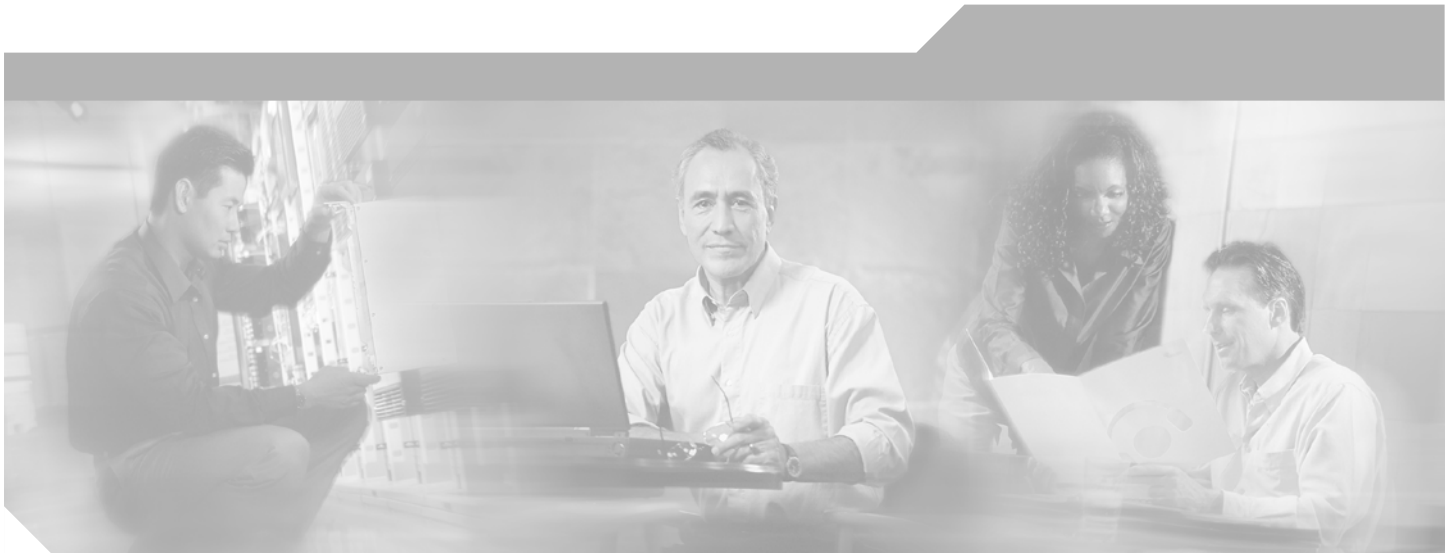


Solution Reference Network Design (SRND) for Cisco IPICS Release 1.0(2)

December, 2006

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

Text Part Number: OL-10928-02

Solution Reference Network Design (SRND) for Cisco IPICS Release 1.0(2)

CONTENTS

Preface

Overview

This *Solution Reference Network Design (SRND)* document provides design considerations and guidelines for deploying Cisco IPICS. This document should be used with the following related documentation:

- For Cisco IPICS documentation, go to this URL:

  http://www.cisco.com/univercd/cc/td/doc/product/cis/cupids/index.htm

- For other SRND documents, go to this URL:

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

Revision History

This document may be updated at any time without notice. You can obtain the latest version of this document at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/cis/c_ipics/index.htm

Check the Cisco.com website periodically for documentation updates by comparing the date on the title page of your copy with the date of the online document.

Organization

This manual is organized as follows:

Chapter 1, "Introducing Cisco IPICS"	Describes the advantages and benefits that Cisco IPICS offers and introduces the primary components that make up a Cisco IPICS deployment
Chapter 2, "Cisco IPICS Component Considerations"	Provides information about various Cisco IPICS components
Chapter 3, "Cisco IPICS Infrastructure Considerations"	Provides information about network infrastructure considerations that you must be aware of when you deploy Cisco IPICS

Chapter 4, "Understanding Dial Peers"	Provides an overview of dial peers, which will help you understand how Cisco IPICS operates
Chapter 5, "Cisco IPICS Deployment Models"	Describes the deployment models for Cisco IPICS

Related Documentation

The following Cisco IPICS documentation is available at this URL:

- *Cisco IPICS PMC Quick Start Guide, Release 1.0(1)*—This document provides tips and quick references for the most frequently used procedures that a user can perform on the Cisco IPICS PMC.
- *Cisco IPICS PMC Debug Reference Quick Start Guide, Release 1.0(1)*—This document provides a quick reference for troubleshooting and debugging the Cisco IPICS PMC.
- *Cisco IPICS Server Administration Guide, Release 1.0(1)*—This document contains information about the key configuration, operation, and management tasks for the Cisco IPICS server.
- *Cisco IPICS Server Installation Guide, Release 1.0(1)*—This document describes how to install and configure the Cisco IPICS server software and Linux operating system.
- *Cisco IPICS Troubleshooting Guide, Release 1.0(1)*—This document contains reference material about how to maintain and troubleshoot the Cisco IPICS system.
- *Cisco IPICS Backup and Restore Guide, Release 1.0(1)*—This document describes the administrative procedures that you use to backup and restore the database files on the Cisco IPICS server.
- *Cisco IPICS Command Line Interface, Release 1.0(1)*—This document describes the commands that you can use from the command line interface (CLI) to obtain information or to change settings for the Cisco IPICS PMC.
- *Release Notes for Cisco IPICS Release 1.0(2)*—This document contains a description of the new and changed features, important notes, caveats, and documentation updates for this release of Cisco IPICS.
- *Cisco IPICS 1.0(2) Resources Card (Documentation Locator)*—This document provides a summary of the documentation that is available for this release of Cisco IPICS.
- *Cisco IPICS Compatibility Matrix*—This document contains information about compatible hardware and software that is supported for use with Cisco IPICS.

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

http://www.cisco.com/univercd/cc/td/doc/product/cis/c_ipics/index.htm

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

Obtaining Documentation

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

Cisco.com

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

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

Product Documentation DVD

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

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

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

Ordering Documentation

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

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

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

Documentation Feedback

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

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

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

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

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- For Nonemergencies—psirt@cisco.com

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

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

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

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

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

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

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

Obtaining Technical Assistance

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

Cisco Technical Support & Documentation Website

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

http://www.cisco.com/techsupport

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

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

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

Submitting a Service Request

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

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

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

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

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

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

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

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

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

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

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

  http://www.ciscopress.com

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

  http://www.cisco.com/packet

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

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

  or view the digital edition at this URL:

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

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

  http://www.cisco.com/ipj

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

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

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

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

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

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

Introducing Cisco IPICS

Cisco IP Interoperability and Collaboration System (Cisco IPICS) is an intelligent platform that controls media and information, enabling intra- and inter-organizational communication, interoperability, and operational efficiencies. By taking advantage of IP standards and protocols, Cisco IPICS bridges communications from existing and proprietary radio networks to IP networks and devices such as the Cisco IPICS Push-to-Talk Management Center (PMC), and supported models of the Cisco Unified IP Phone.

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

Communications interoperability, data integration, and true event- and incident-based contextual collaboration between agencies and organizations are important requirements in many markets, including the following segments:

- Enterprise (operations and safety and security)
- Commercial
- Financial Services
- Retail
- Education
- Healthcare
- Utilities
- Oil and gas
- Public safety
- Transportation
- Military/Defense

- 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, the Cisco IPICS solution provides the following benefits:

- Incident management framework graphical user interface (GUI)—Facilitates tasks that are associated with operations and command and control
- 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 new products, such as the Cisco IPICS server and the PMC, and existing technologies, such as land mobile radio (LMR), Cisco gateways, and VoIP. A deployment also employs applications of existing technologies, such as the use of the router media services (RMS) functionality for channel mixing.

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

Figure 1-1 Cisco IPICS Components

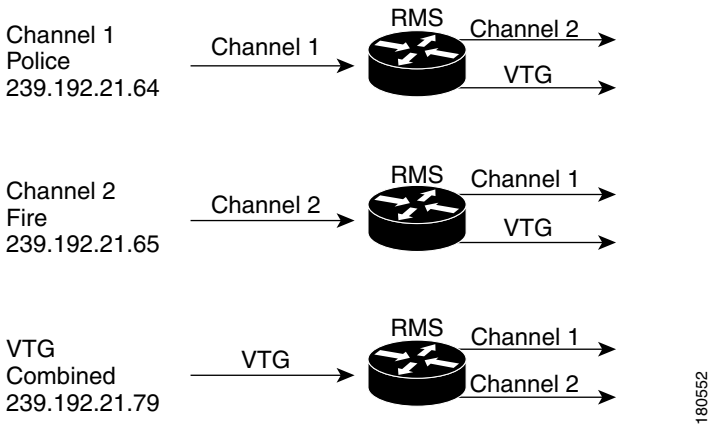


Table 1-1 provides an overview of the Cisco IPICS components. Other chapters in this manual provide more detailed information about using and configuring several of these components. In addition, Cisco provides a wide variety of technical and user documentation that explains in detail Cisco components 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, refer to *Cisco IPICS Compatibility Matrix*.

Table 1-1 Cisco IPICS Component Overview

Component	Description
Cisco IPICS server	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 Media Convergence Server (MCS) platforms and performs these functions: • Hosts the Cisco IPICS Administration Console, which is an incident management framework administration GUI that enables dynamic resource management for users, channels, and virtual talk groups (VTGs). • Provides Cisco IPICS authentication and security services • Stores configuration and operational data. • Enables integration with various media resources, such as RMS components, PMCs, and Cisco Unified IP Phones.
Push-to-Talk Management Center (PMC)	PC-based software application that runs on Microsoft Windows 2000 and Windows XP operating systems. The PMC comprises a stand-alone audio application that enables end-users, dispatch personnel, and administrators to participate, via an IP network, in one or more talk groups or VTGs at the same time. Through an intuitive interface, the PMC application lets users monitor and participate in one or multiple PTT channels or VTGs at the same time. Users install the PMC application on a PC after downloading the software from the Cisco IPICS server. Thereafter, Cisco IPICS automatically upgrades the PMC with new versions when they become available. In addition, Cisco IPICS manages configurations and settings on PMCs.This managed client approach simplifies the support of a Cisco IPICS deployment. The Cisco IPICS dispatcher assigns the channels and VTGs to the PMC users.

Table 1-1 Cisco IPICS Component Overview

Component	Description
Router media service (RMS)	Enables media services on selected Cisco routers and provides these capabilities: • Provides the functions that are required to combine two or more VTGs. • Multicast channel mixing, using the Cisco Hoot 'n' Holler feature, to support VTGs. • Enables PTT media convergence for multicast, unicast, TDM, and SIP endpoints. • Eliminates maintenance and management overhead for branch-server based media services. • Enables optimization of WAN bandwidth. • Integration with other key router features.
LMR gateway	LMR gateways provide voice interoperability between radio and non-radio networks by bridging radio channels and talk groups to IP multicast streams. The LMR gateway functionality is available in certain versions of Cisco IOS software.
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 CallManager or for Cisco CallManager Express.

CHAPTER 2

Cisco IPICS Component Considerations

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

This chapter includes these topics:

Router Media Service

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

The following sections provide additional information about the RMS:

For detailed information about configuring an RMS for Cisco IPICS, refer to the “RMS Configuration” appendix in *Cisco IPICS Server Administration Guide*.

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

RMS Overview

The primary role of an 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, refer to *Cisco IPICS Server*

Administration Guide.) When you use the Cisco IPICS Administration Console to add an RMS, the loopback pairs are available for assignment. A properly configured RMS makes a list of DS0 loopback channels available for dynamic allocation by the Cisco IPICS server.

The RMS can be installed as a standalone 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 a PMC from the remote location—When a remote PMC connection is started, the PMC authenticates to the Cisco IPICS server. The Cisco IPICS server then configures the RMS to allocate a DS0 loopback pair for each channel or VTG that is assigned to the PMC user. The PMC retrieves configuration information that contains the IP address of the RMS and the channel details with the POTS dial-peer information that the Cisco IPICS server configured in the RMS. Then, when the PMC user activates a channel or VTG, the PMC places a SIP call to the POTS dial-peer in the RMS and connects.
- 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 includes assigning each side of corresponding voice-port for the allocated DS0 loopback pair to a connection trunk.

Supporting 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 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. It is shared across each RMS that is configured in that Cisco IPICS server. Therefore, the network configuration must be able to support all of the configured addresses in each configured RMS. The Cisco IPICS server attempts to load balance across all RMS components that are in the same location.

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 functions 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 VTG Emergency, 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 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 5-2.

RMS Configuration Example

The following example shows what the Cisco IPICS server configures in an 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 IOS configuration output shows what the Cisco IPICS server configured in the RMS to support putting the Police channel in 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 40
 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 40
 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 IOS configuration output shows what the Cisco IPICS server configured in the RMS to support putting the Fire channel in 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 40
 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 40
 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 IOS configuration output examples show what the Cisco IPICS server configures in the RMS when a PMC user who is assigned both the Police and Fire channels connects using the remote location. This configuration allows the PMC to communicate with RMS using unicast. The RMS forwards the unicast stream, which is received from the PMC, 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 PMC device as unicast.

This IOS configuration output is for 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 40
 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 40
 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 IOS configuration output is for the Fire channel:

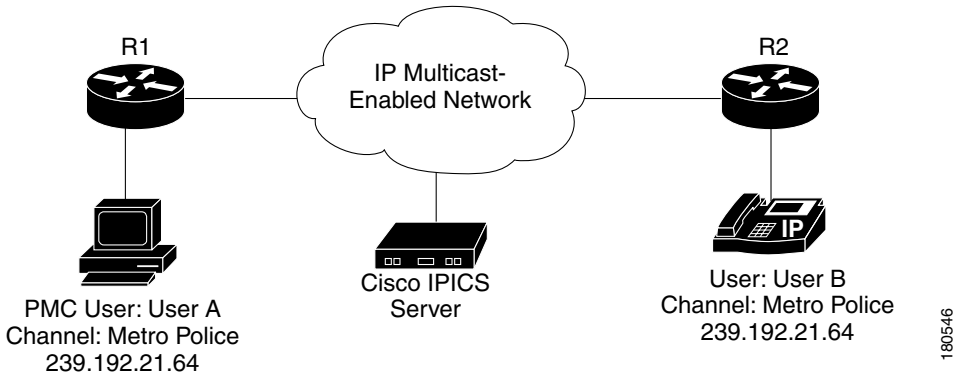
```
dial-peer voice 909290915 voip
 description #0/2/0:15#1164659525833# INUSE 296
 destination-pattern 909290915
 voice-class permanent 1
 session protocol multicast
 session target ipv4:239.192.21.65:21000
 codec g711ulaw
 no vad

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 40
 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 40
 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 (remote PMC to channel, remote PMC to VTG), and to establish connectivity between multicast endpoints that are on different channels (channel to VTG, VTG to VTG).

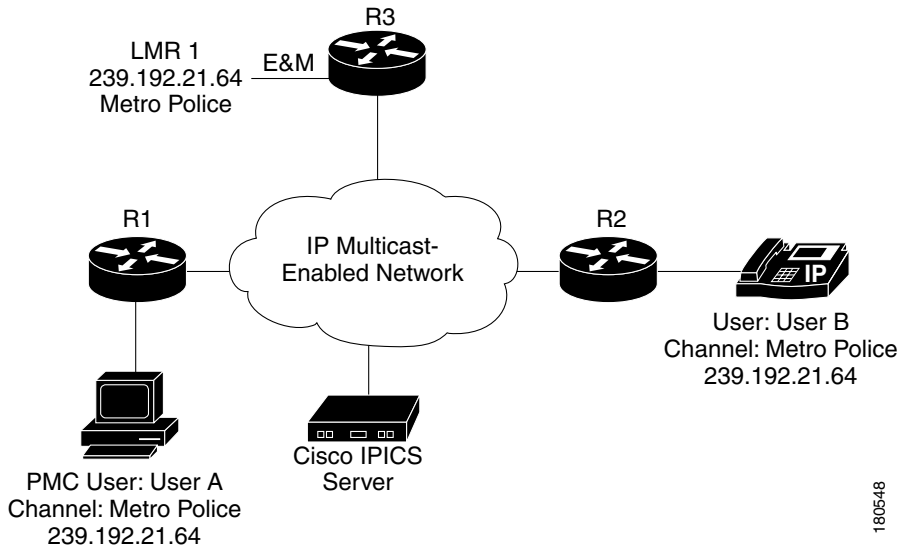
However, there are some communication scenarios that do not require RMS DS0 resources. For example, two multicast users can communicate on a single Cisco IPICS channel without consuming RMS DS0 resources, as illustrated in Figure 2-1. In this example, after the users log in to the Cisco IPICS server, they receive their channel information, which is 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 2-1 Single Cisco IPICS Channel



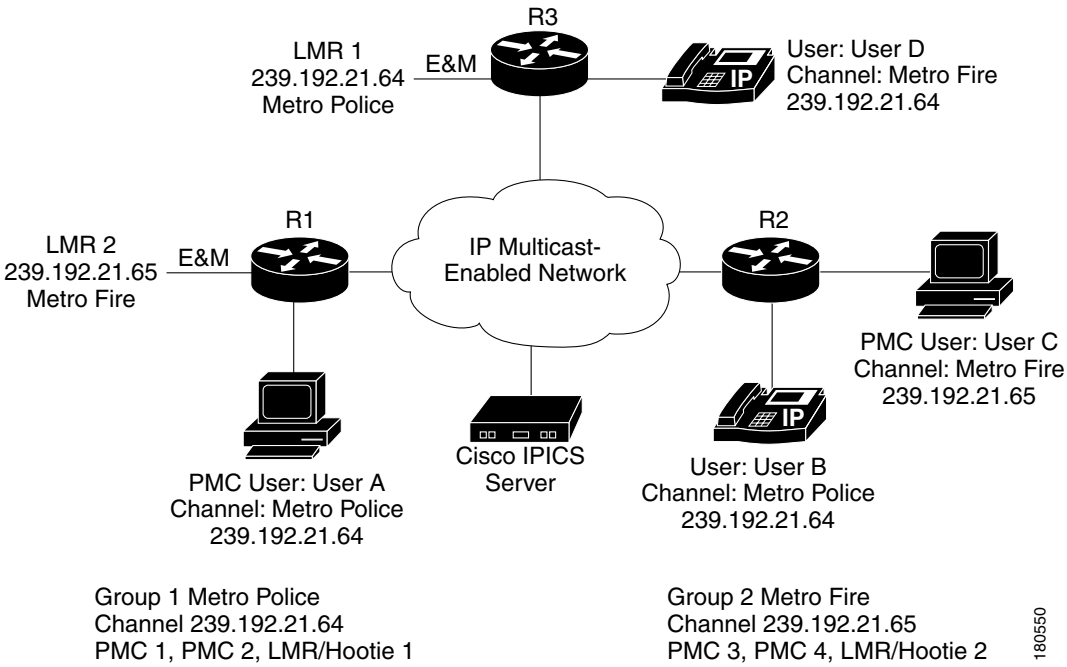
Adding an LMR gateway and an LMR user to this scenario does not necessarily require RMS DS0 resources. If the LMR user is statically configured to use the same channel as the other users, all users can communicate without consuming RMS DS0 resources, as shown in Figure 2-2.

Figure 2-2 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 2-3, 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 2-3 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 PMC users on the remote location), but it will 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 PMC 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.

When a PMC successfully authenticates using the remote location, the RMS allocates a DS0 pair to each channel or VTG that is assigned to that authenticated PMC user. (See the "Remote PMC Users" section on page 2-22 for related information.)

Table 2-1 describes when RMS resources are allocated in various scenarios.

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 PMC	No	1 per assigned channel or VTG

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 and/or ports (such as T1/E1) and the motherboard, but DSPs cannot be shared among analog ports (such as an FXS)).
- You should enable at least 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, refer to *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

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 (bearer) 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. This way, you can 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

Virtual Talk Groups

A virtual talk group (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
- Other VTGs

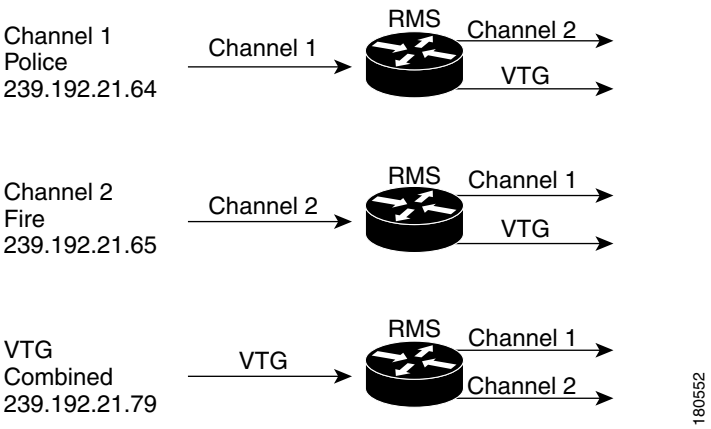
A Cisco IPICS administrator creates Cisco IPICS channels and assigns a multicast address to each one. A Cisco IPICS dispatcher creates VTGs as needed. When a dispatcher creates a VTG, the Cisco IPICS server automatically allocates to the VTG an available address from the multicast pool. So while VTGs 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, an RMS 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 dispatcher creates a VTG named “Combined” and that this VTG includes the Police channel and Fire channel as members. Also assume that each LMR voice port is statically configured with a multicast address, so that LMR police users always send to the Police channel, and LMR fire users always send to the Fire channel. To provide communication between the Police channel and the Fire channel, an RMS must bridge the multicast streams from these channels.

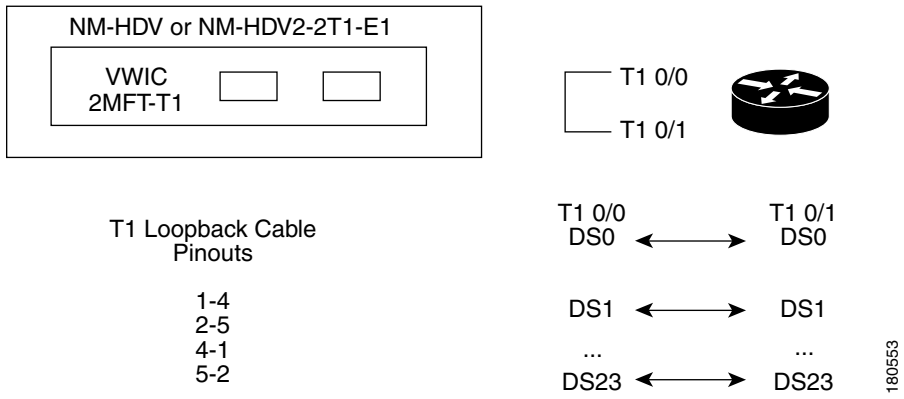
In this example, when a user talks on the Police channel (channel 1), the RMS router must bridge that multicast stream to the Fire channel (channel 2) and to the VTG channel. The RMS must perform similar operations when a user talks on channel 2 or on the VTG channel. See Figure 2-4.

Figure 2-4 VTG Channel Mixing



The RMS accomplishes this media mixing by using T1 or E1 interfaces, which are connected back to back with a T1 Loopback cable, as illustrated in Figure 2-5

Figure 2-5 RMS



In this scenario, the Cisco IPICS server automatically selects two DS0 pairs from the RMS router to use for mixing the channels. The Cisco IPICS server also configures associated voice ports and dial peers.

To continue this example, assume that Cisco IPICS selects timeslots 10 and 14 as shown:

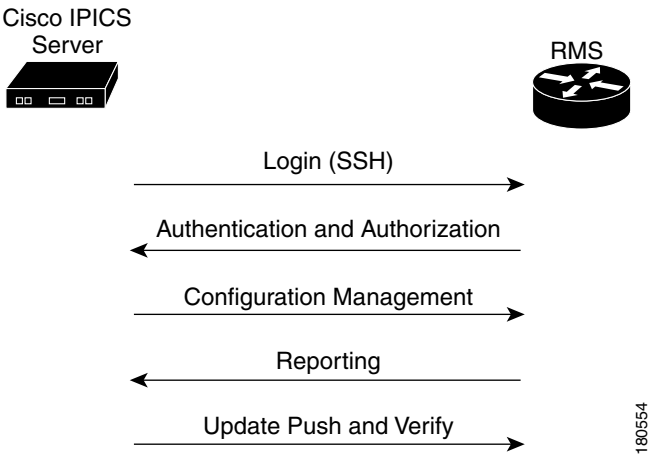
```
T1 0/0:10 --------------T1 0/1:10
VTG Combined             San Jose Police
239.192.21.79            239.192.21.64

