to a radio that provides secure (encrypted or scrambled) communications on the Common Air Interface (CAI) side of the radio. (The level of security that is configured in the data network determines the security of the communications between the LMR gateway and a network attached device, such as an IDC or Cisco Unified IP Phone.)</p> <p>An attribute that is set in the server to indicate that a channel is secure. A PTT channel that is configured as secure cannot be combined with unsecure channels in a VTG.</p>
<b>serial controlled radio</b>	A type of control for a radio that uses out-of-band signaling (usually RS-232). <i>See</i> radio control service.
<b>service delivery area</b>	<i>See</i> coverage.
<b>signal</b>	The detectable transmitted energy that carries information from a transmitter to a receiver.
<b>speaker arbitration</b>	The procedure that is used to determine the active audio stream in a Push-to-Talk system.
<b>spectrum</b>	<p>The usable radio frequencies in the electromagnetic distribution. The following frequencies have been allocated to the public safety community:</p> <p>High HF 25–29.99 MHz  Low VHF 30–50 MHz  High VHF 150–174 MHz  Low UHF 406.1–420/450–470 MHz  UHF TV Sharing 470–512 MHz  700 MHz 764–776/794–806 MHz  800 MHz 806–824/851–869 MHz</p>
<b>spoken names</b>	The recorded names that are used for entities, such as channels, channel groups, VTGs, users, user groups, ops views, and policies. The names can be recorded through the policy engine or externally-recorded .wav files that can be uploaded into the system.
<b>squelch</b>	An electric circuit that stops input to a radio receiver when the signal being received is too weak to be anything but noise.
<b>statically configured tone control</b>	Every stream of data that flows to the LMR gateway can be applied with a preamble and/or guard tone by using a static configuration in the LMR gateway. When traffic is sent on a multicast address, the radio automatically switches (because of the preamble) to the specific radio channel that is requested by the tone control sequence.
<b>stored VTG</b>	Also referred to as inactive VTG.
<b>subchannel</b>	A channel that shares the same multicast address as another channel or channels. These multiple source streams (channels) may be present on a single radio channel.
<b>subscriber unit</b>	A mobile or portable radio unit that is used in a radio system.

<b>system administrator</b>	The Cisco IPICS system administrator is responsible for installing and setting up Cisco IPICS resources, such as servers, routers, multicast addresses, locations, and PTT channels. The system administrator also creates ops views, manages the Cisco IPICS licenses, and monitors the status of the system and its users via the activity log files.
<b>system architecture</b>	The design principles, physical structure, and functional organization of a land mobile radio system. Architectures may include single site, multi-site, simulcast, multicast, or voting receiver systems.
<hr/>	
<b>T</b>	
<b>T1</b>	Digital WAN carrier facility. T1 transmits DS-1-formatted data at 1.544 Mbps through the telephone-switching network, using alternate mark inversion (AMI) or binary 8 zero suppression (B8ZS) coding.
<b>T1 loopback</b>	Allows mapping from multicast to unicast so that unicast phone calls can be patched into an LMR or into other multicast audio streams. A loopback is composed of two of the available T1 interfaces.
<b>talk group</b>	<p>A VTG or a channel.</p> <p>A subgroup of radio users who share a common functional responsibility and, under normal circumstances, only coordinate actions among themselves and do not require radio interface with other subgroups.</p>
<b>TCP</b>	Transmission Control Protocol. A connection-oriented transport layer protocol that provides reliable full-duplex data transmission. TCP is part of the TCP/IP protocol stack.
<b>TDMA</b>	time division multiple access. Type of multiplexing where two or more channels of information are transmitted over the same link by allocating a different time interval (“slot” or “slice”) for the transmission of each channel; that is, the channels take turns to use the link.
<b>terminal</b>	A device capable of sending, receiving, or sending and receiving information over a communications channel.
<b>throughput</b>	The number of bits, characters, or blocks passing through a data communications system, or a portion of that system.
<b>TIA/EIA-102 standards</b>	A joint effort between government and industry to develop voice and data technical standards for the next generation of public safety radios.
<b>tone control</b>	The process of using inband tone sequences to change the behavior of a radio end point. An inband tone can be used to control functions, such as modifying (retuning) the radio frequency (RF channel), changing the transmit power level, and monitoring a channel. The most basic form of tone control (tone keyed) is used to key the radio. With the Cisco IPICS solution, the radio that is being controlled is directly connected to the LMR gateway E&M leads.
<b>tone frequency</b>	A specific form of a function tone. The tone that is used to signal the radio to select a frequency. These audible tone frequencies are generated in the router and combined in a specific sequence to perform a tone control function.
<b>tone keyed</b>	A tone keyed radio requires the presence of a specific tone on the incoming analog (e-lead) port. Without this tone, the radio cannot transmit. The tone is generally used to prevent spurious transmission that may occur because of injected noise.