T1 0/0:14 --------------T1 0/1:14
VTG Combined             San Jose Fire
239.192.21.79            239.192.21.65
```

Also assume that the Cisco IPICS dispatcher places the following users and channels into the Combined VTG channel:

- Channels:
  - Police
  - Fire
- Users:
  - User 1
  - User 2
  - User 3
  - User 4

When the dispatcher activates this VTG, Cisco IPICS uses the Cisco router to configure on the RMS the voice ports and dial peers that are associated with the selected T1 DS0s. See Figure 2-6 and the configuration example that follows this figure.

Figure 2-6 RMS Configuration and Management



The following example shows configurations for this scenario:

```
dial-peer voice 90929090 voip
 description #0/0:10#1152296144646# INUSE 16
 destination-pattern 90929090
 voice class permanent 1
 session protocol multicast
 session target ipv4:239.192.21.79:21000
 codec g711ulaw
 no vad
!
dial-peer voice 90929190 voip
 description #0/1:10#1152296144646# INUSE 16
 destination-pattern 90929190
 voice class permanent 1
 session protocol multicast
 session target ipv4:239.192.21.65:21000
 codec g711ulaw
 no vad
!
dial-peer voice 90929092 voip
 description #0/0:14#1152296144696# INUSE 18
 destination-pattern 90929092
 voice class permanent 1
 session protocol multicast
 session target ipv4:239.192.21.79:21000
 codec g711ulaw
 no vad
!
dial-peer voice 90929192 voip
 description #0/1:14#1152296144696# INUSE 18
 destination-pattern 90929192
 voice class permanent 1
 session protocol multicast
 session target ipv4:239.192.21.64:21000
 codec g711ulaw
 no vad
!
voice-port 0/0:10
 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
 timing hookflash-in 0
 timing hangover 40
 connection trunk 90929090
 description #0/0:10#1152296144646# INUSE 16
!
voice-port 0/0:14
 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 40
 connection trunk 90929092
 description #0/0:14#1152296144696# INUSE 18
!
voice-port 0/1:10
 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
 timing hookflash-in 0
 timing hangover 40
 connection trunk 90929190
 description #0/1:10#1152296144646# INUSE 16
 voice-port 0/1:14
!
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 40
 connection trunk 90929192
 description #0/1:14#1152296144696# INUSE 18
```

Channel Mixing in the RMS using the Cisco Hoot ‘n’ Holler Feature

The RMS uses the Cisco Hoot ‘n’ Holler feature to mix channels. Cisco Hoot 'n' Holler is a communications system in which the three most recent talkers are mixed into one multicast output stream. Also known as *hootie*, these networks provide “always on” multi-user conferences without requiring that users dial in to a conference.

For additional information about Cisco Hoot ‘n’ Holler, refer to the documentation at the following URLs:

- IOS Technology—

  http://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html
- IP Technology—

  http://www.cisco.com/en/US/tech/tk828/tsd_technology_support_protocol_home.html
- *Multicast Hoot ‘n’ Holler White Paper*—

  http://www.cisco.com/warp/public/cc/so/neso/vvda/hthllr/hhoip_wp.pdf

A virtual interface (VIF) is used to associate an IP address with the voice ports on the RMS. In the example shown in Figure 2-4 on page 2-10, the RMS joins channels Police (239.192.21.64), Fire (239.192.21.65), and the Combined VTG (239.192.21.79).

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 router, the IOS arbitration algorithm selects only the three most active voice streams and presents them to the router DSP for mixing. If other voice streams are present, the router drops the longest talker in by using a round-robin arbitration algorithm. See Figure 2-7.

Figure 2-7 Mixing Voice Streams

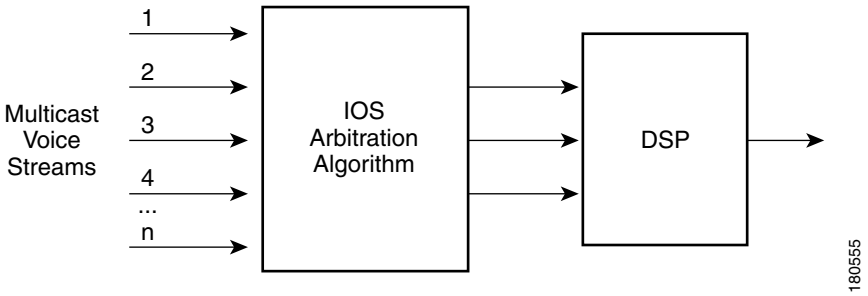


Table 2-2 shows an example of how mixing works in a VTG that has four active users on a channel.

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. IOS arbitration engine at each router receives 3 voice streams.
User D starts speaking while other three users continue speaking.	IOS arbitration engine at each router receives 4 voice streams. The algorithm can present up to 3 voice streams to the DSP. It drops the voice stream from the longest talker, User A, and adds User D to the streams that it presents. Voice streams in the DSP are now from User B, User C, and User D.

Table 2-2 Mixing Example

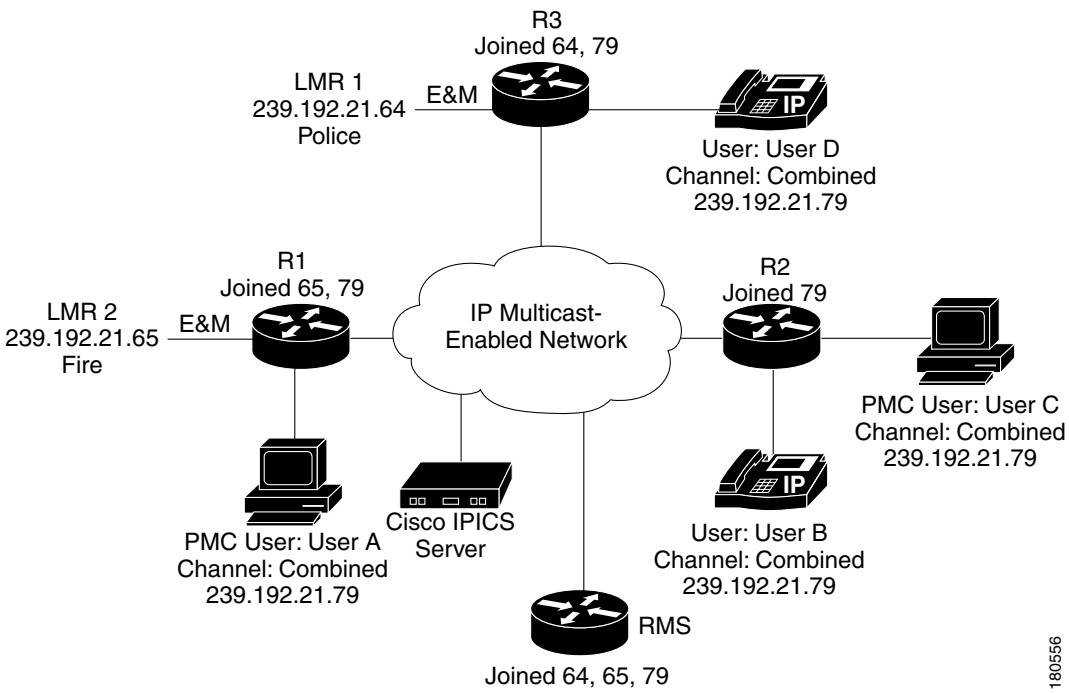
Event	Remarks
After 2 seconds, all 4 users are still speaking.	The current longest talker, User B, is dropped, and User A is added. Voice streams in the DSP are now User C, User D, and User A.
After 2 seconds, all 4 users are still speaking.	The current longest talker, User C, is dropped, and User A is added. Voice streams in the DSP 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.

Cisco IPICS Endpoint Scenarios

When a Cisco IPICS dispatcher activates the Combined VTG (as shown in Figure 2-3 on page 2-8), Cisco IPICS configures the RMS router to mix the Police, Fire, and Combined VTG channels. Users that have been added to the VTG see the new Combined VTG channel on their PMCs 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.

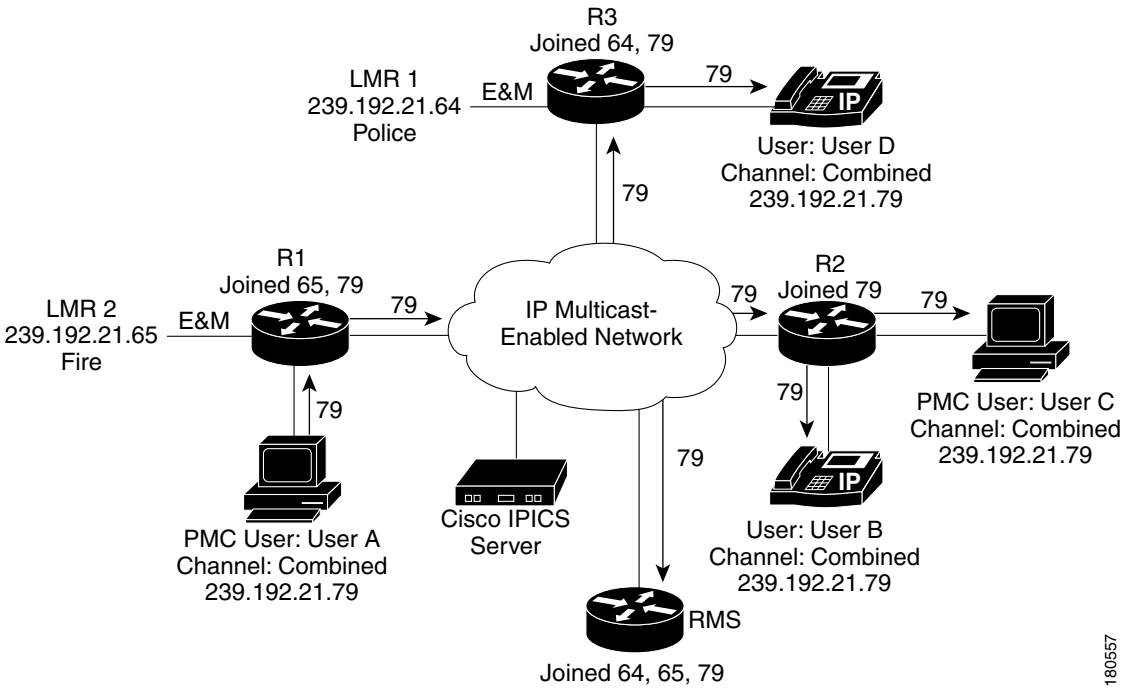
Figure 2-8 illustrates a scenario in which four users have deactivated their police or fire channels and have activated the Combined VTG channel.

Figure 2-8 Multicast Group Membership



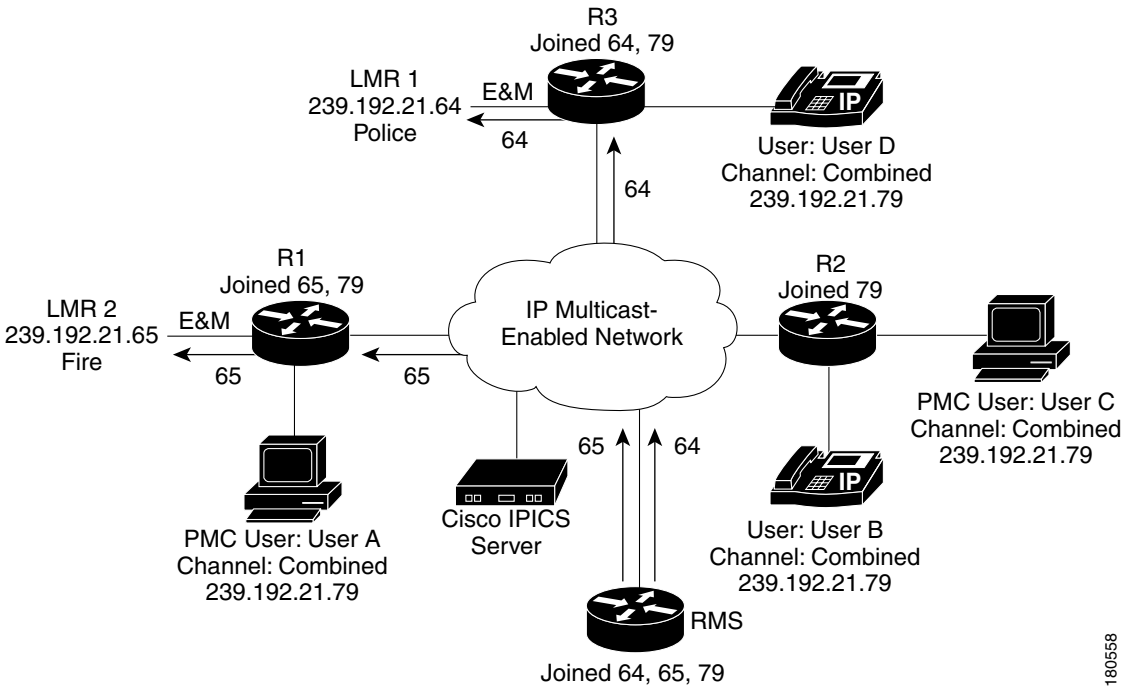
When a user deactivates the Police and or Fire channel and activates the Combined VTG channel, the endpoint sends an Internet Group Management Protocol (IGMP) leave message for the Police and or Fire Channel and an IGMP join message for the Combined VTG channel. The LMR voice port channels are statically configured and the VIF will have already joined the configured multicast group. As shown in Figure 2-9, 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 RMS, which mixes the audio and sends it to the channels in the VTG.

Figure 2-9 Transmitting to the VTG Channel



When the RMS router receives the traffic over the Combined VTG channel, it mixes this channel with the Police and Fire channels and forwards the mixed stream to the LMR endpoints, as shown in Figure 2-10.

Figure 2-10 Transmitting VTG Channel to Police and Fire Channels



When the LMR Police user transmits, the only other endpoint that has joined this multicast channel is the RMS router. The Multicast Distribution tree forwards the multicast voice traffic to the RMS, where it is mixed with the Fire channel and the Combined VTG channel and then forwarded to the other endpoints in the VTG. See Figure 2-11.

Figure 2-11 LMR Multicast Traffic Flow

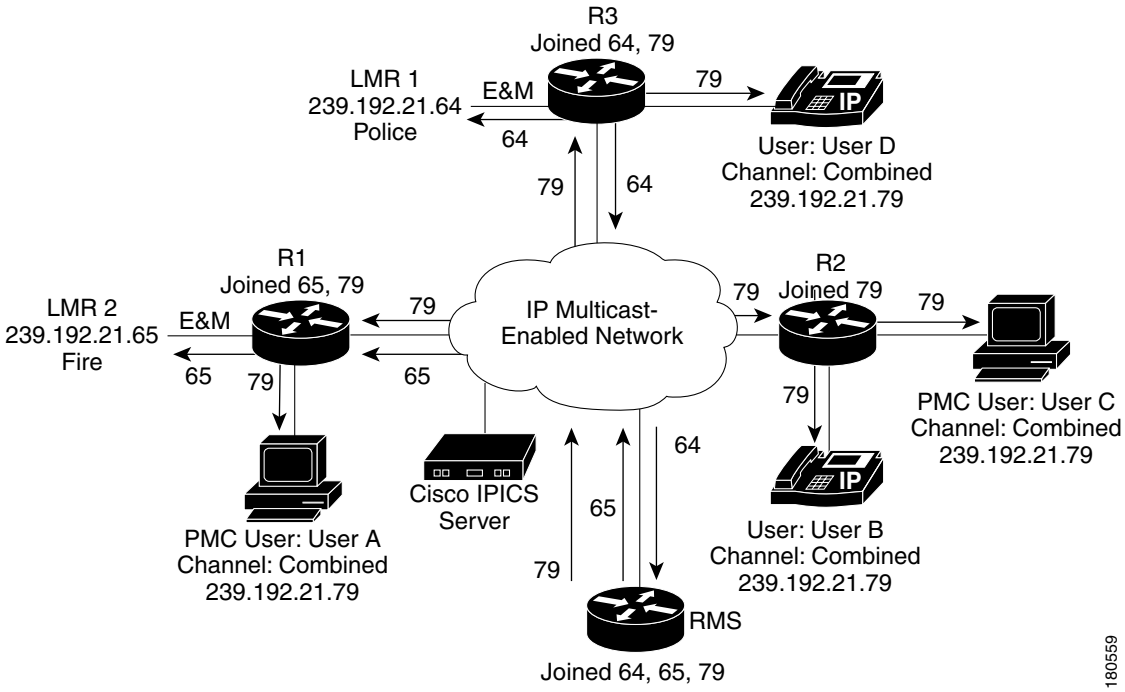
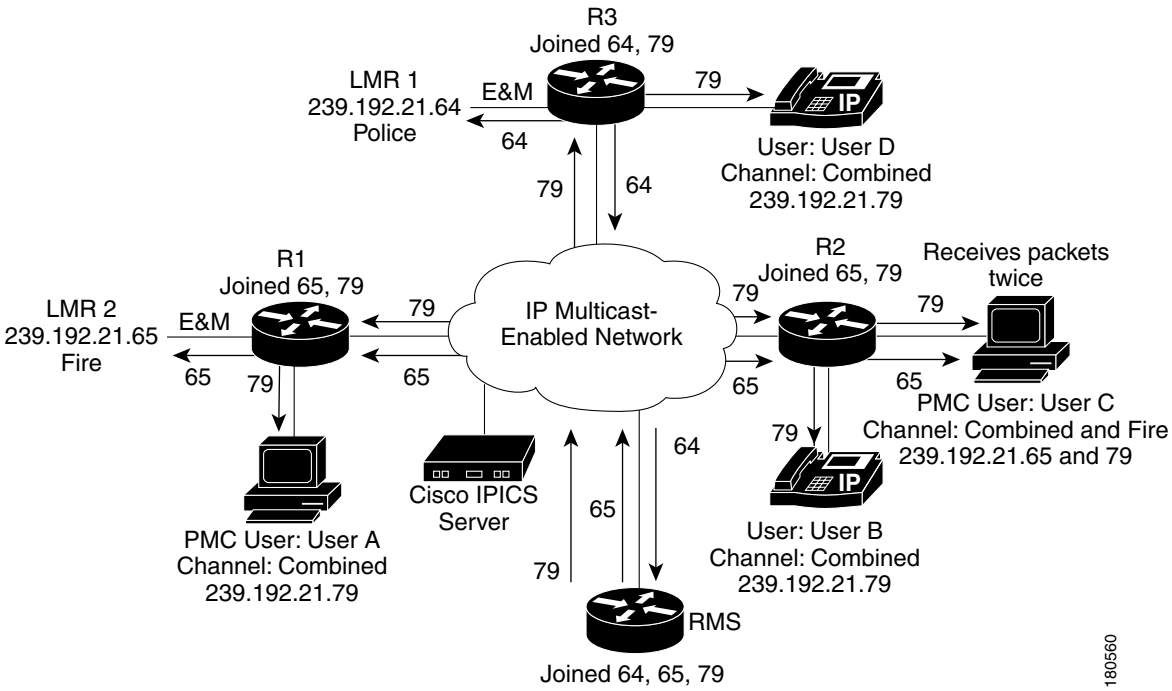


Figure 2-12 shows User C with two active channels: the Fire channel and the Combined VTG channel.

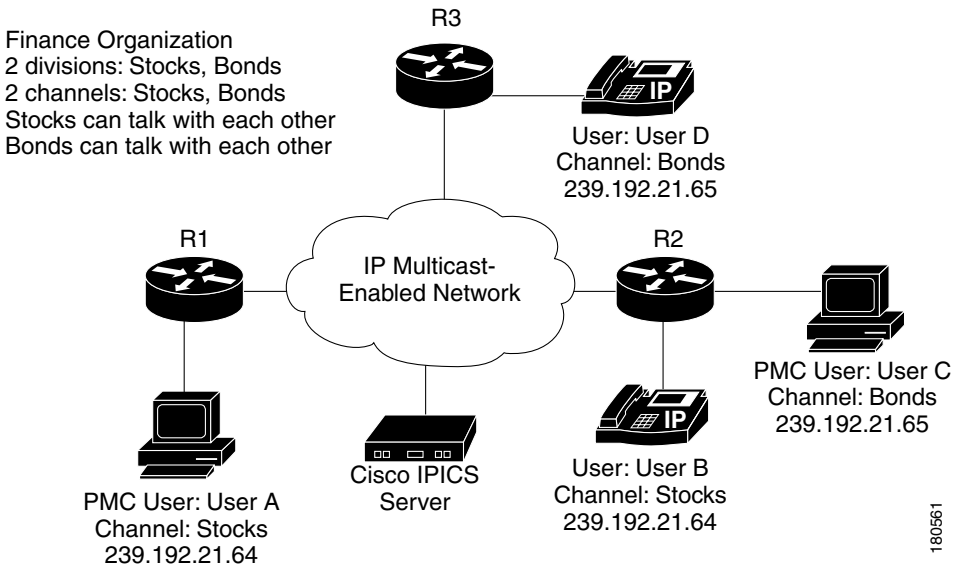
Figure 2-12 Traffic Flow with Two Active Channels



Because User C activated two channels (Fire 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 the case, the duplicate packets can cause audio quality issues. Take care to avoid this scenario.)

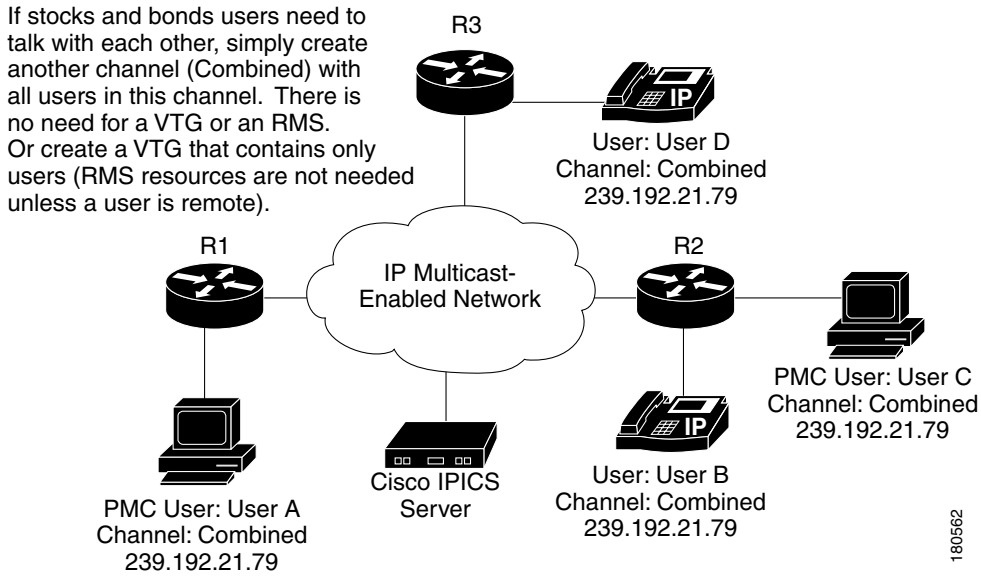
If there are no LMR endpoints in a VTG, RMS DS0 resources may not be required for the VTG. For example, consider a financial institution with one Cisco IPICS channel called Stocks and one channel called Bonds. The users that are associated with the Stocks channel can communicate with each other and the users that are associated with the Bonds channel can communicate with each other. Figure 2-13 illustrates this scenario.

Figure 2-13 Cisco IPICS Scenario with no LMR Endpoints



If a VTG is created that contains users but no channels, RMS DS0 resources are not required. The only resource that is required in this case is a multicast channel from the multicast pool. RMS DS0 resources are not needed because PMC and Cisco Unified IP Phone users, unlike LMR users, are not statically configured for one channel. If users only are placed in the VTG, users see the VTG on their PMCs or phones. When the VTG is activated, these endpoints will simply join the VTG multicast channel that is allocated by the Cisco IPICS server. See Figure 2-14.

Figure 2-14 VTG with Users Only



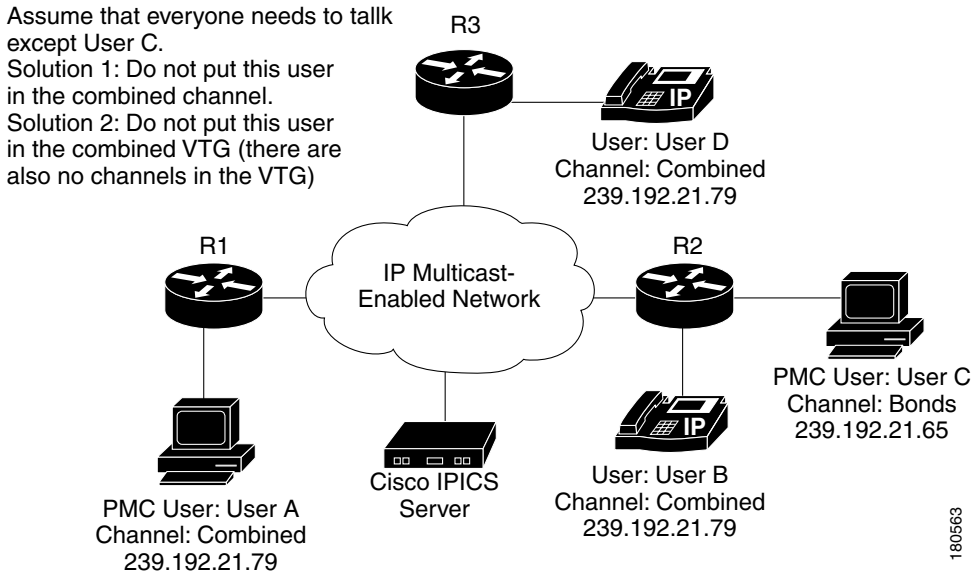
You can also avoid consuming RMS DS0 resources by creating a new channel and associating all users with that channel, instead of creating a VTG. In the example shown in Figure 2-14, there is a channel called Combined. Users see two channels on their PMCs or phones: the Combined VTG channel, and either 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

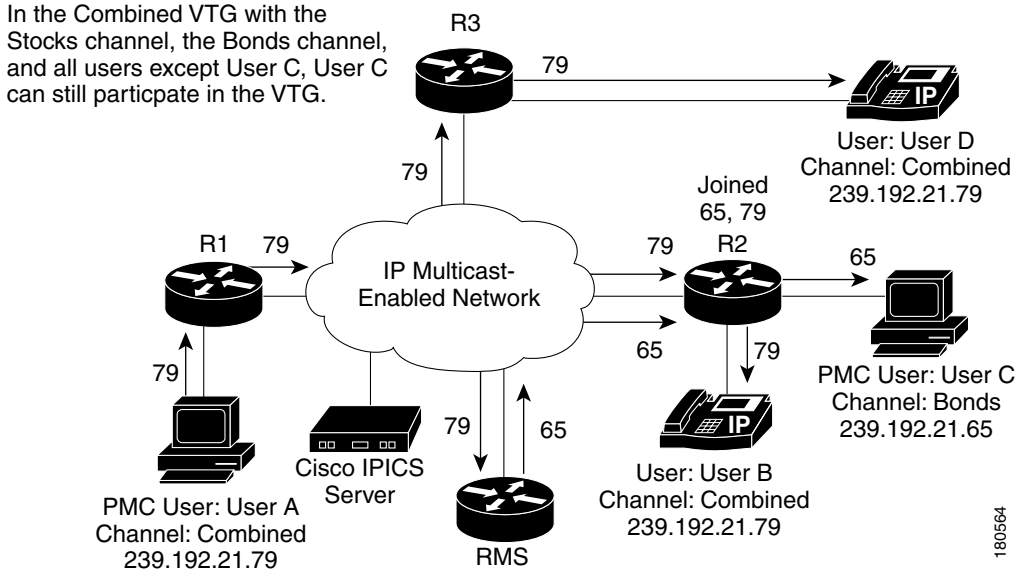
See Figure 2-15.

Figure 2-15 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 PMCs or 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 2-16.

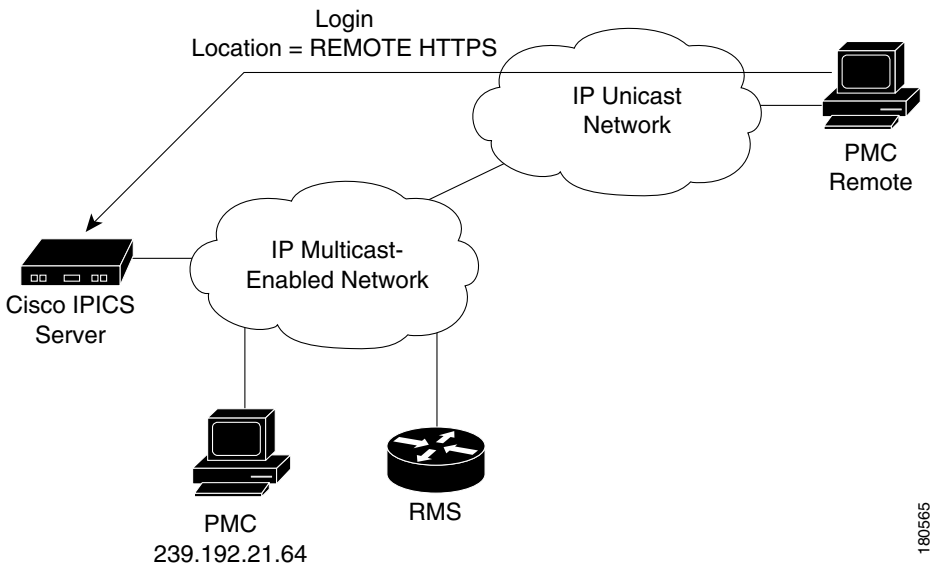
Figure 2-16 Combined VTG with a User Omitted



Remote PMC Users

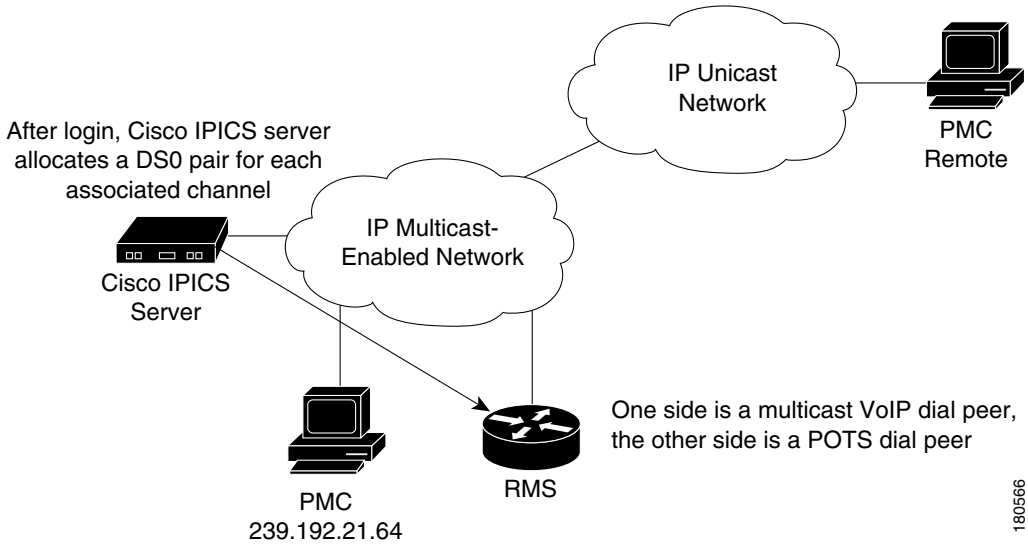
PMC users who are not connected to the Cisco IPICS multicast domain must choose the remote location when they log in to Cisco IPICS, as shown in Figure 2-17. A PMC user that is logged into Cisco IPICS in this way is sometimes called a *remote PMC user*. Examples of such users include those using a satellite connection or those connecting the network through a VPN.

Figure 2-17 Remote PMC User



A remote PMC user cannot connect to the Cisco IPICS domain using multicast. Instead, the remote PMC user connects to the RMS by using a SIP-based (unicast) connection. The RMS then mixes the unicast stream to a multicast stream for the channel that the remote PMC user activated. After the remote PMC user logs into Cisco IPICS, the Cisco IPICS server allocates a DS0 pair on the RMS for every channel that is associated with the user. See Figure 2-18.

Figure 2-18 Timeslot Allocation



Assume that the Cisco IPICS server allocates timeslot 20 for the remote PMC user. In this case, the Cisco IPICS server configures the voice ports and dial peers as follows:

Multicast Side—239.192.21.64

```
voice-port 0/0/0:20
 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
 timing hookflash-in 0
timing hangover 40
 connection trunk 909090920
 description #0/0/0:20#1123534375842# INUSE 92

dial-peer voice 909090920 voip
 description #0/0/0:20#1123534375842# INUSE 92
 destination-pattern 909090920
 voice class permanent 1
 session protocol multicast
 session target ipv4:239.192.21.64:21000
 codec g711ulaw
 no vad
```

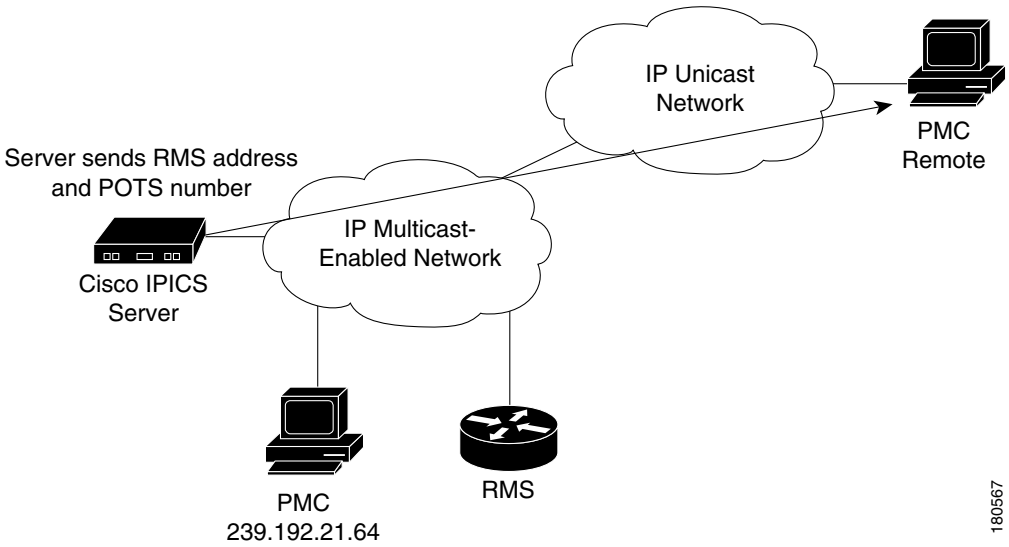
Unicast Side—239.192.21.64

```
voice-port 0/0/1:20
 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
 timing hookflash-in 0
```