<b>tone signaling</b>	Any form of over-the-air audible signals that are intended to terminate at the far end. Examples include alerting tones, DTMF tones, and paging tones.
<b>trigger</b>	A time-based event that invokes a policy on a scheduled basis, without manual intervention.
<b>trunk</b>	A physical and logical connection between two switches across which network traffic travels. In telephony, a trunk is a phone line between two central offices (COs) or between a CO and a PBX.
<b>trunked (system)</b>	Systems with full feature sets in which all aspects of radio operation, including RF channel selection and access, are centrally managed.
<b>trunked radio system</b>	Integrates multiple channel pairs into a single system. When a user wants to transmit a message, the trunked system automatically selects a currently unused channel pair and assigns it to the user, decreasing the probability of having to wait for a free channel.
<b>TUI</b>	telephony user interface. The telephony interface that the dial engine provides to enable callers to perform tasks, such as joining talk groups and invoking policies.
<b>tune (a radio)</b>	To change the current send and receive frequencies on a radio. This task is usually accomplished via a preset with some form of radio control.

---

## U

<b>user</b>	The Cisco IPICS user may set up personal login information and specify communication preferences that are used to configure audio devices. By using a predefined user ID and profile, the user can participate in PTT channels and VTGs by using supported Cisco Unified IP Phone models, the Cisco Mobile Client, or the Public Switched Telephone Network (PSTN) via the telephony dial functionality of the Cisco IPICS IP policy engine. Users may have one or more Cisco IPICS roles, such as system administrator, ops view administrator, operator or dispatcher.
<b>UMS</b>	The Unified Media Service (UMS) is a highly available, software-based media engine that performs several core functions in a Cisco IPICS deployment.
<b>unicast</b>	Specifies point-to-point transmission, or a message sent to a single network destination.

---

## V

<b>VAD</b>	Voice Activity Detection. When VAD is enabled on a voice port or on a dial peer, only audible speech is transmitted over the network. When VAD is enabled on Cisco IPICS, the IDC only sends voice traffic when it detects your voice.
<b>virtual channel</b>	A virtual channel is similar to a channel but a radio system may not be attached. By creating a virtual channel, participants who do not use physical handheld radios to call into a VTG become enabled by using the IDC application or a supported Cisco Unified IP Phone model.
<b>voice interoperability</b>	Voice interoperability enables disparate equipment and networks to successfully communicate with each other.

<b>VoIP</b>	Voice over Internet Protocol. By digitalizing and packetizing voice streams, VoIP provides the capability to carry voice calls over an IP network with POTS-like functionality, reliability, and voice quality.
<b>VOX</b>	Voice-operated transmit. A keying relay that is actuated by sound or voice energy above a certain threshold and sensed by a connected acousto-electric transducer. VOX uses voice energy to key a transmitter, eliminating the need for push-to-talk operation.
<b>VTG</b>	virtual talk group. A VTG can contain any combination of channels, channel groups, users, and user groups. A VTG can also contain other VTGs.
<b>VTG add participant</b>	An action that adds selected participant(s) to the selected VTG.

---

## W

<b>wavelength</b>	The representation of a signal as a plot of amplitude versus time.
<b>wideband channel</b>	Channels that occupy more than 20 kHz.