```
 timing hangover 40
 description #0/0/1:20#1123534375842# INUSE 92

dial-peer voice 909091920 pots
 description #0/0/1:20#1123534375842# INUSE 92
 destination-pattern 8880000081909091920
 port 0/0/1:20
```

After the Cisco IPICS server configures the voice ports and the dial peers, it sends to the remote PMC user the IP address of the RMS and the Plain Old Telephone Service (POTS) number for the unicast connection. See Figure 2-19.

Figure 2-19 Providing RMS and POTS Number to Remote User



When a channel is activated by a remote PMC user, the remote PMC uses the SIP to set up the unicast call. After the SIP call is established, the remote PMC user can send to and receive from the Police channel.

For an example of this process, see the following figures:

- Figure 2-20, "Unicast Connection Set Up"
- Figure 2-21, "SIP Signaling Flow"
- Figure 2-22, "Unicast to Multicast Call Flow"
- Figure 2-23, "Multicast to Unicast Call Flow"

Figure 2-20 Unicast Connection Set Up

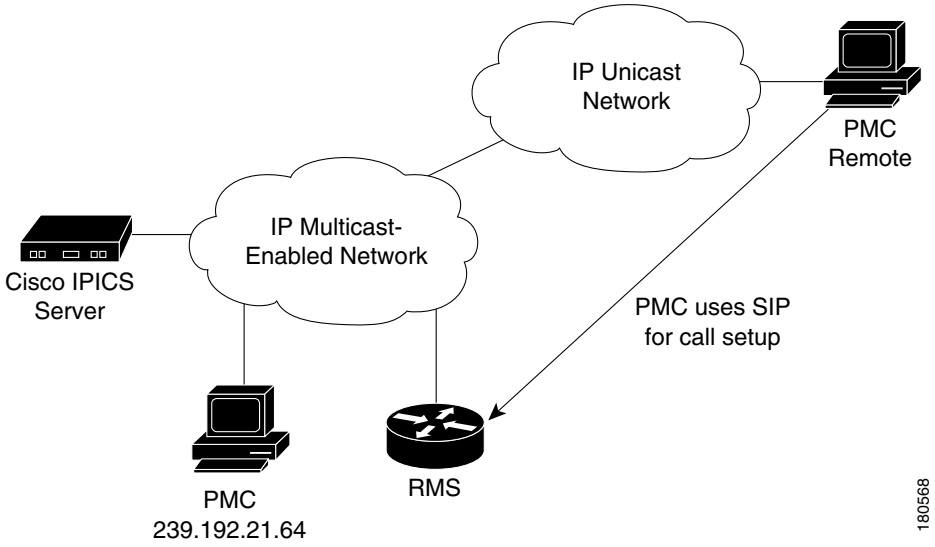


Figure 2-21 SIP Signaling Flow

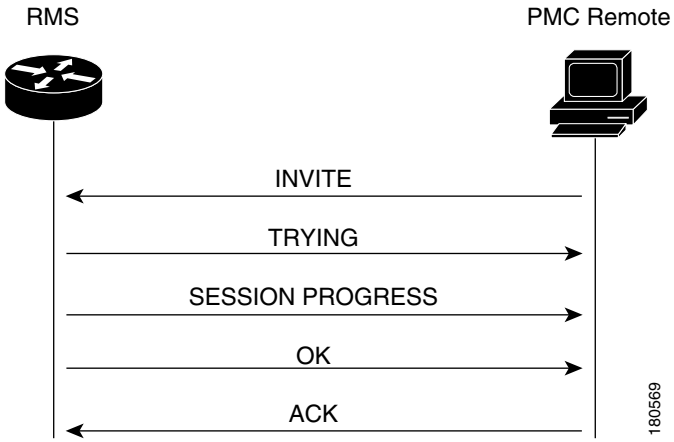


Figure 2-22 Unicast to Multicast Call Flow

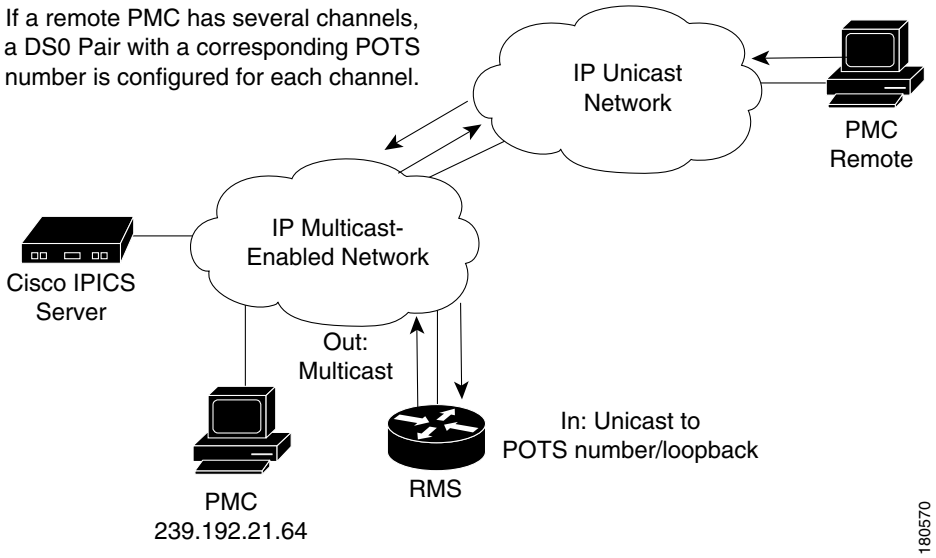
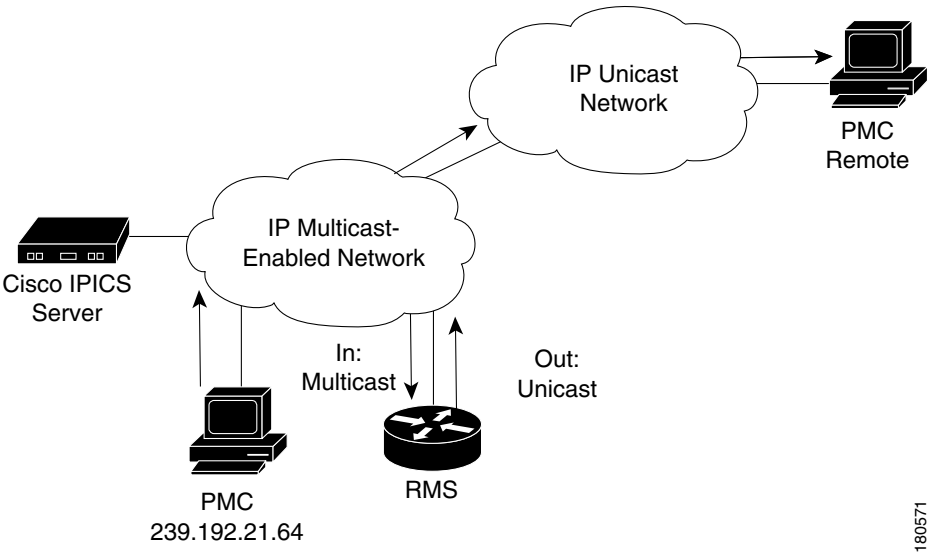


Figure 2-23 Multicast to Unicast Call Flow



When you add an RMS on the Cisco IPICS server, use the loopback address of the RMS router. If there are several paths to the RMS router and a physical interface is used, the RMS will be unreachable if the physical interface goes down or becomes unreachable. If the loopback address is used as the IP address when adding the RMS on the Cisco IPICS server, that server will push this IP address to the PMCs as the SIP proxy address.

Land Mobile Radio Gateway

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 additional information about LMRs, refer to the documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/lmrip/index.htm
.htm

Cisco Unified IP Phones

If your Cisco IPICS deployment includes Cisco Unified CallManager or Cisco CallManager 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 function similarly to a PMC, providing an easy-to-use GUI that allows users to monitor or participate in a PTT channels or VTG over a VoIP network. However, unlike a PMC, a phone can participate in only 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 is displayed on the phone.

A phone that is configured to work as a PTT device uses a stand-alone LMR PTT audio client. This Extensible Markup Language (XML) application enables the display of interactive content with text and graphics on the phone.

To enable this feature, Cisco Unified CallManager or Cisco CallManager Express must be deployed in your IP telephony (IPT) network, and either of these applications must be configured with the IP address of the Cisco IPICS server. A Cisco Unified IP Phone use this IP address to locate the server and download the PTT XML application.

For related information about configuring this feature, refer to the “Setting Up the Cisco IP Phone for use with Cisco IPICS” appendix in *Cisco IPICS Server Administration Guide*. For a list of Cisco Unified IP Phones that Cisco IPICS supports as PTT devices, refer to *Cisco IPICS Compatibility Matrix*. These documents are available at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cis/c_ipics/index.htm

Cisco Unified CallManager Configuration Overview

You use the Cisco IP Phone Services Configuration page in the Cisco Unified CallManager 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.

Figure 2-24 shows the Cisco IP Phone Services page.

Figure 2-24 Cisco IP Phone Services Configuration Page

After you configure a list of IP phone services, Cisco Unified IP Phone users can access the Cisco Unified CallManager 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 that users have one-button access to the services.

For detailed information about configuring phone services, refer to the "Cisco IP Phone Services" chapter in *Cisco Unified CallManager System Guide*, which is available at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/voice/c_callmg/

Cisco CallManager Express Configuration Overview

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

```
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
```

Cisco IPICS Infrastructure Considerations

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

To access related documentation, refer to the following URLs:

- IP multicast:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/himc_c/index.htm
- Quality of Service:

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124cg/hqos_c/index.htm
- Voice over IP (VoIP):

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcg/vcl.htm
- Hoot 'n' Holler:

  http://www.cisco.com/en/US/netsol/ns340/ns394/ns165/ns70/networking_solutions_package.html

This chapter includes these topics:

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 microseconds 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 using QoS features. For related information, see the"Quality of Service" section on page 3-8.
- 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 3-8.
- 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.
- PMCs using remote location—PMCs that choose the remote location use SIP to set up the connection to the RMS. Because SIP is sensitive to latency and excessive delays, this type of connection may experience timeouts and call setup failures. If you experience connectivity or audio quality issues when you use a PMC that is deployed over a WAN, try to isolate the problem by testing a remote PMC connection that is not deployed over a WAN. If you cannot duplicate the problem on the PMC that is not deployed over the WAN, Cisco recommends that you assess the WAN infrastructure to determine if excessive latency or resource limitations in the WAN are causing the problems.

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.

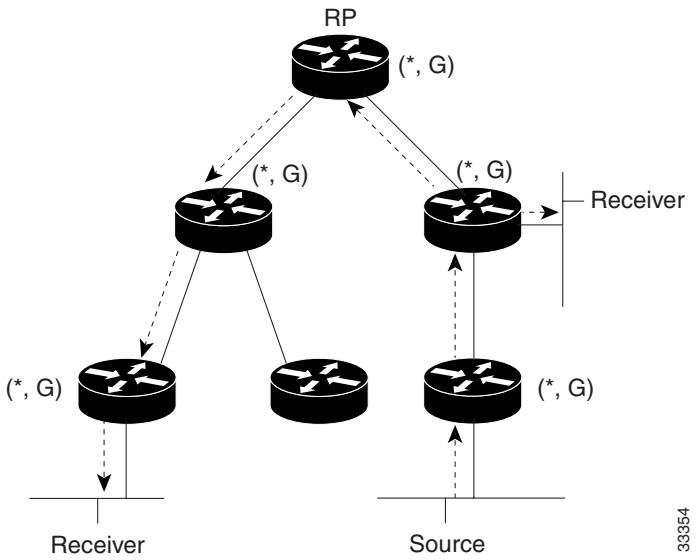
Cisco recommends using bidirectional PIM for Cisco IPICS. Bidirectional PIM is an extension of the PIM suite of protocols that implements shared sparse trees with bidirectional data flow. In contrast to PIM-sparse mode, bidirectional PIM avoids keeping source-specific states in a router and allows trees 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 that is rooted in that IP address. The IP address does not need to be a router. It can be any unassigned IP address on a network that can be reached throughout the PIM domain.

Figure 3-1 shows 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 3-1 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 provides 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. 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 eliminate 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.

Bandwidth Planning

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

- Codec used for VoIP—See the "Codecs" section on page 3-4
- The number of voice streams that will be mixed—See the "Mixing Voice Streams" section on page 3-8

In addition, you should 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 3-8.

Codecs

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

Choosing a Codec

When choosing a codec for Cisco IPICS, consider the issues that are described in Table 3-1.

Table 3-1 Codec Considerations

	G.711	G.729a
Delay	• Total delay is 25ms less per sample than for G.729a. • Transcoding increases delay.	• Total delay is 25ms greater per sample than for G.711. • Some Cisco IPICS deployments that use G.729a require additional transcoding to convert the G.729a streams to G.711 stream for mixing. This additional DSP function increases delay significantly.
Voice Quality	• Assuming that good VoIP conditions exist, delivers a MOS of 4.1 with a high degree of consistency. • Does tandem well, so no voice quality degradation results from transcoding.	• 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. • 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 then a similar packet loss rate under G.711. • Does not tandem as well as G.711. • Transcoding decreases voice quality from a MOS of 3.7 to 3.2.
Bandwidth	• Typically consumes 3 times more bandwidth than G.729a.	• Offers bandwidth savings over G.711. • A Cisco IPICS deployment that connects sites via a WAN may use G.729a to reduce WAN bandwidth, which also may reduce WAN costs.

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 packets includes an IP, UDP, and Real-time Transport Protocol (RTP) header, which adds 40 bytes to the packet. Layer 2 headers (such as Frame Relay, Point-to-Point Protocol, 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 (8K CS-ACELP)

50 packets/second

20ms 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 (64K PCM)

50 packets/second

20ms 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 3-2 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 3-2 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 RMS resources are not used. When remote users connect over a WAN that is not multicast enabled, the RMS converts a multicast stream to an IP unicast stream, which conserves bandwidth on the WAN. When the IP unicast voice stream arrives at the RMO, the RMS converts the IP unicast stream to an multicast stream. When the voice streams traverse a WAN, the RMS resources are used. In this scenario the RMS gateways are configured for M1:U12:M2 unicast connection trunks. For additional information, see the "M1:U12:M2 Connection Trunks" section on page 5-13.

As an example of the bandwidth affect of PMCs that are deployed across a WAN, assume that 40 PMC users are communicating over a WAN. Although each multicast voice stream is converted to an IP unicast voice stream so that it can traverse as a IP unicast stream, this scenario could still require substantial bandwidth, depending on the number of channels and the codec type that is used by each PMC. In this example, the bandwidth requirements are as follows:

G.729a

40 PMC Users x 8 Channels per User x (24 kbps + 3.6kbps) = 8.832 kbps

G.711

40 PMC Users x 8 Channels per User x (80 kbps + 12 kbps) = 29,440 kbps

cRTP, Variable-Payload Sizes and Aggressive VAD

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

- RTP Header Compression, page 3-6
- Adjustable Byte Size of the Voice Payload, page 3-7
- Aggressive Voice Activity Detection, page 3-7

RTP Header Compression

As described in the "Codecs" section on page 3-4, 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, refer to *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

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. You can calculate the number of packets that are sent per second as shown in these examples:

G.729a codec, with default 20byte payload/packet

Codec rate: 8,000 bits/second * 8 bits = 1,000 byes/second

Sampling interval: 10 ms

Default payload size: 20 bytes/packet (2 samples/packet)

1,000 bytes/sec/20bytes/pkt = 50 packets/sec

G.729a codec, with 40 bytes defined in VoIP dial-peer

Codec rate: 8,000 bits/second * 8 bits = 1,000 byes/second

Sampling interval: 10 ms

Payload size: 40 bytes/packet

1,000 bytes/sec/40 bytes/pkt = 25 packets/sec

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 digital signal processor (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 by up to 50%.

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 Squelch (COS). 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 burst 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 handle 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 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 2-10, the DSPs in a Cisco IPICS deployment can mix up to three voice streams. However, the DSPs do not perform a summation function. For example, if three G.729a streams (24K each with headers) are received by a router or gateway, the mixed stream would consume 72K 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 K stream.

It is important to consider this issue when you plan bandwidth in a Cisco IPICS network. It is especially important when planning WAN bandwidth, which can be more expensive and less available then 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 VoIP QoS. This section provides an overview of these feature for Point-to-Point Protocol (PPP) and Frame Relay WAN topologies and for deployments on LAN media.

This section includes these topics:

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 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 packet. 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 re 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 network 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.

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 3-10
- Low Latency Queuing, page 3-10

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

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr

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 use 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-list102 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 with Frame Relay

If you deploy Cisco IPICS in a Frame Relay network, be aware that Frame Relay does not inherently provide QoS. Frame Relay is a best-effort service that expects upper-layer applications to handle retransmissions that occur because of packet loss in the Frame Relay cloud.

Frame Relay typically provides the following parameters:

- Committed Information Rate (CIR)—Amount of bandwidth that the Frame Relay carrier guarantees to be available at all times for a particular PVC. The carrier does not make any guarantees for packets sent above CIR.
- Burst—Maximum amount of data that the Frame Relay carrier allows to be sent on a particular PVC.

To offer the QoS over Frame service, carriers use a technique called *over-provisioning bandwidth*, in which they sell more bandwidth then they can provide at a particular time. This technique works because not all Frame Relay customers require all available bandwidth at one time.

Some Frame Relay carriers also guarantee a Frame Relay network that is always available and that will not drop any customer packets.

A Frame Relay carrier employs a variety of methods to offer a CIR + Burst service, including the following:

- Marking packets with discard eligible (DE) or dropping the packets—Because real-time applications such as VoIP use UDP for transport, there is no mechanism for packets to be retransmitted. This situation is not a problem for VoIP because users would not want to hear a dropped word later in a sentence. Packet loss is generally not acceptable for real-time VoIP applications because it can result in choppy audio and garbled speech.
- Buffering all packets above the CIR—Eliminates lost packets, but can introduce jitter and delay because of the depth or rate at which the Frame Relay switches empty buffers.

Table 3-3 summarizes key recommendations when deploying Cisco IPICS on a network with Frame Relay.

Table 3-3 Recommendations when Deploying Cisco IPICS with Frame Relay

Recommendation	Technique	Comments
To avoid introducing packet loss or jitter into a Cisco IPICS network, make sure that traffic that exceeds the CIR is not sent into a Frame Relay network.	Use the IOS Frame Relay Traffic Shaping (FRTS) feature.	Allows a router to police traffic on a per-PVC basis so that it does not send any traffic above the CIR.
In a Frame Relay environment, make sure that packets that are sent across a WAN link do not exceed the Committed Information Rate (CIR)	Enable the FRF.12 feature in the Frame network.	FRF.12 is a Frame-Relay-Forum Implementation Agreement that specifies how to fragment and reassemble packets on a Frame Relay network at Layer 2 of the OSI model. By fragmenting large data packets, the smaller Cisco IPICS packets will not be delayed or subject to serialization, which helps to eliminate delay and jitter of the Cisco IPICS packets. Because the fragmentation and reassembly is done at Layer 2 of the OSI model, it does not adversely effect any upper-layer protocols (such as IPX or Appletalk or IP with DNF bits set) that do not handle fragmentation.
Implement a queuing technique that provides strict priority to Cisco IPICS packets.	Use a technique such as Low-Latency Queuing (LLQ)	The LLQ feature brings strict priority queuing to the Class-Based Weighted Fair Queuing (CBWFQ) method. Strict priority queuing allows delay-sensitive data such as voice to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic.

Example

Consider a Cisco IPICS Frame Relay network with the following characteristics:

- Three routers connected through 64 K Frame Relay PVCs in a hub and spoke topology, with Router-1 being the hub.
- All routers configured to traffic-shape their data and voice on the WAN to CIR, and all routers using IP RTP Priority to guarantee QoS for the Cisco IPICS packets.
- Frame Relay broadcast-queue enabled on the serial interfaces.
- One Cisco IPICS Channel configured.

Because the broadcast queue is only 40 packets deep by default and Cisco IPICS components (PMC, Cisco Unified IP Phone, RMS) transmits packets at 50 packets/second, the broadcast-queue must be set to prevent voice packets from dropping and to maintain voice quality. The recommended setting for the broadcast-queue is 64 8000 25 (64 queue size, 8,000 bytes per second (64,000 bps), and 25 packets per second).

Frame Relay Broadcast Queue

Broadcast queue is a feature that is used in medium and large IP or IPX networks where routing and service access point (SAP) broadcasts must flow across a Frame Relay network. The broadcast queue is managed independently of the normal interface queue, has its own buffers, and has a configurable size and data rate.

To enable broadcast queue, use this interface command:

frame-relay *broadcast-queue size byte-rate packet-rate*

A broadcast queue is given a maximum transmission rate (throughput) limit, which is measured in bytes per second and packets per second. The queue is serviced to ensure that only this maximum rate is provided. Because the broadcast queue has priority when transmitting at a rate below the configured maximum, it has a guaranteed minimum bandwidth allocation. The two transmission rate limits are intended to avoid flooding the interface with broadcasts. The actual limit in any second is the first rate limit that is reached. Given the transmission rate restriction, additional buffering is required to store broadcast packets.

The broadcast queue can be configured to store a large number of broadcast packets. You should set the queue size to a value that avoids loss of broadcast routing update packets. The exact size depends on the protocol being used and the number of packets required for each update. To be safe, the queue size should be set so that one complete routing update from each protocol and for each data-link connection identifier (DLCI) can be stored. As a general rule, start with 20 packets per DLCI. The byte rate should be less than both of the following:

- *n*/4 times the minimum remote access rate (measured in bytes per second), where *n* is the number of DLCIs to which the broadcast must be replicated
- 1/4 the local access rate (measured in bytes per second)

The packet rate is not critical if the byte rate is set conservatively. In general, the packet rate should be set assuming 250-byte packets. The frame-relay broadcast-queue command defaults are as follows:

- Size—64 packets
- Byte-rate—256000 bytes per second
- Packet-rate—36 packets per second

The following configuration is an example of a Frame Relay connection with an ear and mouth (E&M) port:

```
Router-1 (Hub Router)

hostname FR-1
!
ip multicast-routing
!
voice class permanent 1
 signal timing oos timeout disabled
 signal keepalive disabled
 signal sequence oos no-action
!
interface Vif1
ip address 1.1.1.1 255.255.255.0
ip pim sparse-dense-mode
!
router rip
network 1.1.1.0
network 5.5.5.0
network 5.5.6.0
!
```

```
interface Serial0/0
no frame-relay broadcast-queue
encapsulation frame-relay
frame-relay traffic-shaping
frame-relay broadcast-queue 64 8000 250
!
interface Serial0/0.1 point-to-point
ip address 5.5.5.1 255.255.255.0
ip pim sparse-dense-mode
frame-relay class ipics
frame-relay interface-dlci 100
frame-relay ip rtp header-compression
!
interface Serial0/0.1 point-to-point
ip address 5.5.6.1 255.255.255.0
ip pim sparse-dense-mode
frame-relay class ipics
frame-relay interface-dlci 100
frame-relay ip rtp header-compression
!
map-class frame-relay ipics
frame-relay cir 128000
frame-relay bc 1280
frame-relay mincir 128000
no frame-relay adaptive-shaping
frame-relay fair-queue
frame-relay fragment 160
frame-relay ip rtp priority 16384 16384 128
!
voice-port 1/0/0
 connection trunk 111
 operation 4-wire
!
dial-peer voice 1 voip
 destination-pattern 111
 voice class permanent 1
 session protocol multicast
 session target ipv4:239.111.0.0:21000
 ip precedence 5
!

Router-2 (Spoke Router)

hostname FR-2
!
ip multicast-routing
!
voice class permanent 1
 signal timing oos timeout disabled
 signal keepalive disabled
 signal sequence oos no-action
!
interface Vif1
ip address 1.1.2.1 255.255.255.0
ip pim sparse-dense-mode
!
router rip
network 1.1.2.0
network 5.5.5.0
!
interface Serial0/0
no frame-relay broadcast-queue
encapsulation frame-relay
frame-relay traffic-shaping
```

```
frame-relay broadcast-queue 64 8000 250
!
interface Serial0/0.1 point-to-point
ip address 5.5.5.2 255.255.255.0
ip pim sparse-dense-mode
frame-relay class ipics
frame-relay interface-dlci 100
frame-relay ip rtp header-compression
!
map-class frame-relay ipics
frame-relay cir 128000
frame-relay bc 1280
frame-relay mincir 128000
no frame-relay adaptive-shaping
frame-relay fair-queue
frame-relay fragment 160
frame-relay ip rtp priority 16384 16384 128
!
voice-port 1/0/0
 connection trunk 111
 operation 4-wire
!
dial-peer voice 1 voip
 destination-pattern 111
 voice class permanent 1
 session protocol multicast
 session target ipv4:239.111.0.0:21000
 ip precedence 5
!

Router-3 (Spoke Router)

hostname FR-3
!
ip multicast-routing
!
voice class permanent 1
 signal timing oos timeout disabled
 signal keepalive disabled
 signal sequence oos no-action
!
interface Vif1
ip address 1.1.3.1 255.255.255.0
ip pim sparse-dense-mode
!
router rip
network 1.1.3.0
network 5.5.6.0
!
interface Serial0/0
no frame-relay broadcast-queue
encapsulation frame-relay
frame-relay traffic-shaping
frame-relay broadcast-queue 64 8000 250
!
interface Serial0/0.1 point-to-point
ip address 5.5.6.2 255.255.255.0
ip pim sparse-dense-mode
frame-relay class ipics
frame-relay interface-dlci 100
frame-relay ip rtp header-compression
!
map-class frame-relay ipics
frame-relay cir 128000
```

```
frame-relay bc 1280
frame-relay mincir 128000
no frame-relay adaptive-shaping
frame-relay fair-queue
frame-relay fragment 160
frame-relay ip rtp priority 16384 16384 128
!
voice-port 1/0/0
!connection trunk 111
!operation 4-wire
!
dial-peer voice 1 voip
!destination-pattern 111
!voice class permanent 1
!session protocol multicast
!session target ipv4:239.111.0.0:21000
!ip precedence 5
!
end
```

Configuration with Bidirectional PIM Multicast

Bidirectional PIM multicast is preferred over unidirectional multicast when two PVCs, one dedicated to channel traffic and the other to data traffic, are used. It helps to reduce the number of ip mroute entries that are needed in the router to route multicast traffic. Bidirectional PIM requires one router in the network to act as the rendezvous point (RP).

In the following configuration example, the RP is the loopback interface of Router-1. (The RP can be any interface on any router in the network, as long as it is reachable.)

```
Router-1 (RP node)

hostname bidir-rp
!
ip multicast-routing
!
voice class permanent 1
 signal timing oos timeout disabled
 signal keepalive disabled
 signal sequence oos no-action
!
voice class permanent 2
 signal timing oos timeout disabled
 signal keepalive disabled
 signal sequence oos no-action]
!
interface Loopback1
ip address 10.10.2.1 255.255.255.0
ip pim sparse-mode
!
interface Vif1
ip address 10.1.2.1 255.255.255.0
ip pim sparse-mode
load-interval 30
!
router rip
network 10.1.2.0
network 10.100.0.0
network 10.101.0.0
!
interface Serial0/0
no ip address
```

```
encapsulation frame-relay IETF
load-interval 30
no fair-queue
frame-relay traffic-shaping
frame-relay lmi-type cisco
!
interface Serial0/0.1 point-to-point
description channel pvc
bandwidth 256
ip address 10.100.100.1 255.255.255.0
ip pim sparse-mode
frame-relay interface-dlci 100
class channel
!
interface Serial0/0.2 point-to-point
description data pvc
ip address 10.101.101.1 255.255.255.0
frame-relay interface-dlci 200
class data
!
ip classless
ip pim bidir-enable
ip pim rp-address 10.10.2.1 10 override bidir
!
map-class frame-relay channel
frame-relay cir 128000
frame-relay bc 1000
frame-relay be 0
no frame-relay adaptive-shaping
!
map-class frame-relay data
frame-relay cir 768000
frame-relay mincir 128000
frame-relay adaptive-shaping becn
!
voice-port 1/0/0
 voice class permanent 1
 timeouts wait-release 3
 timing dialout-delay 70
 connection trunk 111
 operation 4-wire
 signal lmr
!
dial-peer voice 1 voip
destination-pattern 111
session protocol multicast
session target ipv4:239.111.0.0:21000
ip precedence 5
!
end

Router-2 (non-RP node)

hostname bidir-2
!
ip multicast-routing
!
voice class permanent 1
 signal timing oos timeout disabled
 signal keepalive disabled
 signal sequence oos no-action
!
voice class permanent 2
 signal timing oos timeout disabled
```

```
 signal keepalive disabled
 signal sequence oos no-action
!
interface Loopback1
ip address 10.10.3.1 255.255.255.0
ip pim sparse-mode
!
interface Vif1
ip address 10.1.3.1 255.255.255.0
ip pim sparse-mode
load-interval 30
!
router rip
network 10.1.3.0
network 10.100.0.0
network 10.101.0.0
!
interface Serial0/0
no ip address
encapsulation frame-relay IETF
load-interval 30
no fair-queue
frame-relay traffic-shaping
frame-relay lmi-type cisco
!
interface Serial0/0.1 point-to-point
description channel pvc
bandwidth 256
ip address 10.100.100.2 255.255.255.0
ip pim sparse-mode
frame-relay interface-dlci 100
class channel
!
interface Serial0/0.2 point-to-point
description data pvc
ip address 10.101.101.2 255.255.255.0
frame-relay interface-dlci 200
class data
!
ip classless
ip route 10.10.2.1 255.255.255.255 Serial0/0.1
ip pim bidir-enable
ip pim rp-address 10.10.2.1 10 bidir
!
map-class frame-relay channel
frame-relay cir 128000
frame-relay bc 1000
frame-relay be 0
no frame-relay adaptive-shaping
!
map-class frame-relay data
frame-relay cir 768000
frame-relay mincir 128000
frame-relay adaptive-shaping becn
!
voice-port 1/0/0
 voice class permanent 1
 playout-delay nominal 100
 playout-delay minimum high
 playout-delay mode adaptive
 playout-delay maximum 250
 timeouts wait-release 3
 timing dialout-delay 70
 connection trunk 111
```

```
 operation 4-wire
 signal lmr
!
dial-peer voice 1 voip
 destination-pattern 111
 session protocol multicast
 session target ipv4:239.111.0.0:21000
 ip precedence 5
```

QoS with Point-to-Point Connections

This section provides information for WANs that have point-to-point connections that include any of these encapsulations:

- Point-to-Point Protocol (PPP)
- Multilink Point-to-Point Protocol (MLPPP)
- High-Level Data Link Control (HDLC)

Guaranteed bandwidth is not an issue on point-to-point (or leased) lines, but you do need to consider connection speed and queuing in these situations. As described in the "QoS with Frame Relay" section on page 3-11, links below 768 K require that larger data packets be fragmented to avoid serialization. In addition, you should use a queuing technique that provides strict priority to Cisco IPICS packets, such as IP RTP Priority, or Low-Latency Queuing.

The FRF.12 fragmentation and reassembly technique that is discussed in the "QoS with Frame Relay" section on page 3-11 does not apply to point-to-point links. For point-to-point links below 768 K, use Multilink PPP (MLPPP) for encapsulation. MLPPP provides feature called Link Fragmentation and Interleaving (LFI). LFI is similar in operation to FRF.12 in that it handles fragmentation at Layer 2.

LFI is not required for networks with link speeds above 768 K because 1,500 bytes packet do not cause more than approximately 10 ms of transport delay. This delay should be acceptable for most delay budgets, so for these networks, HDLC or PPP encapsulation are acceptable.

The following example shows configuring MLPPP with LFI:

```
interface Serial0
bandwidth 64
no ip address
no ip directed-broadcast
encapsulation ppp
no ip route-cache
no ip mroute-cache
no fair-queue
ppp multilink
multilink-group 1
!
interface Multilink 1
ip address 10.1.1.1 255.255.255.252
no ip directed-broadcast
no ip route-cache
ip rtp header-compression iphc-format
ip tcp header-compression iphc-format
no ip mroute-cache
fair-queue 64 256 1000
ppp multilink
ppp multilink fragment-delay 10
ppp multilink interleave
multilink-group 1
ip rtp priority 16384 16383 30
```

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 Catalyst switch for PMCs or 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 (Fibs) to ensure interoperation and provide for future expansion. These standards include:
  - RFC 2474 Class Selector Codepoints
  - RFC 2597 Assured Forwarding Classes
  - RFC 3246 Expedited Forwarding

Note Because SIP-based PMCs are in the data VLAN instead of in the voice VLAN, Cisco IPICS automatically pushes QoS configuration for PMCs to the RMS.

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 Catalyst switches (when supported)
- If the combined WAN circuit-rate is significantly below 100 Mbps and the Catalyst 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 theses recommendations.

- Police traffic flows 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.
- Cisco Catalyst platforms do not support DSCP-Based WRED. Scavenger-class remarking is a viable alternative.
- 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. 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, refer to *Cisco Unified Communications SRND Based on Cisco Unified CallManager 4.x*, which is available at this URL:

http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guide_book09186a00806e8a79.htmlf

A trust boundary can include PMCs (local and remote), LMRs, and Cisco Unified IP Phones. IP precedence should be marked for PMCs and 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
!
```

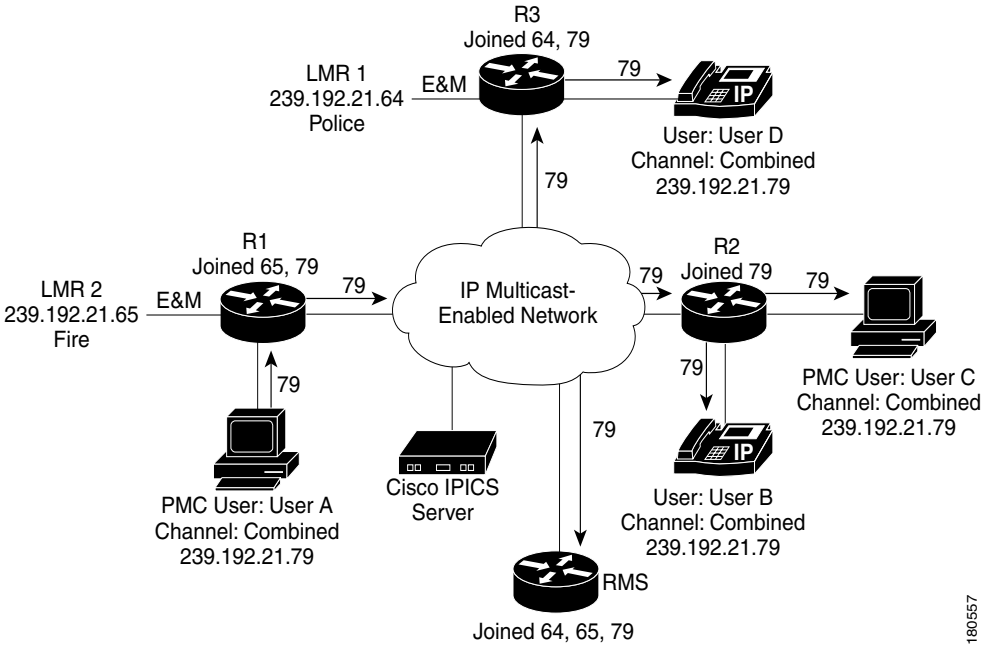
For a PMC using the remote location, an RMS marks the IP precedence value of 5. The Cisco IPICS server provides the QoS and other necessary configurations to the RMS server for the PMC.

Cisco IPICS traffic that comes from a PMC, 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 through out the network.

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 3-2 shows a trust boundary.

Figure 3-2 Trust Boundary



The following example shows access layer QoS configuration for a Cisco Catalyst 3550:

```
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 or IPICS Engineering team might have some recommendations)
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
```

```
Modified this list since the multicast addresses recommend above are incorrect. Just need
the last entry, unless also using GLOP then keep 233
! 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 PMC clients SIP signaling
CAT3550(config-ext-nacl)# permit udp <RMS IP Address> <Any > eq 5060
! <Any> is the address on Remote PMC SIP Client
CAT3550(config-ext-nacl)#end
CAT3550#
```

Port Utilization

This section describes the ports that can be used in a Cisco IPICS deployment. You can use this information to determine how best to define the QOS or firewall settings at a port level, if required. Information about how to facilitate modifications to the port ranges are included.

Table 3-4 describes the default ports that are used by Cisco IPICS components.

Table 3-4 Default Ports used by Cisco IPICS Components

Protocol	Device	Destination Port	Remote Device
HTTP	PMC	TCP 80	Cisco IPICS server
	Cisco IPICS Administration Console	TCP 80	Cisco IPICS server
	Cisco Unified IP Phone	TCP 80	Cisco Unified CallManager, Cisco Unified CallManager Express
HTTPS	PMC	TCP 443	Cisco IPICS server
	Cisco IPICS Administration Console	TCP 443	Cisco IPICS server
SIP	PMC / Policy Engine	UDP 5060	RMS / Policy Engine SIP provider **Note** Used for remote PMC to RMS and for Policy Engine to SIP provider

Table 3-4 Default Ports used by Cisco IPICS Components (continued)

Protocol	Device	Destination Port	Remote Device
RTP/RTCP	PMC	UDP 16384-32766	RMS **Note** The session target for voice multicasting dial peers is a multicast address in the range 224.0.1.0 through 239.255.255.255. This session target must be the same for all routers in a session. The audio RTP port is an even number in the range 16384 through 32767, and must also be the same for all routers in a session. An odd-numbered port (UDP port number + 1) is used for the RTCP traffic for that session.
	Policy Engine	UDP 32768-61000	Cisco Unified CallManager, Cisco Unified CallManager Express
ICMP (PING)	PMC	ICMP	Cisco IPICS server
IGMP	PMC	ICMP	Multicast group
SSH	Cisco IPICS server	TCP 22	RMS

Guidelines for Using IP Multicast Addresses with Cisco IPICS

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

- Cisco strongly recommends that you configure IP multicast addresses that are only in the 239.192.0.0 to 239.251.255.255 range.
  - 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.
  - For more information, refer to RFC 3171, *Internet Assigned Numbers Authority (IANA) Guidelines for IPv4 Multicast Address Assignment* and to RFC 2365, *Administratively Scoped IP Multicast*.
- Cisco IPICS permits the use of IP multicast addresses that span the range 224.0.0.0 through 239.255.255.255, where the first octet contains 224, 232, 233, 238 or 239 and subsequent octets contain 0 through 255.
  - Although these well-known group address ranges can be used with Cisco IPICS, they should not be used because they can cause undesirable results if they are used improperly.
  - Refer to RFC 3171 for more information and use guidelines for these IP multicast addresses.

For additional information about the use of IP multicast addressing, refer to the following URL:

http://www.cisco.com/en/US/tech/tk828/tsd_technology_support_protocol_home.html

Multicast and Unicast

When the IPICS solution is configured, channels are assigned static multicast IP addresses and port pairs. Ports that are assigned to a PMC must be within the acceptable port range for a PMC.In addition, the multicast addresses that are defined in the multicast address pool for dynamic allocation must be within the acceptable port range for a PMC.

When a PMC connects using the remote location, it establishes a unicast media connection to an RMS. The UDP port that is assigned for the media connection will be allocated from within the supported range.

QOS Policy Considerations

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

Securing the Cisco IPICS Infrastructure

The following sections provide information about providing system security for Cisco IPICS:

Secure Socket Layer

Cisco IPICS uses Secure Socket Layer (SSL) to encrypt communications between a PMC and 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. In addition, the RMS control uses SSH as a client.

For additional information, refer to the “Installing Third Party Certificates on the Cisco IPICS server section in *Release Notes for Cisco IPICS, Release 1.0(2)*.

Cisco Security Agent

The Cisco Security Agent (CSA), which is optionally available separately from Cisco IPICS, provides intrusion detection and prevention for the Cisco IPICS server and the for the PMC. Instead of focusing on attacks, CSA focuses on preventing malicious and undesired activities on the host. CSA detects and blocks the damaging activities. CSA ships with pre-defined policies that prevent most types of malicious activity from occurring. Since malicious activity is always undesired, security at this level is very inexpensive to deploy. Little or no environment tuning is required. In rare cases, critical business applications can be affected if CSA prevents your web server from adding a new user account

Firewalls and Access Control Lists

Use a firewall and access control lists (ACLs) in front of the 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 to 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 uses UDP ports 21000 through 65534, and a firewall must only open the ports that are needed to support 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 TACACS+ and 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, 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 BPDU Guard and Root Guard
- Disperse critical resources to provide redundancy
- Provide limited and controlled access to power switches
- Use IDS Host software on the Cisco IPICS server and other network servers to ensure security of voice applications

Cisco IPICS Network Management System

When you plan for managing and monitoring a Cisco IPICS network, define the parameters that can be 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 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 Software, including Layer 2 switches. For more detailed information about CMM, refer to this URL:

http://www.cisco.com/en/US/products/ps6337/index.html

If you are using 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 Enterprise IPT management solution, which uses OpenView Gateway Statistics Utility (GSU) Reporting Solution and CiscoWorks IP Telephony Environment Monitor (ITEM) solution 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 underutilized or imbalanced gateway resources, and provides historical trending and forecasting of capacity requirements

Other items to monitor in a Cisco IPICS network in include the following:

- Cisco IPICS server health
- Cisco IPICS services health
- IP gateway health
- Cisco Unified CallManager functionality
- QoS monitoring
- L2/L3 switches and applications

Understanding Dial Peers

Actions taken by a Cisco IPICS administrator or dispatcher often cause the Cisco IPICS server to perform dynamic voice port and dial peer configuration updates to the RMS. In addition to the configuration changes performed by the server, it is sometimes necessary to perform manual configuration changes to the RMS to enable functionality such as unicast connection trunks in a packet network.

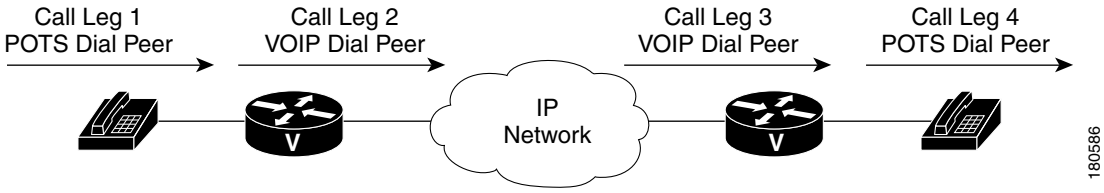
Dial peers identify call source and destination endpoints and define the characteristics that are applied to each call leg in a call connection. Understanding the principles behind dial peers can increase your understanding of how Cisco IPICS works.

This chapter includes these topics:

Dial Peer Call Legs

A traditional voice call over the PSTN uses a dedicated 64 K 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 4-1.

Figure 4-1 Dial Peer Call Legs



A dial peer is associated with each call leg. Attributes that are defined in a dial peer and that are 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 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, which normally is the voice port that connects the router to the local PSTN, 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.