---

## A

access control list (ACL) [4-10, 4-15](#)  
 aggressive VAD [4-7](#)  
 Android devices [2-29](#)  
 Assured Forwarding [4-11](#)  
 assured forwarding 31 (AF31) [4-8](#)  
 Asynchronous Transfer Mode Peak Cell Rate (ATM PCR) [4-4](#)

---

## B

bandwidth  
     codec affect on [4-5](#)  
     consumption [4-5, 4-6](#)  
     issues [4-4](#)  
     modifying consumption [4-6](#)  
     multicast over GRE [7-12](#)  
     planning [4-4](#)  
     provisioning [4-2](#)  
     usage [4-5, 4-6](#)  
     voice payload [4-7](#)  
 bidirectional PIM [4-2, 4-3](#)  
 bridging channels [2-11](#)  
     *See also* mixing  
 broadcast VTG [2-16](#)  
 burst [4-4](#)

---

## C

cabling, for VIC2-2E/M interface card [3-2](#)  
 call leg [5-1, 5-3](#)  
 Carrier Operated Relay (COR) [3-11, 4-7](#)

carrier operated relay (COR) [3-8](#)  
 Carrier Operated Squelch [3-11](#)  
 Carrier Operated Squelch (COS) [3-8, 4-7](#)  
 Cisco Instant Connect for Android Devices  
     description [2-29](#)  
     guidelines [2-29](#)  
     overview [1-3](#)  
     using with Cisco Jabber [2-31](#)

### Cisco IOS

configuration for LMR gateway [3-7](#)  
 queuing techniques [4-9](#)

### Cisco IPICS

codec [4-4](#)  
 components  
     Cisco Instant Connect for Android Devices [1-3](#)  
     Cisco Instant Connect for Microsoft Windows [1-4](#)  
     Cisco Instant Connect MIDlet [1-4](#)  
     Cisco IPICS server [1-3](#)  
     Cisco Unified IP Phone gateway [1-4](#)  
     DFSIG [1-4](#)  
     IDC [1-3](#)  
     ISSIG [1-4](#)  
     LMR gateway [1-4](#)  
     mobile client [1-3](#)  
     networking components [1-4](#)  
     overview [1-2](#)  
     RMS [1-3, 2-5](#)  
     UMS [1-3, 1-4](#)  
 deployment models [7-1](#)  
 markets [1-1](#)  
 mobile client, using DNS with [2-30](#)  
 multiple site model [7-2](#)

- overview [1-1](#)
- single site model [7-1](#)
- UMS configuration for mixing [2-16](#)
- voice streams supported [2-13](#)
- WAN deployment issues [4-1](#)
- Cisco IPICS Dispatch Console
  - See* IDC
- Cisco IP Interoperability and Collaboration System
  - See* Cisco IPICS
- Cisco Jabber [2-31](#)
- Cisco Multicast Manager (CMM) [4-16](#)
- Cisco Safety and Security Desktop (SASD), use with IDC [2-39](#)
- Cisco Unified Communications Manager
  - configuration overview [2-35](#)
  - using with Cisco Unified IP Phone [2-34](#)
- Cisco Unified Communications Manager Express
  - configuration [2-35](#)
  - using with Cisco Unified IP Phone [2-34](#)
- Cisco Unified IP Phone
  - Cisco Communications Manager Express configuration for [2-35](#)
  - Cisco Unified Communications Manager configuration for [2-35](#)
  - configuring for Cisco IPICS [2-34](#)
  - overview [1-4](#)
  - services [2-34](#)
- Class-Based Weighted Fair Queuing (CBWFQ) [4-10](#)
- codec
  - bandwidth use [4-5](#)
  - choosing [4-4](#)
  - considerations [4-4](#)
  - G.711 [4-4](#)
  - G.729a [4-4](#)
  - types in Cisco IPICS [4-4](#)
  - voice quality [4-4](#)
- Committed Information Rate (CIR) [4-4](#)
- compressed RTP (cRTP) [4-5](#)
- cRTP [4-6](#)
- Customer Edge Router (CE) [7-4](#)

---

## D

- Data MDT [7-5, 7-9](#)
- Data Multicast Distribution Tree (MDT) [7-4](#)
- Default-MDT [7-4, 7-5](#)
- delay [4-1, 4-9](#)
- dense mode (SM) [4-2](#)
- destination pattern [5-3](#)
- DFSIG
  - components [3-71](#)
  - description [3-71](#)
  - overview [1-4](#)
- dial peer
  - call leg [5-1, 5-3](#)
  - destination pattern [5-3](#)
  - inbound [5-2](#)
  - inbound call leg [5-3](#)
  - matching inbound call leg [5-3](#)
  - matching outbound call leg [5-4](#)
  - outbound [5-2](#)
  - outbound call leg [5-4](#)
- POTS [5-2](#)
- session target [5-3](#)
- VoFR (Voice over Frame Relay) [5-2](#)
- voice-network [5-2](#)
- Voice over IP (VoIP) [5-2](#)
- dial pool [6-2](#)
- dial port, usage [6-2](#)
- Digital Fixed Station Interface Gateway
  - See* DFSIG
- digital signal processor (DSP) [4-7](#)
- discard eligible (DE) [4-11](#)
- DNS, configuration for mobile client [2-30](#)
- DS0
  - allocation [2-5](#)
  - channel optimization [2-13, 3-12](#)
  - loopback channels [2-5](#)
  - remote location requirements [2-12](#)
  - resource allocation [2-12](#)



- resource consumption [2-10, 2-11](#)
- resources not required [2-20](#)
- DSCP per-hop behaviors (Fibs) [4-11](#)
- DSP
  - channel optimization [2-13, 3-12](#)
  - signal detection [4-7](#)
- dspfarm [2-13, 3-12](#)
- duplicate packets [2-20](#)

---

## E

- E&M interface card
  - cabling [3-2](#)
  - overview [3-2](#)
- ear and mouth (E&M)
  - analog signaling types [3-4](#)
  - interface [3-1](#)
  - interface card [3-4](#)
  - Type III interface [3-5](#)
  - Type II interface [3-4](#)
  - Type V interface [3-6](#)
- EF Johnson radios, configuring serial radio control for [3-55](#)
- egress
  - policing [4-11](#)
  - shaping [4-11](#)
- endpoints
  - communication between [2-10, 2-15](#)
  - duplicate packets [2-20](#)
- expedited forwarding (EF) [4-8](#)

---

## F

- feedback tones, for trunked radios [3-64](#)
- firewall [4-15](#)
- following [2-7](#)
- Frame Relay
  - IP RTP Priority [4-9](#)
  - LLQ [4-10](#)

---

## G

- G.711 [4-4, 7-2](#)
- G.729a [4-4](#)
- GRE tunnel [7-11](#)

---

## H

- Hoot 'n' Holler [3-1, 4-8](#)

---

## I

- IDC
  - overview [1-3](#)
  - use with SASD [2-39](#)
- incident VTG [2-16](#)
- Internet Group Management Protocol (IGMP) [2-16, 2-17](#)
- interoperability and collaboration [1-1](#)
- IP
  - precedence [4-8](#)
  - RTP Priority [4-9](#)
- IPSSec VPN [7-13](#)
- ISSIG
  - components [3-70](#)
  - description [3-70](#)
  - interoperability modes [3-71](#)
  - overview [1-4](#)
- ISSI Gateway
  - See* ISSIG

---

## J

- jitter [4-2, 4-9](#)

---

## L

- land mobile radio
  - See* LMR

## land mobile radio gateway

- configuring for E&M communication [3-57, 3-61](#)

- configuring for serial radio control [3-58, 3-63](#)

- connecting

- EF Johnson radio to [3-56](#)

- Sprint Nextel (iDEN) handset [3-60](#)

LDAP [2-29](#)

LEAF [7-4](#)

leased line [7-3](#)

licenses, for Cisco IPICS [6-1](#)

Lightweight Directory Access Protocol (LDAP) [2-29](#)

LMR

- audio connection to Cisco IPICS [3-2](#)

- channel [2-16](#)

- communication with endpoints [2-16](#)

- endpoints in [2-12](#)

- gateway

- Cisco IOS configuration for [3-7](#)

- radio interface [3-2](#)

- integration with Cisco IPICS [3-1](#)

- interface with Cisco IPICS [3-2](#)

- recording multicast traffic [3-69](#)

- use with Cisco Hoot 'n' Holler [3-1](#)

location, with UMS [2-3](#)

loopback [2-5](#)

- voice port [2-15](#)