The specific type of voice-network dial peer depends on the packet network technology as follows:

- VoIP (Voice over IP)—Points to the IP address of the destination router that terminates the call
- VoFR (Voice over Frame Relay)—Points to the data-link connection identifier (DLCI) of the interface from which the call exits the router
- VoATM (Voice over ATM)—Points to the ATM virtual circuit for the interface from which the call exits the router

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 to the router. An outbound call leg originates when an outgoing call is placed from the router. Figure 4-2 illustrates call legs from the perspective of the originating router. Figure 4-3 illustrates call legs from the perspective of the terminating router.

Figure 4-2 Originating Router Call Legs

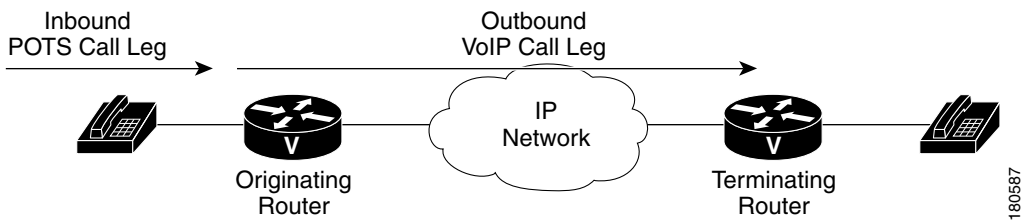
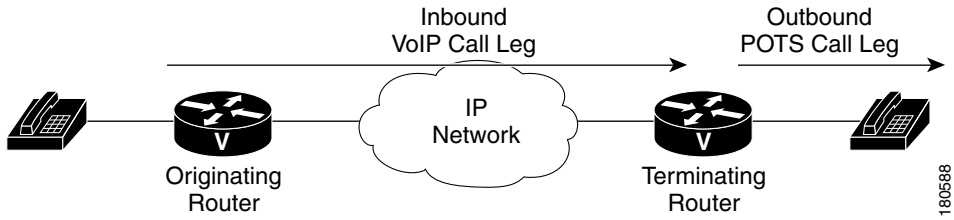


Figure 4-3 Terminating Router Call Legs



For inbound calls from a POTS interface that are destined for the packet network, the router matches a POTS dial peer for the inbound call leg and a voice-network dial peer, such as VoIP or VoFR, for the outbound leg. For inbound calls from the packet network, the router matches a POTS dial peer to terminate the call and a voice-network 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 according to the session target in voice-network 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 voice-network 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 a 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 voice-network dial peer for the outbound call leg. For calls coming into the router from the packet network, the router matches an outbound POTS dial peer to terminate the call and an inbound voice-network dial peer for features such as codec, VAD, and QoS.

Matching Inbound 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 calling number or ANI. It is configured by using the destination-pattern dial-peer configuration command in POTS or voice-network 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 that all the attributes to be configured in the dial peer or that every attribute match the call setup information. The router stops searching when 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.

Matching Outbound Dial Peers

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 using the configured attributes in the matching dial peer.

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

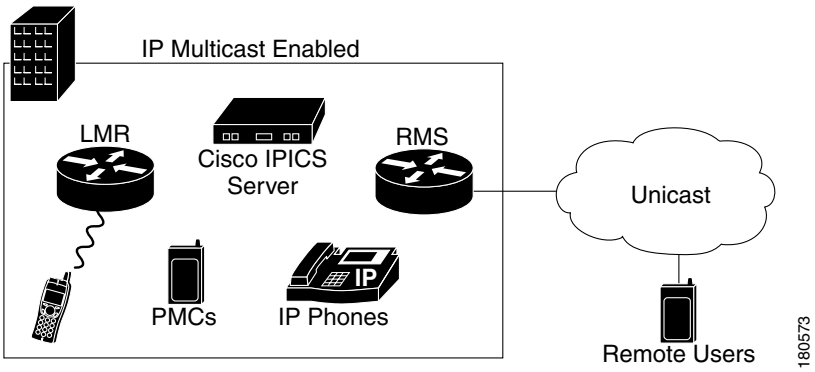
The Cisco IPICS single site model represents a deployment in a single multicast domain. Cisco IPICS components are located at one multicast-enabled site or campus, with no Cisco IPICS multicast services provided over an IP WAN. The single site model typically is deployed over a LAN or a metropolitan area network (MAN), either of which carries the multicast voice traffic within the site. Calls from beyond the LAN or MAN use the Cisco IPICS remote capability to connect to the Cisco IPICS domain via a SIP setup unicast call.

The single site model has the following design characteristics:

- Cisco IPICS server
- RMS
- PMCs
- Cisco Unified IP Phones
- LMR gateways (optional)
- Multicast-enabled network using PIM Sparse mode.
- RMS digital signal processor (DSP) resources for conferencing and transcoding

Figure 5-1 illustrates the Cisco IPICS single site model.

Figure 5-1 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 3, “Cisco IPICS Infrastructure Considerations.”)

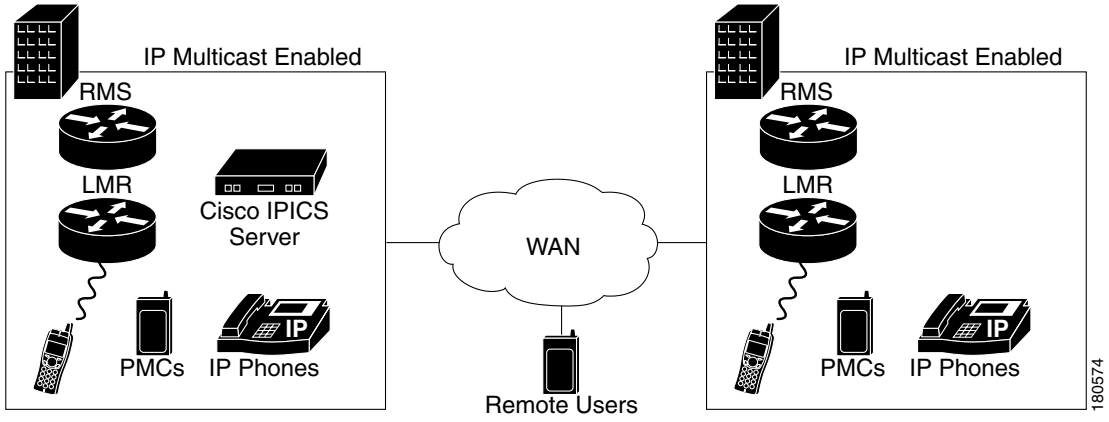
Multiple Site Model

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 may be enabled between sites, but it does not have to be. 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) or M1:U12:M2 connection trunks between sites. IPSec VPNs can also be configured between sites to secure inter-site traffic.

Figure 5-2 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 5-2 Multiple Site Model



In the multiple site model, connectivity options for the IP WAN include the following:

- Leased lines
- Frame Relay
- Asynchronous Transfer Mode (ATM)
- ATM and Frame Relay Service Inter-Working (SIW)
- MPLS Virtual Private Network
- Voice and Video Enabled IP Security Protocol (IPSec) VPN (V3PN)

Routers that reside at the WAN edges 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 typically is scarce.

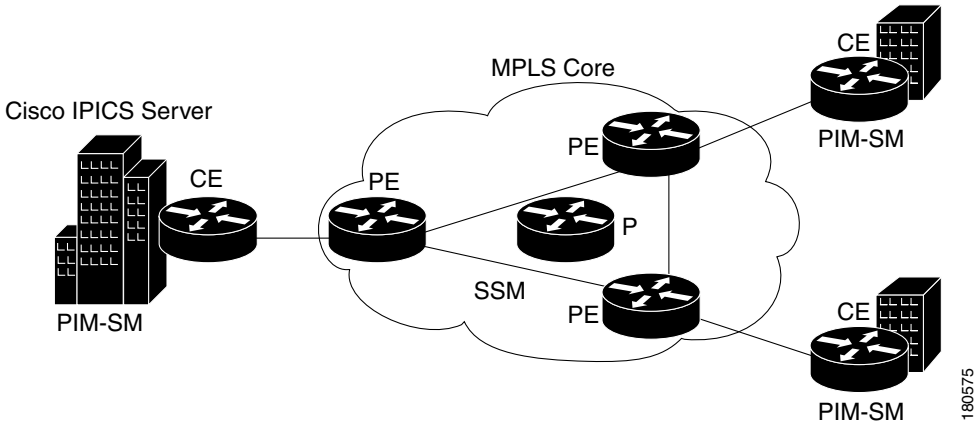
MPLS with Multicast VPNs

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 MPLS 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, refer to the documentation at this URL:

http://www.cisco.com/en/US/products/ps6552/products_ios_technology_home.html

Figure 5-3 illustrates the topology that is discussed in this section.

Figure 5-3 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 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 with 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 route 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. Multicast is used in the core network, so 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 refer to the topology illustrated in Figure 5-3 on page 5-4. 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 is the most widely deployed multicast protocol and is 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 recommended 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 that are 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, use an address outside of this administratively scoped multicast range (as recommended in RFC 2365, *Administratively Scoped Multicast*). 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 as SSM addresses by using 232 in the second octet. In the design that this document discusses, the range is divided for default-MDT and data MDT. (Data MDT is discussed in the "VPN Multicast Routing" section on page 5-5. 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 that is 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 a customer by configuring the PE router as an RP inside the VPN. In the topology that this section discusses, the VPN customer provides the RP service and the PE routers 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-RP inside the VPN. To do so, configure the following on all customer facing interfaces:

```
ip pim sparse-dense-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 5-5, 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 ?
*>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 that is 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 perform additional lookups to determine which MVRF to forward this traffic to, as it is en effect a receiver for this traffic. Verify the `I` 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                                                            Prio/Mode
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` 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                                                            Prio/Mode
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-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-list 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 group-to-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-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 5-5. 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-dense-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:

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.

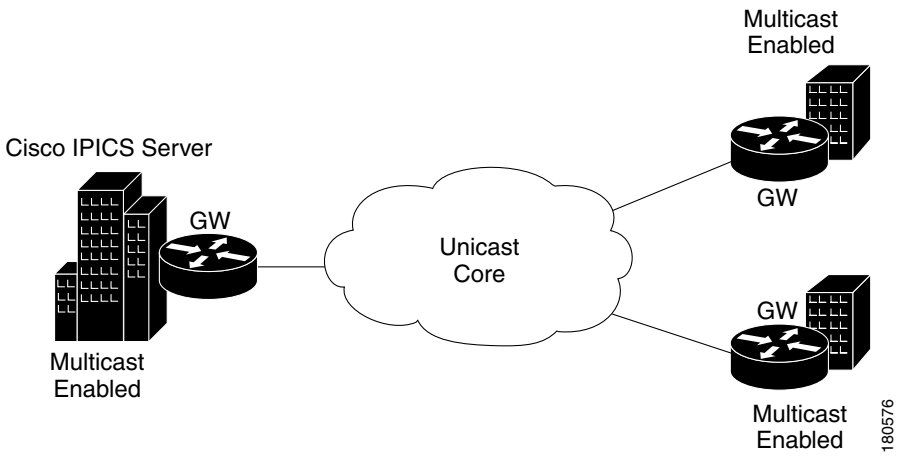
```
PE1#show ip pim vrf ipics mdt receive

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 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 5-4.

Figure 5-4 Multicast Islands



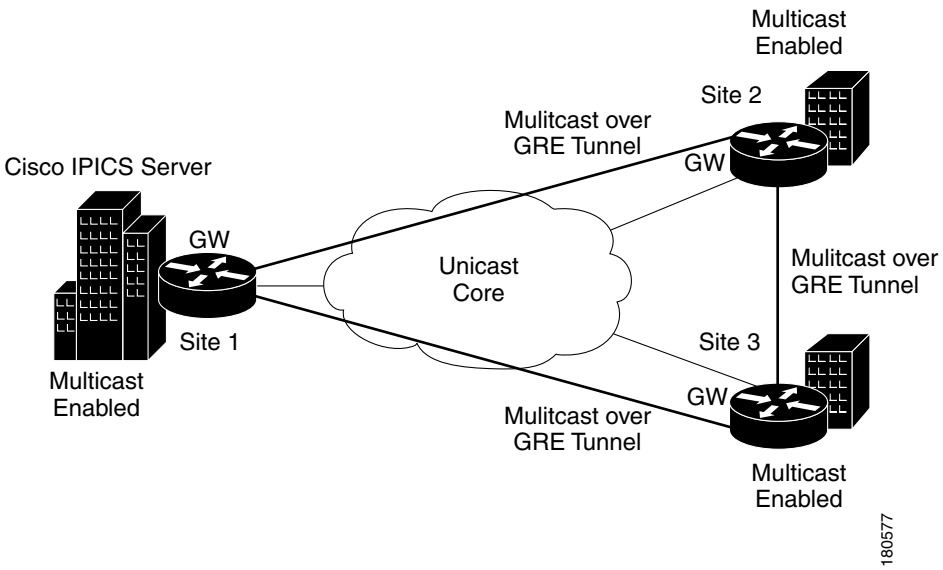
You can use either of these techniques to provide multicast support between the islands:

- Multicast over GRE, page 5-11
- M1:U12:M2 Connection Trunks, page 5-13

Multicast over GRE

This section provides an overview of how to configure multicast over GRE. Figure 5-5 illustrates a Cisco IPICS deployment with multicast over GRE.

Figure 5-5 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 1and Site 3, and between Site 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-dense-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-dense-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 5-1 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 5-1 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 how many active channels/VTGs/PMC users 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 3-2 on page 3-5.

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

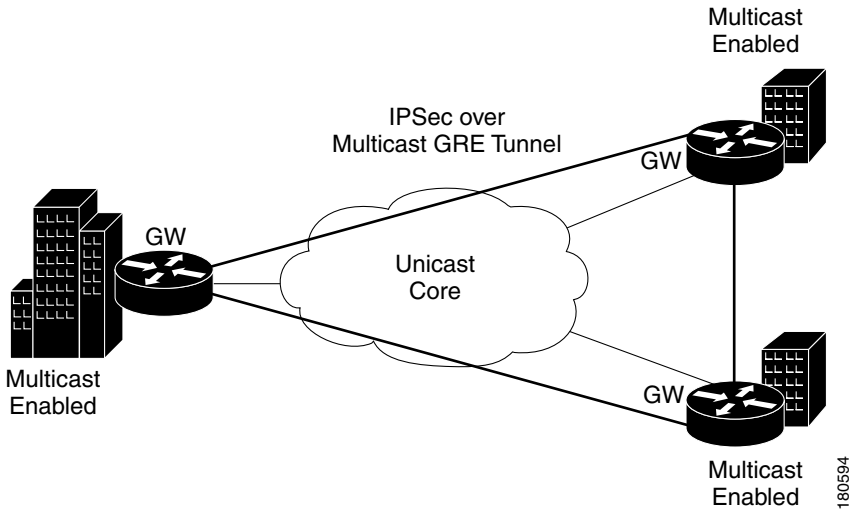
(Call bandwidth is the value from Table 3-1 on page 3-4.)

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

IPSSec VPNs can be implemented over multicast GRE tunnels. See Figure 5-6.

Figure 5-6 IPSec over Multicast GRE Tunnels

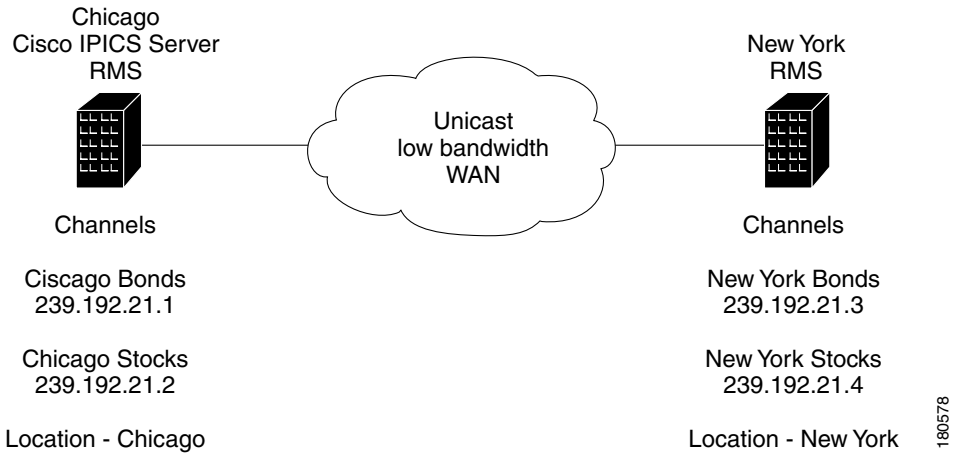


There are a number of ways to configure IPSec over GRE tunnels. Refer to the appropriate Cisco documentation.

M1:U12:M2 Connection Trunks

M1:U12:M2 connection trunks provide an alternative to multicast over GRE tunnels for transporting real-time multicast voice traffic between Cisco IPICS islands. For example, consider the situation shown in Figure 5-7.

Figure 5-7 Unicast-Only Intersite Connection



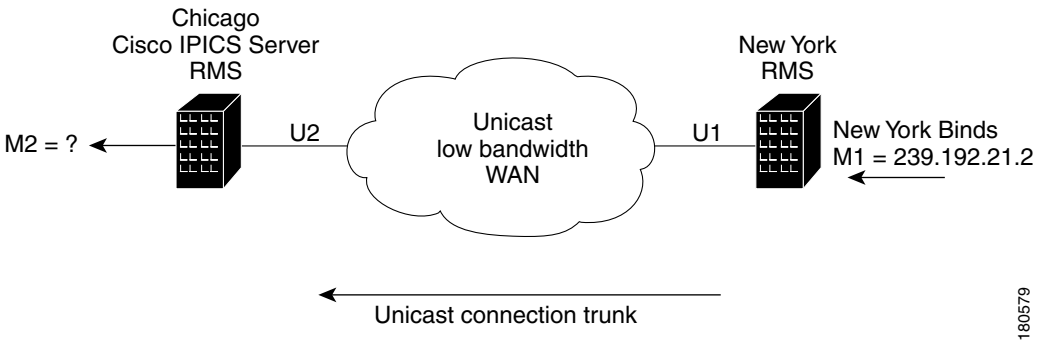
In this example, the Stocks and Bonds Company has offices in Chicago and New York. Each location has two channels configured on the Cisco IPICS server. Because there is no multicast support between Chicago and New York, this scenario requires separate multicast domains, each with its own RP. The locations that are configured on the Cisco IPICS server represent the two multicast domains, Chicago and New York. The channels and the RMS in Chicago must be configured with location Chicago, and the channels and the RMS in New York must be configured with location New York.

Users in Chicago can communicate with each other using the Chicago Stocks or the Chicago Bonds channels. Users in New York can communicate with each other using the New York Stocks or the New York Bonds channels.

Chicago Stocks and Chicago Bonds can be placed in a VTG. Both of these channels have location Chicago, so the Cisco IPICS server mixes these channels using the RMS in Chicago. Similarly, New York Stocks and New York Bonds can be placed in a VTG. Both of these channels have location New York, so the Cisco IPICS server mixes these channels using the RMS in New York.

Interdomain VTGs are not possible. VTGs automatically have the location All, which assumes that all channels and users in the VTG are in the same multicast domain. You can work around this limitation using M1:U12:M2 connection trunks, as shown in Figure 5-8.

Figure 5-8 M1:U12:M2 Connection Trunk



In this example, assume that a VTG consisting of Chicago Bonds and New York Bonds is required. The M1:U12:M2 connection trunk maps the multicast traffic from the New York Bonds channel (M1) to a unicast address (U1) to transport this traffic across the unicast VoIP network. The unicast traffic that is

received by the Chicago RMS is mapped to the multicast address M2. The M2 multicast address will be assigned to the New York Bonds proxy channel in Chicago and placed in a VTG with the Chicago Bonds channel. M2 should be assigned a valid multicast address in the Chicago multicast domain. To avoid conflicts, it should not be an address that is part of the multicast pool or an address that is used by any other channel.