Low-Latency Queuing (LLQ) [4-9, 4-10](#)

---

## M

mixing

- audio [2-17](#)

- channels in VTG [2-15](#)

- DSP function [4-8](#)

- voice streams [2-17, 4-8](#)

mobile client [2-29](#)

- DNS, using with [2-30](#)

- overview [1-3](#)

MPLS

- in multiple site model [7-2](#)

- VPN [7-3](#)

- with multicast VPN [7-3](#)

multicast [4-6, 7-2](#)

- address

- for VTG communication [2-15](#)

- guidelines for using [2-41](#)

- address pool [2-6, 2-12](#)

- bandwidth [7-12](#)

- call flow to unicast [2-24](#)

- domain [7-2, 7-4, 7-5](#)

- endpoints, communication between [2-10](#)

- GRE tunnel [7-15](#)

- island

- overview [7-10](#)

- topology [7-10](#)

- over GRE [7-11](#)

- singularity

- GRE tunnel [7-14](#)

- overview [7-13](#)

Multicast Virtual Route Forwarding (MVRF) [7-4](#)

multicast VPN (MVPN) [7-4](#)

- provider network configuration for [7-5](#)

- provider network verification [7-7](#)

- routing [7-5](#)

multiple site model

- connectivity options [7-3](#)

- overview [7-2](#)

- topology [7-3](#)

Multiprotocol Label Switching

*See* MPLS

---

## N

network

- management [4-15](#)

- security in [4-14](#)

networking components, overview [1-4](#)

---

**O**

over-detection [4-7](#)

---

**P**

packet

    delay [4-9](#)

    errors [4-2](#)

    loss [4-2, 4-9](#)

patch VTG [2-16](#)

Permanent Virtual Circuit (PVC) [4-3](#)

PIM-SSM [7-4](#)

ping-pong effect [3-64](#)

point-to-point call [2-31](#)

policing [4-11](#)

pooled radio

    allocating [3-53](#)

    configuring [3-53](#)

    overview [3-52](#)

Protocol Independent Multicast (PIM)

    bidirectional [4-2, 4-3](#)

    dense mode (DM) [4-2](#)

    overview [4-2](#)

    sparse mode (SM) [4-2](#)

Provider Edge Router (PE) [7-4, 7-5](#)

Provider Router (P) [7-4](#)

---

**Q**

QoS

    at WAN edge [4-11](#)

    factors affecting [4-8](#)

    in enterprise [4-12](#)

    in LAN [4-10](#)

    in multiple site model [7-3](#)

    overview [4-8](#)

    policing [4-11](#)

    queuing [4-11](#)

    recommendations for networks [4-8](#)

    trust boundary [4-12](#)

    WAN, use in [4-2](#)

Quality of Service

*See* QoS

queuing

    overview [4-11](#)

    techniques [4-9](#)

---

**R**

RADIUS [4-15](#)

Real-time Transport Protocol (RTP) [4-6](#)

recording

    multicast LMR traffic [3-69](#)

    Tap Cisco IOS configuration [3-69](#)

remote location [2-6, 2-12](#)

remote user, UMS function with [2-4](#)

rendezvous point (RP) [4-2](#)

Reverse Path Forwarding (RPF) [4-3](#)

RMS

    configuration example [2-7](#)

    DS0 [2-5, 2-10, 2-12](#)

    DS0 resources [2-20](#)

    function [2-5](#)

    function in Cisco IPICS [2-10](#)

    installation options [2-5](#)

    mixing [2-16, 2-17](#)

    overview [1-3](#)

    resource allocation [2-12](#)

    resource consumption [2-10, 2-12](#)

router media service

*See* RMS

RTP, header compression [4-6](#)

---

**S**

SASD, use with IDC [2-39](#)

- scan VTG 2-16
  - Secure Socket Layer (SSL) 4-15
  - security
    - access control list (ACL) 4-15
    - firewall 4-15
    - for Cisco IPICS 4-14
    - RADIUS 4-15
    - recommendations 4-15
    - Secure Socket Layer (SSL) 4-15
    - spanning tree (STP) attack mitigation 4-15
    - TACACS+ 4-15
  - serialization 4-9
  - serial radio control
    - EF Johnson Radios
      - components required 3-55
      - configuring LMR gateway for E&M communications 3-57
      - configuring LMR gateway for serial radio control 3-58
      - connecting to LMR gateway 3-56
      - overview 3-55
    - overview 3-55
    - Sprint Nextel (iDEN) handsets
      - components required 3-60
      - configuring handset 3-61
      - configuring LMR gateway for E&M communication 3-61
      - configuring LMR gateway for serial radio control 3-63
      - connecting to LMR gateway 3-60
      - overview 3-59
  - session target 5-3
  - shared tree
    - bidirectional 4-2
    - forwarding traffic 4-3
    - in PIM SIM 4-2
    - unidirectional 4-2
  - single site model
    - benefits 7-2
    - best practices 7-2
    - design characteristics 7-1
    - overview 7-1
    - topology 7-2
  - SIP
    - provider for policy engine 1-4
    - signaling flow 2-23
  - spanning tree (STP) attack mitigation 4-15
  - sparse mode (SM) 4-2
  - Sprint Nextel (iDEN) handset
    - configuring serial radio control for 3-59
  - Sprint Nextel (iDEN handset)
    - configuring for serial radio control 3-61
  - Sustained Cell Rate 4-4
- 
- ## T
- TACACS+ 4-15
  - talk priority 2-4
  - Time to Live (TTL) 2-25
  - tone control
    - 2-wire configuration for single frequency 3-40
    - 4-wire configuration for single frequency 3-41
    - channel configurations in Cisco IPICS 3-51
    - configuration for two-ten frequencies 3-42
    - considerations 3-12
    - frequencies 3-17
    - manual tone configuration 3-14
    - native functionality 3-13
    - phases 3-15
    - signaling 3-15
  - topology
    - MPLS with multicast VPN 7-4
    - multicast island 7-10
    - multiple site model 7-3
    - single site model 7-2
  - trunked radio
    - feedback tones 3-64
    - hybrid configuration 3-65

## trust

- between Cisco IPICS nodes [2-38](#)
- boundary [4-12](#)

---

**U**
UDP port [4-9](#)

## UMS

- audio mixing [2-4](#)
- conserving resources [6-2](#)
- in Cisco IPICS deployment [2-2](#)
- in WAN that is not multicast enabled [4-6](#)
- license [6-1](#)
- locations, instances for [2-3](#)
- overview [1-3, 1-4, 2-2](#)
- remote user, function with [2-4](#)
- resource allocation [2-4](#)
- resource consumption [2-21](#)
- scaling [2-3](#)
- when required [2-3](#)

under-detection [4-7](#)

## unicast

- connection set up [2-23](#)
- in WAN that is not multicast enabled [4-6](#)

## Unified Media Service

*See* UMS

---

**V**
Virtual Private Network (VPN) [7-3](#)

## virtual talk group

*See* VTG

## voice

- packet [4-7](#)
- payload [4-7](#)
- quality [4-4, 4-7, 4-8](#)

## voice activation detection (VAD)

- aggressive [4-7](#)

conventional [4-7](#)enabling [4-7](#)overview [4-7](#)use with LMR [3-8, 3-9](#)Voice and Video Enabled IP Security Protocol (IPSec) [7-3](#)voice streams, supported in Cisco IPICS [2-13](#)VoIP bearer traffic [4-12](#)VoIP traffic, transmission rate [4-5](#)

## VPN

- in deployment scenarios [4-14](#)
- multicast routing [7-5](#)
- with MLPS [7-3](#)

## VTG

- about [2-15](#)
- broadcast [2-16](#)
- communication between channels [2-15](#)
- creation [2-15](#)
- incident [2-16](#)
- LMR endpoints in [2-12](#)
- members [2-15](#)
- mixing of channels [2-15](#)
- multicast address [2-15](#)
- multicast address requirements [2-12](#)
- patch [2-16](#)
- restricting access [2-22](#)
- RMS resource consumption [2-12](#)
- scan [2-16](#)
- types [2-16](#)

---

**W**
Weighted-Fair Queuing (WFQ) [4-9](#)

## wireless network

- configuration example [2-32](#)
- overview [2-31](#)