Most deployments have a range of addresses that are allocated for channel use. The following list of ranges shows a typical approach:

239.192.21.1 - 16: Channel addresses

239.192.21.17 - 32: VTG addresses

Also assume that the following addresses have been assigned:

239.192.21.1: Chicago Bonds

239.192.21.2: Chicago Stocks

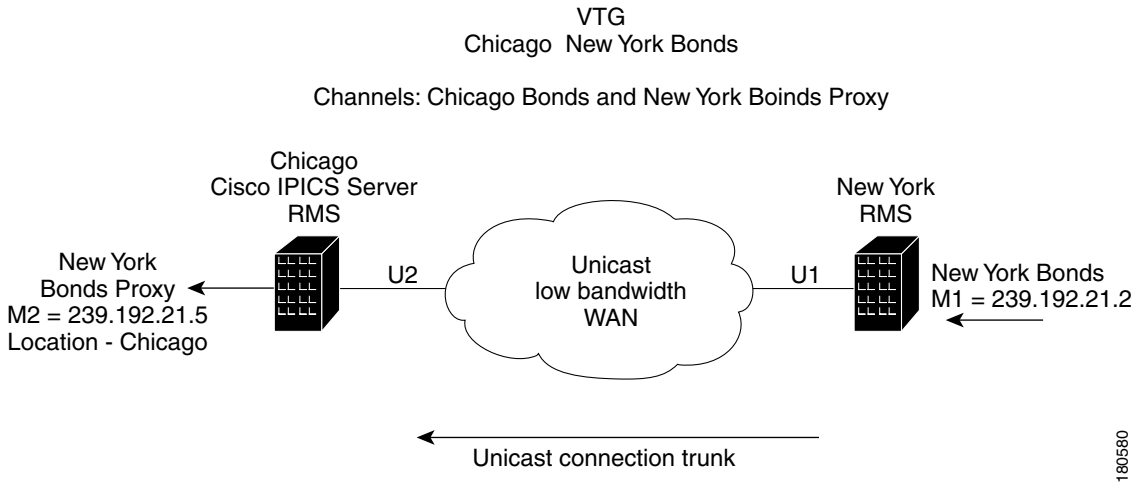
239.192.21.3: New York Bonds

239.192.21.4: New York Stocks

Now assume that the next free address, 239.192.21.5, is used for M2. A VTG can contain channels, users, or both. The VTG being created contains the channel Chicago Bonds, but it also needs to contain a channel that represents New York Bonds. The New York Bonds channel cannot be placed in the VTG because it is not multicast that can be reached by the RMS in Chicago. So a proxy channel is needed to represent the channel New York Bonds in location Chicago.

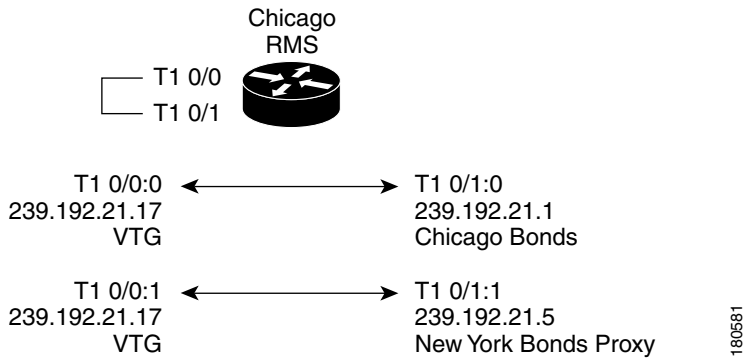
Figure 5-9 shows how to proxy the New York bonds channel in Chicago.

Figure 5-9 Proxy Channel



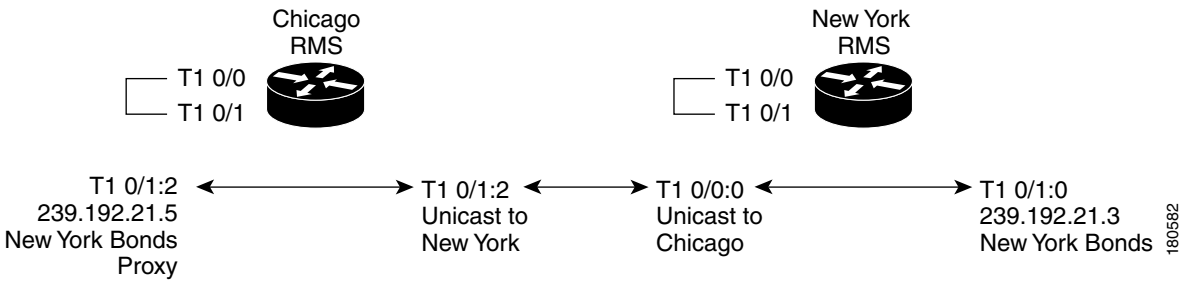
When the VTG called Chicago New York Bonds is created on the Cisco IPICS server, the VTG will contain two channels: Chicago Bonds and New York Bonds Proxy. The Cisco IPICS server configures the RMS in Chicago (both channels have location Chicago) to mix the two channels to the VTG. Assume that Cisco IPICS uses the multicast address 239.192.21.17 for the VTG. Two pairs of DS0s are required on the Chicago RMS to mix the channels to the VTG and the VTG to the channels. Figure 5-10 shows the configuration of the Chicago RMS, which is performed by the Cisco IPICS server for the VTG Chicago New York Bonds. This RMS configuration is the standard for a two-channel VTG.

Figure 5-10 VTG Configuration Performed by the Cisco IPICS Server



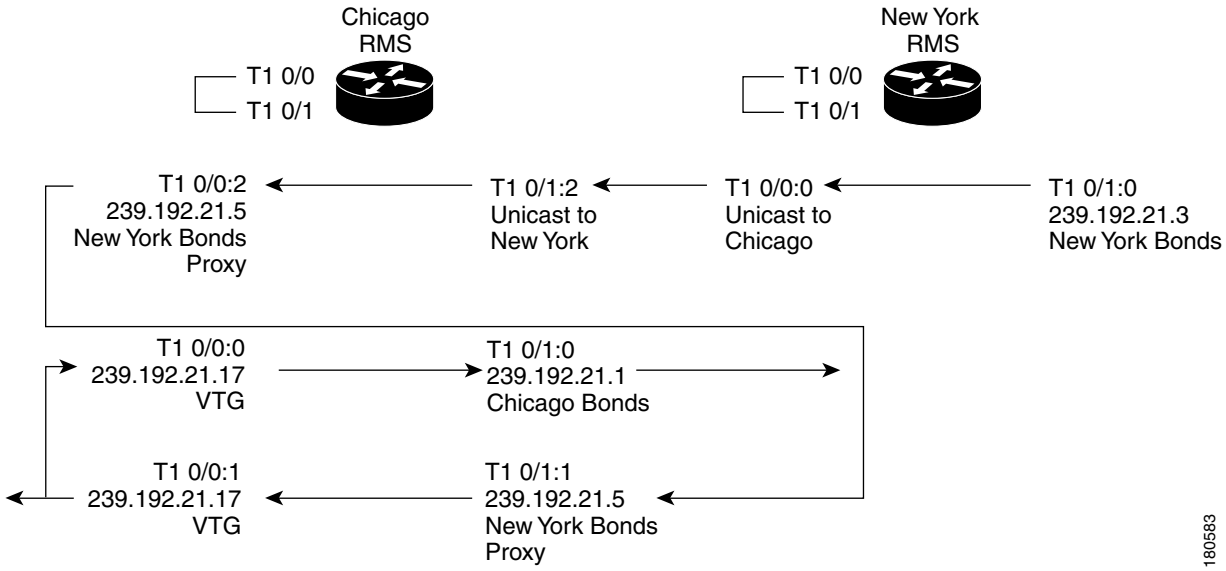
To implement the M1:U12:M2 connection trunk, you must manually configure the RMS. This configuration is needed to transport traffic from New York Bonds to the VTG and from the VTG to New York Bonds. See Figure 5-11.

Figure 5-11 M1:U12:M2 Trunk Configuration



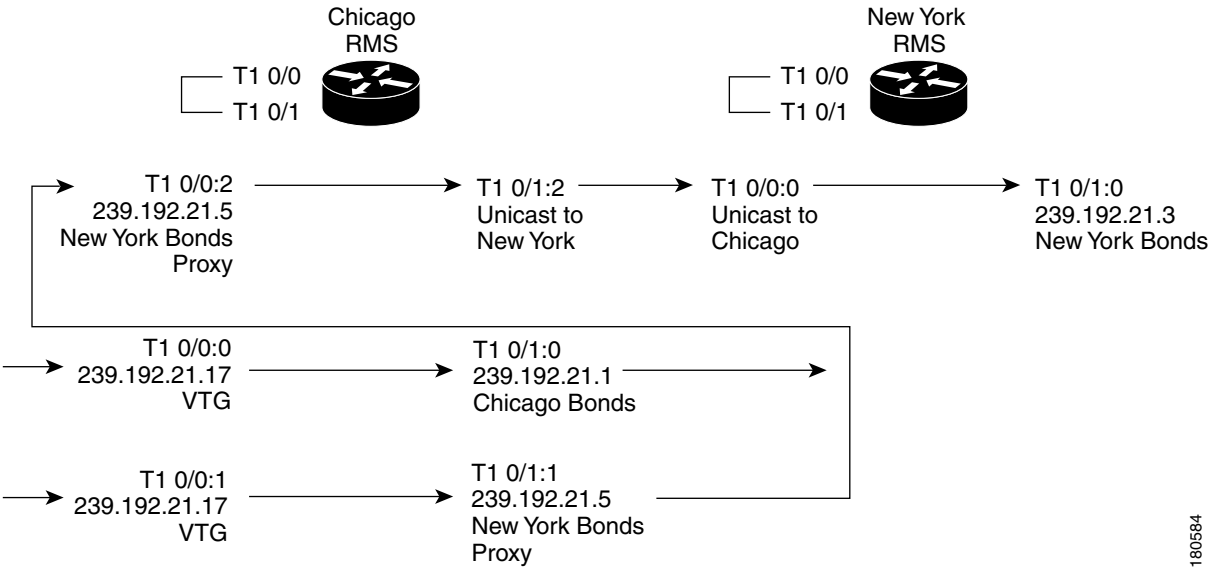
The traffic flow from New York to the VTG is shown in Figure 5-12. In this example, a user in New York is talking on channel New York Bonds on either a PMC, a Cisco Unified IP Phone, or a radio that is connected to an LMR gateway. The destination address is the multicast address that was assigned to the channel when the channel was configured on the Cisco IPICS server. When this traffic reaches the New York RMS, it is sent as unicast across the connection trunk to the Chicago RMS. The Chicago RMS maps the unicast traffic from New York to the New York Bonds Proxy channel, which is mapped to the VTG, which is mapped to the Chicago Bonds channel. Any user listening on either the VTG channel or the Chicago Bonds channel receives the traffic.

Figure 5-12 New York Bonds to the VTG and Chicago Bonds



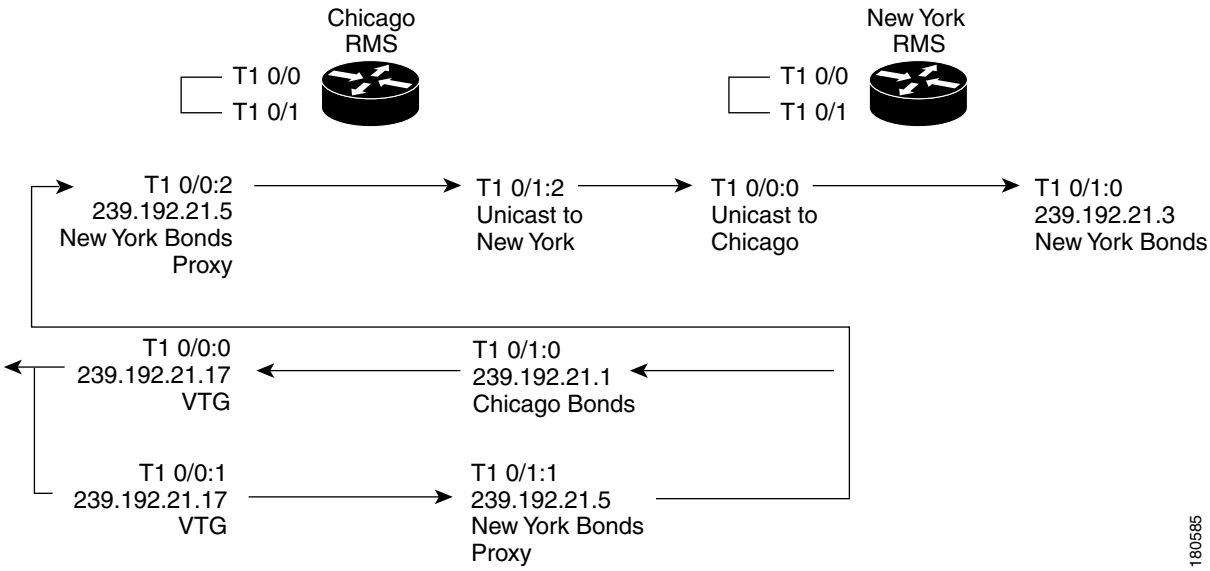
The traffic flow from the VTG to New York Bonds is shown in Figure 5-13. In this example, a user in Chicago talking on the VTG channel sends traffic to the multicast group 239.192.21.17. When this traffic reaches the Chicago RMS, it is mixed to both the New York Bonds Proxy channel and to the Chicago Bonds channel. The traffic that is mapped to the New York Bonds Proxy channel is sent as unicast across the connection trunk to New York, where it is mixed onto the New York Bonds channel.

Figure 5-13 VTG to Chicago and New York Bonds



The traffic flow from Chicago Bonds to New York Bonds is shown in Figure 5-14.

Figure 5-14 Chicago Bonds to VTG and New York Bonds



Whether traffic comes from the VTG (Figure 5-13) or from Chicago Bonds (Figure 5-14) depends on how the VTG is configured. A VTG can have channels, users, or both. If the VTG is created with channels only (Chicago Bonds and New York Bonds Proxy), users in Chicago will not see the VTG channel on their PMCs or Cisco Unified IP Phones. In addition, none of the Chicago users on channel Chicago Bonds or the New York users on channel New York Bonds will know that they are in a VTG. Users in Chicago will send and receive on channel Chicago Bonds and users in New York will send and receive on channel New York Bonds. The only traffic that is sent to or from the VTG channel is internal to the Chicago RMS.

If users associated with channel Chicago Bonds are also placed in the VTG, the VTG appears on their PMCs or Cisco Unified IP Phones. The users can then either activate channel Chicago Bonds or the VTG channel. If they activate the VTG channel, their traffic is sent to the VTG multicast address and mixed to the Chicago Bonds and New York Bonds Proxy channels on the Chicago RMS. Users associated with New York Bonds can never be placed in the VTG because they are in location New York and the VTG is being mixed on the RMS in Chicago.

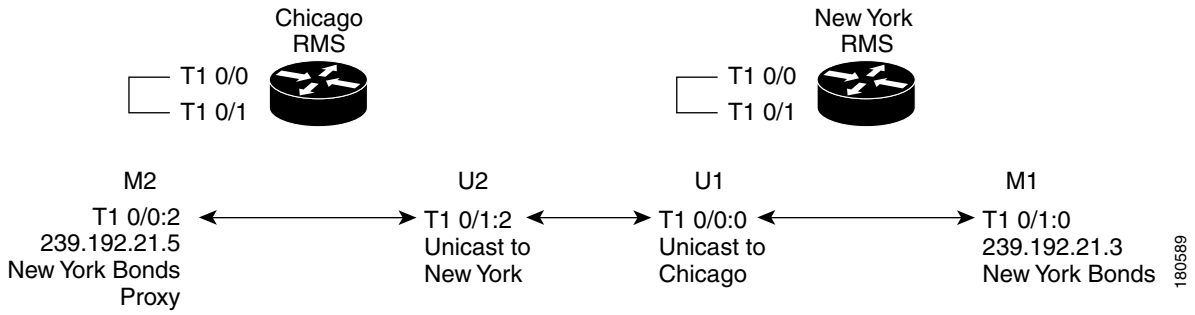
This solution is symmetrical. The VTG could have been created with a Chicago Bonds Proxy with location New York and the New York Bonds channel. In that case, Cisco IPICS would use the New York RMS instead of the Chicago RMS and the operation would be identical to the example presented here.

Unicast Connection Trunk Configuration

This section describes the manual RMS configuration that is required for a unicast connection trunk to enable the M1:U12:M2 Chicago and New York Stocks and Bonds scenario.

Figure 5-15 illustrates the components of the Unicast connection trunk that need to be configured between Chicago and New York.

Figure 5-15 Unicast Connection Trunk Components



Because there are no dialed numbers (from an LMR, PMC, or Cisco Unified IP Phone), the connection trunk digits command is used to generate the dialed number internally and to match a VoIP dial peer. The connection trunk command also establishes a permanent VoIP call between the RMS routers. The sample configuration that follows assumes the use of T1 resources on the RMS and that the T1 ports are configured as follows:

```
controller T1 0/0
 framing esf
 clock source internal
 linecode b8zs
 cablelength short 133
 ds0-group 0 timeslots 24 type e&m-lmr
 ds0-group 1 timeslots 1 type e&m-lmr
 …
 ds0-group 23 timeslots 23 type e&m-lmr
```

If you are using T1 resources on the RMS, Cisco IPICS must be configured to not use the DS0s that are used for the connection trunk.

The following example configuration uses DS0 resources from the RMS T1 loop back on 0/0 and 0/1, so the voice ports must be explicitly blocked to prevent the Cisco IPICS server from dynamically allocating them. To block the DS0s, use the Cisco IPICS Administration Console to disable port 0/0:2 in the Chicago RMS and to disable port 0/0:0 in the New York RMS. (For instructions, refer to the "Viewing and Configuring Loopbacks" section in *Cisco IPICS Server Administration Guide*.) When DS0s are in the Reserved state, the RMS does not attempt to dynamically allocate them.

The following table illustrates the manual configuration that is required to configure the U1 and U2 portions of the connection trunks in the Chicago RMS and New York RMS. In the Session Target fields, substitute the respective RMS Loopback0 IP address for the RMS name.

Chicago Unicast U2	New York Unicast U1
voice-port 0/1:2 timeouts call-disconnect 3 connection trunk 1000 answer mode dial-peer voice 1 voip destination-pattern 1000 session target ipv4:New York RMS (U2) codec g729r8 bytes 20 (Default) vad aggressive ip qos dscp cs5 media dial-peer voice 2 pots destination-pattern 2000 port 0/1:2	voice-port 0/0:0 timeouts call-disconnect 3 connection trunk 2000 dial-peer voice 1 voip destination-pattern 2000 session target ipv4:Chicago RMS (U1) codec g729r8 bytes 20 (Default) vad aggressive ip qos dscp cs5 media dial-peer voice 2 pots destination-pattern 1000 port 0/0:0

The following table illustrates the manual commands required to configure the voice port and dial peer entries in the New York RMS to enable the M1 portion of the M1:U12:M2 connection trunk.

New York Multicast Voice Port	New York Multicast Dial Peer M1
voice-port 0/0:1 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 40 connection trunk 2001	dial-peer voice 3 voip destination-pattern 2001 session protocol multicast session target ipv4:239.192.21.3:21000 (New York Bonds M1) codec g711ulaw vad aggressive

The following table illustrates the manual commands required to configure the voice port and dial peer entries in the Chicago RMS to enable the M2 portion of the M1:U12:M2 connection trunk.

Chicago Multicast Voice Port	Chicago Multicast Dial Peer M2
voice-port 0/0:2 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 40 connection trunk 1001	dial-peer voice 3 voip destination-pattern 1001 session protocol multicast session target ipv4:239.192.21.5:21000 (New York Bonds Proxy M2) codec g711ulaw vad aggressive

Connection Trunk Verification

The following output shows the IOS commands that can be used in an RMS to determine the status of the connection trunk. This sample output shows the dial peers used and shows that the trunked connections are in the connected state.

```
New York#show voice call status
CallID CID   ccVdb      Port      DSP/Ch Called # Codec    Dial-peers
0xF    11F0  0x6772A350 0/0:0.24  0/13:1 2000     g729r8   2/1
0x11   11F3  0x67729198 0/1:0.24  0/13:3 2001     g711ulaw 0/3
2 active calls found

Chicago#show voice call summary | i TRUNKED
0/1:2.24    g729r8      y S_CONNECT          S_TRUNKED
0/0:2:0.24  g711ulaw    y S_CONNECT         S_TRUNKED
```

Bandwidth Considerations for Unicast Connection Trunks

Hoot ‘n’ holler mixing algorithms are described in Chapter 2, “Cisco IPICS Component Considerations” and bandwidth considerations and are described in Chapter 3, “Cisco IPICS Infrastructure Considerations.” To determine the bandwidth required for one unicast connection trunk, find the bandwidth requirement for one voice stream in Table 3-2 on page 3-5.

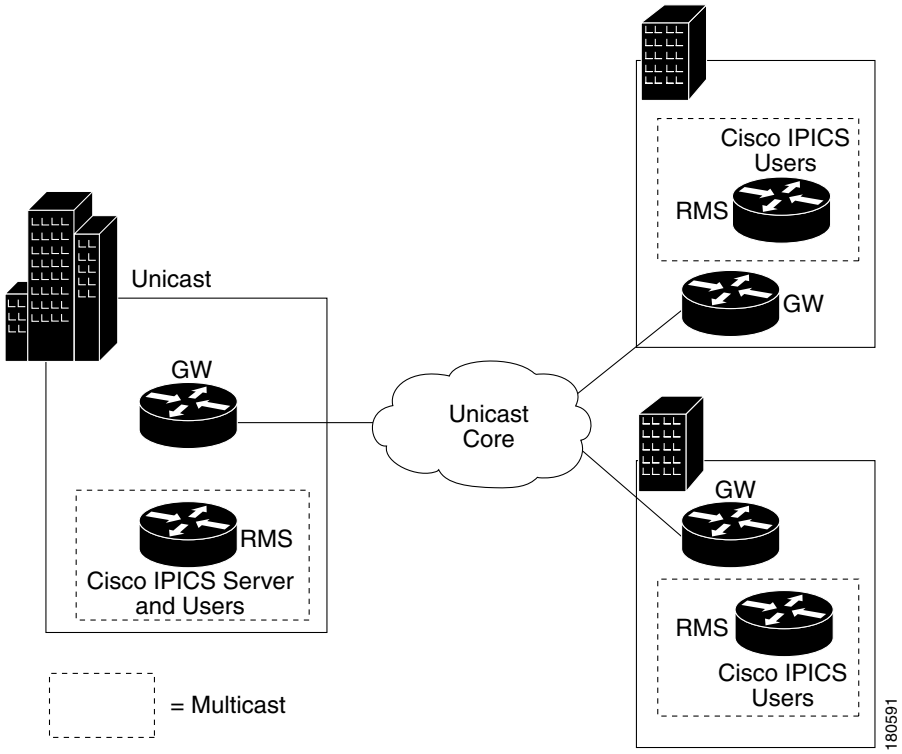
For example, using the G.729 codec, 20 byte payload size, and cRTP with VAD requires 7.3 kbps.

This calculation is the bandwidth for one connection trunk. If more than one connection trunk is used, multiply this number by the number of trunks.

Multicast Singularities

A multicast singularity is a restrictive case of the multicast island scenario. In this case, multicast routing is not enabled between sites. Within a site, multicast is enabled only on Cisco IPICS specific devices: RMS, LMR gateways, PMCs, and Cisco Unified IP Phones. These Cisco IPICS devices reside in a multicast singularity, as shown in Figure 5-16.

Figure 5-16 Multicast Singularities



The singularities can be connected by using multicast over GRE tunnels (as shown in Figure 5-17) or by using M1:U12:M2 connection trunks (as shown in Figure 5-18).

Figure 5-17 Multicast Singularities with GRE Tunnels

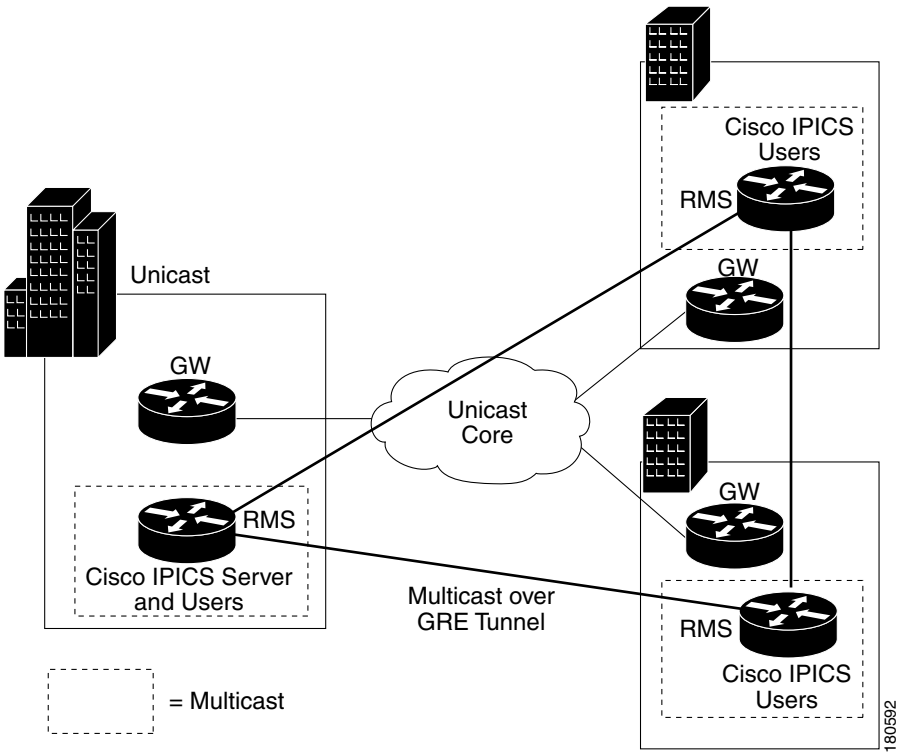
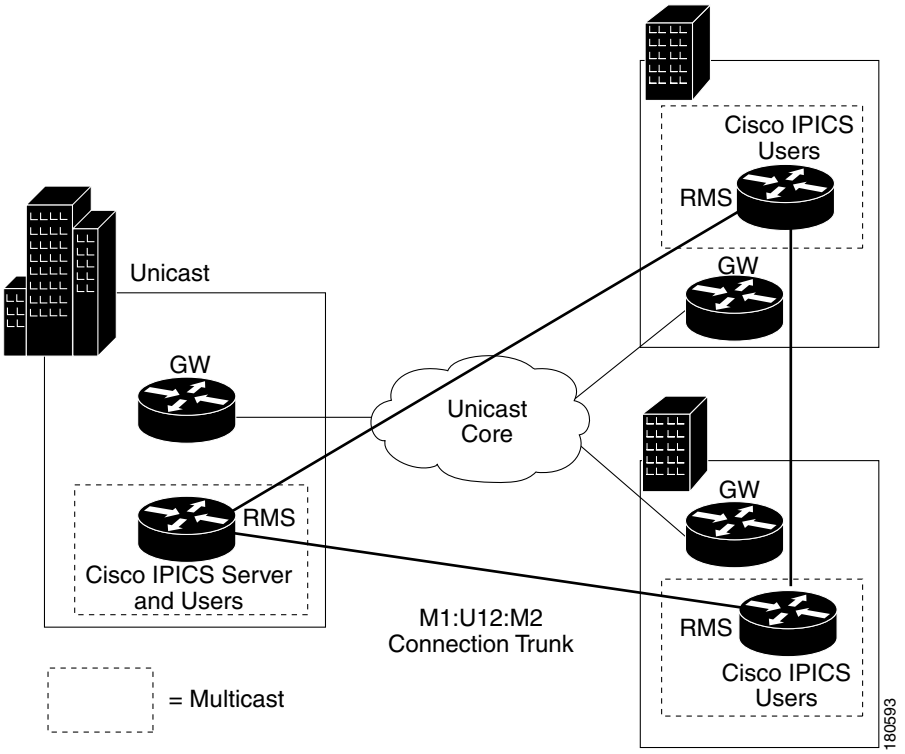


Figure 5-18 Multicast Singularities with M1:U12:M2 Connection Trunks



The configuration of a multicast over GRE tunnel is identical to the multicast island scenario except the tunnel must be configured between the RMS routers and not the gateway routers because the gateway routers are not enabled for multicast. The configuration of an M1:U12:M2 connection trunk is identical to the multicast islands scenario. In both cases, the trunk must be configured between the RMS routers.

The following rules apply to a multicast singularity:

- All RMS and LMR gateways must reside in a multicast singularity. That is, these devices must be on directly connected multicast enabled LANs.
- All users within the multicast singularity can use a PMC or a Cisco Unified IP Phone because they are in the multicast enabled zone.
- Users outside the multicast singularity can use the PMC if they connect using the remote location.
- Users outside the multicast singularity cannot use the Cisco Unified IP Phone because this device supports only multicast.

It is possible to have multiple multicast singularities within the same site with the singularities connected with multicast over GRE tunnels. This solution depends on the policies of the organization.

A

action A discrete function that is performed through a policy. Discrete functions include activate VTG, notification, VTG add participant, dial-out, and invite to VTG.

activate VTG 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.

activated A state that indicates that the SIP (unicast) or multicast channel is fully operational. When a channel/VTG on the PMC is enabled and activated, all of the PMC buttons are operational.

activating A state that becomes effective when you click the **Activate** button on the PMC. The Activate button appears highlighted while the other PMC buttons remain in an inactive state as the system attempts to activate and connect.

activation button This button toggles activate and deactivate functionality on the PMC. Click this button on the PMC to activate a channel (to call out); click it again to deactivate the channel.

active virtual talk group 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.

Administration Console 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.

alert tone buttons Buttons on the PMC that can play out alert tones on one channel or multiple channels.

all talk button Allows you to simultaneously talk on all of the channels that you selected.

autonomous system A radio system under one administrative control; also known as a management domain. This system is usually mapped to an agency.

B

backward compatibility 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.

bandwidth 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.

base station 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

CAI common air interface. The standard for the digital wireless communications medium that is employed for P25-compliant radio systems and equipment. The standard for P25 Phase I incorporates Frequency Division Multiple Access (FDMA) technology.

call delay 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.

call setup time The time that is required to establish a circuit-switched call between users or terminals.

carrier A wave that is suitable for modulation by an information-bearing signal.

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

channel 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. *See* PTT channel.

channel capacity The maximum possible information transfer rate through a channel, subject to specified constraints.

channel folder A logical grouping of channels

channel select check box Provides the ability to select or deselect the specified channel on the PMC for send and receive data.

channel spacing The distance from the center of one channel to the center of the next-adjacent-channel. Typically measured in kilohertz.

Cisco Unified CallManager The software-based call-processing component of the Cisco IP telephony solution. Cisco Unified 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.

Cisco IPICS 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.

Cisco IPICS IP policy engine 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.

Cisco IPICS server Provides the core functionality of the Cisco IPICS system. The Cisco IPICS server software runs on the Linux operating system on selected Cisco Media Convergence Server (MCS) platforms. 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 IP policy engine, which enables telephony dial functionality and is responsible for the management and execution of policies and user notifications.

Cisco Unified IP Phone 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.

Cisco Security Agent Provides threat protection for server and desktop computing systems (endpoints) by identifying, preventing, and eliminating known and unknown security threats.

CLI command-line interface. An interface that allows the user to interact with the operating system by entering commands and optional arguments.

codec coder-decoder.

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

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

conference of conferences A conference that consists of two or more VTGs.

conventional radio system A non-trunked system that is similar to telephone party-line in that the user determines availability by listening for an open channel.

COR carrier operated relay. A signal from a receiver that indicates that the receiver is receiving a signal and that the receiver is not squelched.

coverage 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.

D

delay time The sum of waiting time and service time in a queue.

decrypt Cryptographically restore ciphertext to the plaintext form it had before encryption.

decryption Reverse application of an encryption algorithm to encrypted data, thereby restoring that data to its original, unencrypted state.

dial engine scripts Scripts that the Cisco IPICS dial engine executes to provide the telephony user interface (TUI) for interaction with incoming and outgoing phone calls.

dial-in A phone call that is dialed in to the policy engine.

dial-in floor control 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.

dial number 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.

dial out invite An action that invites selected user(s) to the selected VTG.

A phone call that is dialed out by the policy engine to a phone user to invite the user in to a talk group.

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

digit ID 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.

digital modulation technique A technique for placing a digital data sequence on a carrier signal for subsequent transmission through a channel.

dispatcher The Cisco IPICS dispatcher is responsible for setting up the VTG templates, activating the VTGs to begin conferences, and adding and/or removing participants in VTG templates and active VTGs. The dispatcher also monitors the active VTGs and events, can mute and unmute PMC users, as necessary, and sets up system policies.

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

dynamic regrouping 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

E & M recEive and transMit (or ear and mouth). The E&M interface provides voice signals from radio channels, which are then mapped to IP multicast or unicast. The E&M interface provides the most common form of analog trunking.

1. Trunking arrangement that is generally used for two-way switch-to-switch or switch-to-network connections. Cisco's analog E&M interface is an RJ-48 connector that allows connections to PBX trunk lines (tie lines). E&M also is available on E1 and T1 digital interfaces.

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.

encipher To convert plain text into an unintelligible form by using a cipher.

encode To modify information into the required transmission format.

encryption Application of a specific algorithm so as to alter the appearance of data and make it incomprehensible to unauthorized users.

event An active VTG in the Cisco IPICS solution.

F

FDM frequency-division multiplexing. Technique whereby information from multiple channels can be allocated bandwidth on a single wire based on frequency.

FDMA frequency-division multiple access. A a channel access method in which different conversations are separated onto different frequencies. FDMA is employed in narrowest bandwidth and multiple-licensed channel operations.

FLEXlm Cisco software that enforces licensing on certain systems; FLEXlm ensures that Cisco IPICS software will work only on the supported and licensed hardware.

floor control The standard mechanism for Push-to-Talk speaker arbitration.

frame 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.

frequency For a periodic function, frequency represents the number of cycles or events per unit of time.

frequency assignment Assignment that is given to a radio station to use a radio frequency or radio frequency channel under specified conditions.

frequency hopping The repeated switching of frequencies during radio transmission according to a specified algorithm, intended to minimize unauthorized interception or jamming of telecommunications.

frequency modulation Modulation technique in which signals of different frequencies represent different data values.

frequency sharing 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.

G

gateway 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.

GRE 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.

H

H.323 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.

high-band frequency Refers to the higher frequency levels in the VHF band, typically 138-222 MHz.

Hoot ‘n’ Holler (Hootie) 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

I

inactive VTG A VTG that is stored for use. The Cisco IPICS server stores inactive VTGs so that they can be automatically activated by a policy or manually activated by a dispatcher.

incident management framework A software framework that includes an adaptable GUI to facilitate resources, such as users, radio channels, cameras, and sensor information, for delivery that is based upon policy or incident needs.

interference 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.

interoperability The capability of equipment manufactured by different vendors to communicate with each other successfully over a network.

invitation policy 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.

invite to VTG 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.

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

K

keepalive 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.

key The parameter that defines an encryption code or method.

kilohertz (kHz) A unit of frequency that denotes one thousand Hz.

L

latch The PMC functionality that allows a Cisco IPICS user to lock in a PTT channel.

linear modulation 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.

LMR 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.

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&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.

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.

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 PMC to directly tune in to the multicast channel. Multicast address/port combinations are also used by gateways and RMS 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.

multiselect buttons Provides the ability to select or deselect all channels on the PMC.

mute The functionality that enables a dispatcher to mute a PMC user from talking or transmitting voice on one or more channels. The dispatcher can mute the microphone of the user or both the microphone and the speaker.

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.

National Telecommunication and Information Administration 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.

network An interconnection of communications entities.

NAT Network Address Translation. Provides a mechanism for translating addresses that are not globally unique into globally routable addresses for connection to the Internet.

not activated 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 PMC buttons appear highlighted.

notification 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.

An email, SMS, pager, or phone call that is placed to a user for the purpose of sending a notification message.

O

offline mode When the connection to the server goes offline, the PMC enters offline mode. Offline mode enables continuous communication during periods of server downtime. Using offline mode requires at least one successful login to the server.

operator The Cisco IPICS operator is responsible for setting up and managing users, configuring access privileges, and assigning user roles and ops views.

ops view 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.

ops view administrator The ops view administrator has the ability to administer resources that are assigned to the ops view that the ops view administrator belongs to. Ops view administrator capabilities include managing and monitoring the activity logs that are filtered by ops views and accessible in the Administration Console Activity Log Management window.

OTAR 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

packet A logical grouping of information that includes a header that contains control information. Usually also includes user data.

packet switching 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.

PIM 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.

PIM dense mode 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.

PIM sparse mode 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.

PMC Push-to-Talk Management Center. A standalone PC-based software application that simulates a handheld radio to enable PTT functionality for PC users. This application enables Cisco IPICS PMC end-users, dispatch personnel, and administrators to participate in one or more VTGs at the same time.

PMC ID The unique ID that the Cisco IPICS server generates for each PMC to track requests between the PMC and the server and to verify and manage concurrent PMC usage for licensing requirements.

policy 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.

policy channel A channel that can be set up by the dispatcher and configured as a designated channel; that is, a channel that is always open to enable your interaction with the dispatcher.

policy execution status An indicator of policy execution success or failure. The Cisco IPICS administration console provides a status for each action under a policy,

portalization A web programming paradigm for customizing the interface and functionality of a client application.

protocol A set of unique rules that specify a sequence of actions that are necessary to perform a communications function.

PTT Push-to-talk. A signal to a radio transmitter that causes the transmission of radio frequency energy.

PTT channel 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.

PTT channel button The button on the PMC 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.

PTT channel group A logical grouping of available PTT channels that can be used for categorization.

Q

QoS quality of service. A measurement of performance for a transmission system, including transmission quality and service availability.

queue 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.

queuing delay 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

radio channel 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.

radio equipment 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.

receive indicator The indicator on the PMC that blinks green when traffic is being received.

remote connection Cisco IPICS uses this type of connection to provide SIP-based trunking into the RMS component, which is directly tuned into the multicast channel.

RF 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.

RF repeater 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.

RMS router media service. Component that enables the Cisco IPICS PMC to remotely attach to a VTG. It also provides support for remotely attaching (combining) two or more VTGs through its loopback functionality.

The RMS mixes multicast channels in support of VTGs and it also mixes PMC SIP-based (unicast) connections to a multicast channel or VTG. The RMS can be installed as a stand-alone component (RMS router) or as an additional feature that is installed in the LMR gateway.

RTP Real-Time Transport Procotol. Commonly used with IP networks to provide end-to-end network transport functions for applications transmitting real-time data, such as audio, video, or simulation data, over multicast or unicast network services.

S

scanning 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.

script prompts 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.

secure channel 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 a PMC or Cisco Unified IP Phone.)

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.

service delivery area *See* coverage.

signal The detectable transmitted energy that carries information from a transmitter to a receiver.

skin Skins form the appearance of the PMC. In Cisco IPICS, skins are customizable and available in various options, including 4-channel and 8-channel mouse and touch screen formats.

speaker arbitration The procedure that is used to determine the active audio stream in a Push-to-Talk system.

spectrum The usable radio frequencies in the electromagnetic distribution. The following frequencies have been allocated to the public safety community:

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.

spoken names 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.

squelch An electric circuit that stops input to a radio receiver when the signal being received is too weak to be anything but noise.

stored VTG Also referred to as inactive VTG.

subscriber unit A mobile or portable radio unit that is used in a radio system.

system administrator 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 PMC versions, and monitors the status of the system and its users via the activity log files.

system architecture 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.

T

T1 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.

T1 loopback 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.

talk group A VTG or a channel.

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.

TCP 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.

TDMA 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.

terminal A device capable of sending, receiving, or sending and receiving information over a communications channel.

throughput The number of bits, characters, or blocks passing through a data communications system, or a portion of that system.

TIA/EIA-102 standards A joint effort between government and industry to develop voice and data technical standards for the next generation of public safety radios.

tone control The process of sending a 2175 Hz inband tone with voice transmission to control receiving radios remotely. An inband tone can be used to control functions such as frequency selection and channel monitoring.

transmit indicator On some of the PMC skins, this indicator blinks red when traffic is being transmitted.

trigger A time-based event that invokes a policy on a scheduled basis, without manual intervention.

trunk 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.

trunked (system) Systems with full feature sets in which all aspects of radio operation, including RF channel selection and access, are centrally managed.

trunked radio system 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.

TUI 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.

U

user The Cisco IPICS user may set up personal login information, download the PMC application, customize the PMC skin, 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 the PMC, supported models of Cisco Unified IP Phones, and 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.

unicast Specifies point-to-point transmission, or a message sent to a single network destination.

V

VAD 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 PMC only sends voice traffic when it detects your voice.

virtual channel 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 PMC application or a supported Cisco Unified IP Phone model.

voice interoperability Voice interoperability enables disparate equipment and networks to successfully communicate with each other.

voice replay A feature that allows the PMC user to replay buffered audio on a per channel basis.

VoIP 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.

volume indicator The volume indicator on the PMC that shows the current volume level on the channel in a graphical format.

volume up/down buttons The buttons on the PMC that let you control the volume level.

VOX 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.

VTG virtual talk group. A VTG can contain any combination of channels, channel groups, users, and user groups. A VTG can also contain other VTGs.

VTG add participant An action that adds selected participant(s) to the selected VTG.

VTG template Before becoming active, a VTG is in an inactive state as a VTG template. The server stores VTG templates so that they can be automatically activated by a policy or manually activated by a dispatcher. Also known as a preconfigured VTG.

W

wavelength The representation of a signal as a plot of amplitude versus time.

wideband channel Channels that occupy more than 20 kHz.

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W